Computing Isomorphisms between Products of Supersingular Elliptic Curves

Pierrick Gaudry[a], Julien Soumier[a], Pierre-Jean Spaenlehauer[a]

[a] *Université de Lorraine, CNRS, Inria*

Abstract

The Deligne-Ogus-Shioda theorem guarantees the existence of isomorphisms between products of supersingular elliptic curves over finite fields. In this paper, we present methods for explicitly computing these isomorphisms in polynomial time, given the endomorphism rings of the curves involved. Our approach leverages the Deuring correspondence, enabling us to reformulate computational isogeny problems into algebraic problems in quaternions. Specifically, we reduce the computation of isomorphisms to solving systems of quadratic and linear equations over the integers derived from norm equations. We develop ℓ-adic techniques for solving these equations when we have access to a low discriminant subring. Combining these results leads to the description of an efficient probabilistic Las Vegas algorithm for computing the desired isomorphisms. Under GRH, it is proved to run in expected polynomial time.

Keywords: Superspecial abelian surfaces, Isogenies

1. Introduction

Computing isogenies between elliptic curves has been a vast field of research in the last decade, leading to the development of higher-dimensional techniques in cryptography [1, 2]. In particular, abelian varieties of dimension $g \geq 2$ isogenous to a product of supersingular elliptic curves play an important role in this setting [3, 4, 5, 6, 7] . An important feature of such abelian varieties is that they are all isomorphic over an algebraic closure. Studying the effectiveness of this result leads to interesting algorithmic questions.

Let $\mathbb{F}_q$ be a finite field of characteristic $p > 0$. An abelian variety defined over $\mathbb{F}_q$ is *superspecial* if it is $\overline{\mathbb{F}_q}$-isomorphic to a product of supersingular elliptic curves defined over $\overline{\mathbb{F}_q}$. The Deligne-Ogus-Shioda theorem [8] states that for all $g > 1$, all dimension-g superspecial abelian varieties defined over $\mathbb{F}_q$ are $\overline{\mathbb{F}_q}$-isomorphic (as unpolarized abelian varieties). The aim of this paper is to investigate computational aspects of this theorem.

*This work received funding from the France 2030 program managed by the French National Research Agency under grant agreement No. ANR-22-PETQ-0008 PQ-TLS.

Email addresses: `pierrick.gaudry@loria.fr` (Pierrick Gaudry), `julien.soumier@inria.fr` (Julien Soumier), `pierre-jean.spaenlehauer@inria.fr` (Pierre-Jean Spaenlehauer)

Problem 1.1 (Effective Deligne-Ogus-Shioda problem)**.** *Let $g \geq 2$ be an integer. Given supersingular elliptic curves $E_1, \ldots, E_g$ and $E_1', \ldots, E_g'$ defined over $\mathbb{F}_q$, compute an $\overline{\mathbb{F}_q}$-isomorphism $E_1 \times \cdots \times E_g \to E_1' \times \cdots \times E_g'$.*

This appears to be a difficult computational problem. Indeed, computing the endomorphism ring of a supersingular curve is a computational problem which is considered hard, and the security of several cryptographic constructions relies on it. Solving Problem 1.1 would provide non-trivial information about the endomorphism rings of the curves: From an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$, we can compute four isogenies $\varphi_{ij} : E_j \to E_i'$, and the composition $\widehat{\varphi}_{21}\varphi_{22}\widehat{\varphi}_{12}\varphi_{11} : E_1 \to E_1$ is in general a non-trivial endomorphism of E_1.

In this paper, we study Problem 1.1 in the context where the endomorphism rings of the elliptic curves are given. In this setting, Deuring's correspondence allows us to translate Problem 1.1 into a problem about quaternion algebras.

Contributions. We focus on the case $g = 2$, which is the base case which serves as a building block for the general case $g \geq 2$. Therefore our main problem is the computation of an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$ between two products of supersingular elliptic curves, assuming that their endomorphisms rings are known. Endomorphism rings are given via an efficient representation of a $\mathbb{Z}$-basis together with an explicit isomorphism with a maximal order in the quaternion algebra $\mathscr{B}_{p,\infty}$. Our main contribution is a polynomial-time algorithm that computes an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$ between products of maximal elliptic curves over $\mathbb{F}_{p^2}$, assuming that e know the endomorphism rings of the curves. This algorithm relies on two main subroutines. The first one describes how to build a two by two matrix of isogenies which is an isomorphism, given its first column. The second one allows us to compute isomorphisms of the form $E^2 \to E_1' \times E$ when we know a non-scalar low-discriminant endomorphism in $\mathrm{End}(E)$.

In order to design such algorithms, we need some new computational techniques. For instance, we provide a quasi-linear quaternionic method to divide an endomorphism by an isogeny, see Proposition 4.7. Our main theoretical tool is a necessary and sufficient criterion to decide whether a pair of separable isogenies $\varphi_{11} : E_1 \to E_1'$, $\varphi_{21} : E_1 \to E_2'$ of coprime degrees can appear as the first column of a matrix $(\varphi_{ij})_{i,j \in \{1,2\}}$ describing an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$: this happens precisely when the direct sum of the kernels of φ_{11} and φ_{21} is the kernel of an isogeny $E_1 \to E_2$. This result is formalized in Theorem 5.4.

This criterion is used in our algorithms for both subroutines. In the low-discriminant case, we also use the fact that we can solve efficiently norm equations in low-discriminant imaginary quadratic orders. Consequently we are able to find particular endomorphisms, which allows us to apply our criterion. In both cases, we use Wesolowski's variant [9] of KLPT algorithm [10] as an important building block, whose complexity is proved under GRH.

Finally, we provide a proof-of-concept implementation in the computer algebra software `Magma`, which demonstrates some of the algorithms presented in this paper. In those files we only provide the quaternionic part of the isomorphisms, meaning that we output four ideals $\{I_{ij}\}_{1 \leq i,j \leq 2}$, which are kernel ideals of four isogenies $\varphi_{I_{ij}}$, which form a matrix that represents an isomorphism. This implementation is available at the following url: `https://gitlab.inria.fr/superspecial-surfaces-isomorphisms/experiments`. To recover the isogenies, one can use IdealToIsogeny algorithms, described for example in [6, 11].

Related works. Superspecial abelian varieties are central objects in the recent developments of *isogeny-based cryptography*, as they are the main characters of the new high-dimensional techniques, see e.g. [5, 12, 2]. Being able to compute isomorphisms between such objects would be a useful computational tool. In particular, one typical setting is to consider a special curve which has the property that its endomorphism ring contains a low-discriminant imaginary quadratic order. For instance, when $p \equiv 3 \bmod 4$, the endomorphism ring of the elliptic curve E_0 defined over $\mathbb{F}_{p^2}$ by the equation $y^2 = x^3 + x$ contains a subring isomorphic to $\mathbb{Z}[i]$. Being able to compute an isomorphism between a superspecial abelian variety and E_0^g would give access to these low-discriminant subrings of endomorphisms. Another application of our work is the representation of some polarized abelian varieties. In particular, the Ibukiyama–Katsura–Oort correspondence shows that superspecial principally polarized abelian surfaces (up to polarized isomorphisms) can be represented via two by two matrices over the quaternions (modulo congruence). Algorithms have been recently developed in [13] to perform efficient computations via this representation. Our algorithms contribute to this toolbox since isomorphisms between products of supersingular elliptic curves can be used to compute the Ibukiyama–Katsura–Oort representation of principally polarized abelian surfaces that are not Jacobians of genus-2 curves.

The proof of [14, Thm A.1] provides an explicit construction of an isomorphism between the products $E \times E/(K_1 + K_2)$ and $E/K_1 \times E/K_2$ for K_i finite étale subgroups of coprime orders. This result has similarities with our Theorem 5.4, but it is not general enough for our purposes.

Organization of the paper. First Section 2 describes the background on Deuring correspondence, products of supersingular elliptic curves and efficient representations of isogenies. We state our main results in Section 3. In Section 4, we develop theoretical and computational tools that will be required in the main algorithms. Section 5 is devoted to the computation of isomorphisms between products of supersingular elliptic curves provided that we know their endomorphism rings.

Acknowledgements. We are grateful to Benjamin Wesolowski for providing the ideas that led to the general algorithm in Section 5.4. We thank Jean Kieffer and Damien Robert for fruitful discussions, and the isocrypt people for their interest. We thank Marc Houben for pointing us to [14, Thm A.1].

2. Background

For an elliptic curve E over a field F, we denote by $\mathrm{End}(E)$ its ring of endomorphisms defined over $\overline{F}$, the algebraic closure of F. We also assume that the characteristic p of finite fields is greater than 3. For $p = 2$ (resp. $p = 3$), the algorithmic questions discussed in this paper are trivial since all supersingular elliptic curves over $\mathbb{F}_4$ (resp. $\mathbb{F}_9$) are isomorphic.

Throughout this paper, we use the formalism of group schemes to describe *kernels* of (non-necessarily separable) isogenies, so that any nonzero isogeny (even if it is purely inseparable) has a non-trivial kernel. We refer to [15] for more details on this formalism. In particular, for an elliptic curve E defined over $\overline{\mathbb{F}_p}$, there are bijections between proper left-ideals in $\mathrm{End}(E)$, finite group subschemes in E, and isogenies with domain E up to post-composition by isomorphisms. This follows from the fact that all left-ideals in

End(E) are *kernel ideals*, see [15, Thm. 3.15] for the cases where End(E) has rank 1 or 4, and [16, Thm. 20.(a)] for the CM-case. We also use the following convenient notation: given a finite subgroup scheme K of an elliptic curve E, we let $E \to E/K$ denote the geometric quotient of E by K, where K acts by translation. Therefore, an elliptic E' is isomorphic to E/K if and only if there exists an isogeny $E \to E'$ whose kernel is K. We call the map $E \to E/K$ the canonical isogeny with kernel K.

The main family of curves that we consider are *maximal* elliptic curves over $\mathbb{F}_{p^2}$, i.e. elliptic curves whose number of rational points equals the Hasse-Weil upper bound.

Definition 2.1. *Let E be an elliptic curve over $\mathbb{F}_{p^2}$. We say that E is* maximal *when $\#E(\mathbb{F}_{p^2}) = (p+1)^2$.*

Remark 2.2. *Any supersingular curve E over a field k of characteristic $p > 0$ is $\overline{k}$-isomorphic to a curve defined over $\mathbb{F}_{p^2}$, see [17, Prop. 42.1.7]. Therefore, for computational purposes, it is convenient to consider supersingular curves defined over $\mathbb{F}_{p^2}$. Moreover any such curve is $\overline{\mathbb{F}_p}$-isomorphic to a maximal curve E' (see [18, Lem. 4] and [19, Prop. 5.1]), which has the convenient property that all endomorphisms and isogenies with domain E are also defined over $\mathbb{F}_{p^2}$, see [19, Lem. 5.7].*

2.1. Deuring correspondence

We recall key concepts of the Deuring correspondence. For a more comprehensive study of the subject, we refer to [20] and [17].

2.1.1. Quaternion algebras.

Let p be a prime. We focus on the (unique up to isomorphism) quaternion algebra $\mathscr{B}_{p,\infty}$ over $\mathbb{Q}$ which ramifies at p and ∞. The algebra $\mathscr{B}_{p,\infty}$ is non-commutative, and it has dimension 4 over $\mathbb{Q}$. When $p \equiv 3 \bmod 4$ a $\mathbb{Q}$-basis is $1, i, j, k$, where

$$i^2 = -1, \quad j^2 = -p \quad \text{and} \quad k = i\,j = -j\,i.$$

Any element $\alpha \in \mathscr{B}_{p,\infty}$ can be encoded by coordinates $(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in \mathbb{Q}^4$, such that $\alpha = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$. The *conjugate* of $\alpha = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \in \mathscr{B}_{p,\infty}$ is $\overline{\alpha} = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$. Its *reduced trace* is $\mathrm{Trd}(\alpha) = \alpha + \overline{\alpha} = 2\alpha_0$ and its *reduced norm* is $\mathrm{Nrd}(\alpha) = \alpha \cdot \overline{\alpha} = \alpha_0^2 + \alpha_1^2 + p(\alpha_2^2 + \alpha_3^2) \in \mathbb{Q}$. Every nonzero $\alpha \in \mathscr{B}_{p,\infty}$ is invertible, i.e. there exists a unique $\beta \in \mathscr{B}_{p,\infty}$ such that $\alpha \cdot \beta = \beta \cdot \alpha = 1$.

We now focus on subrings in $\mathscr{B}_{p,\infty}$ involved in the Deuring correspondence:

Definition 2.3 (Quaternion order)**.** *An order in $\mathscr{B}_{p,\infty}$ is a subring which has rank 4 as a $\mathbb{Z}$-module. An order is maximal when it is not contained in a strictly larger order.*

Example 2.4. *Assume that $p \equiv 3 \bmod 4$. A non-maximal order of $\mathscr{B}_{p,\infty}$ is $\mathbb{Z}[i, j]$. This order is contained in $\mathbb{Z}[i, \frac{1+k}{2}]$ [10, Lem. 2], which is maximal.*

Definition 2.5 (Left/Right Order)**.** *Let I be a rank-4 $\mathbb{Z}$-module in $\mathscr{B}_{p,\infty}$. The left and* right *orders of I are:*

$$\mathscr{O}_L(I) = \{\alpha \in \mathscr{B}_{p,\infty} : \alpha I \subset I\}, \quad \mathscr{O}_R(I) = \{\alpha \in \mathscr{B}_{p,\infty} : I\alpha \subset I\}.$$

When $I \subset \mathscr{O}_L(I)$ (or equivalently $I \subset \mathscr{O}_R(I)$, see [17, Lem. 16.2.8]), we say that I is an integral ideal.

Integral ideals in maximal orders are actually locally principal [17, Cor. 17.2.3]. It implies that the completion $I \otimes \mathbb{Z}_\ell$ of an ideal $I \subset \mathscr{O}$ at a prime ℓ unramified in $\mathscr{B}_{p,\infty}$ generates a principal ideal in $\mathscr{O} \otimes \mathbb{Z}_\ell \cong \mathrm{M}_2(\mathbb{Z}_\ell)$. We study localizations in more details in Section 4.4.

Remark 2.6. *An integral ideal I is a left-$\mathscr{O}_L(I)$ ideal, and a right-$\mathscr{O}_R(I)$ ideal. When $\mathscr{O}_L(I)$ (equivalently, $\mathscr{O}_R(I)$) is maximal, then I is called a connecting ideal for $\mathscr{O}_L(I)$ and $\mathscr{O}_R(I)$. If $\mathscr{O}_1, \mathscr{O}_2 \subset \mathscr{B}_{p,\infty}$ are two maximal orders, we let $\mathrm{Conn}(\mathscr{O}_1, \mathscr{O}_2)$ denote all integral connecting ideals.*

Definition 2.7 (Ideal norm)**.** *[17, Thm. 16.1.3] Let $I \subset \mathscr{B}_{p,\infty}$ be an ideal. The* reduced norm *of I is $\mathrm{Nrd}(I) = \gcd(\{\mathrm{Nrd}(\alpha) : \alpha \in I\})$. Moreover, $\mathrm{Nrd}(I)^2 = [\mathscr{O}_L(I) : I] = [\mathscr{O}_R(I) : I]$.*

Proposition 2.8. *[17, Lem. 16.3.7] Let $\mathscr{O}_1, \mathscr{O}_2, \mathscr{O}_3 \subset \mathscr{B}_{p,\infty}$ be three maximal orders. If $I \in \mathrm{Conn}(\mathscr{O}_1, \mathscr{O}_2)$ and $J \in \mathrm{Conn}(\mathscr{O}_2, \mathscr{O}_3)$, then $I \cdot J \in \mathrm{Conn}(\mathscr{O}_1, \mathscr{O}_3)$ and $\mathrm{Nrd}(I \cdot J) = \mathrm{Nrd}(I) \cdot \mathrm{Nrd}(J)$.*

2.1.2. The correspondence.

Endomorphism rings of supersingular elliptic curves are isomorphic to maximal orders in $\mathscr{B}_{p,\infty}$. The purpose of Deuring correspondence is to provide a set of tools for representing geometric objects related to supersingular elliptic curves as algebraic objects in $\mathscr{B}_{p,\infty}$.

Theorem 2.9. *[17, Thm. 42.1.9] Let E be a supersingular elliptic curve defined over $\overline{\mathbb{F}_p}$. Then the endomorphism ring $\mathrm{End}(E)$ is isomorphic to a maximal order in $\mathscr{B}_{p,\infty}$.*

Let $\mathscr{O} \subset \mathscr{B}_{p,\infty}$ be a maximal order isomorphic to the endomorphism ring $\mathrm{End}(E)$ of a supersingular elliptic curve E defined over $\overline{\mathbb{F}_q}$. We will implicitly use the isomorphism $\mathrm{End}(E) \to \mathscr{O}$ in what follows. There is an anti-equivalence between the category of supersingular elliptic curves over $\overline{\mathbb{F}_q}$ and the category of invertible left $\mathscr{O}$-modules. This anti-equivalence is given explicitly via the contravariant functor $\mathrm{Hom}(\_, E)$, see [17, Thm. 42.3.2]. This equivalence establishes a dictionary between the geometric world of supersingular elliptic curves and the algebraic world of quaternion orders.

On the one hand, let J be a left $\mathrm{End}(E)$-ideal. It defines a subgroup scheme $E[J] := \cap_{\alpha \in J} \ker \alpha$ in E, which is the kernel of an isogeny $\varphi_J : E \to E/E[J]$, see [17, 42.2.1]. If φ_J is separable, then $E[J] = \{P \in E(\overline{\mathbb{F}_q}) \mid \forall \alpha \in I, \alpha(P) = 0\}$. On the other hand, let $\varphi : E \to E'$ be an isogeny. Then $I_\varphi := \mathrm{Hom}(E', E)\varphi$ is a left $\mathrm{End}(E)$-ideal which connects the endomorphism rings of E and $E' \simeq E/\ker(\varphi)$, regarded as maximal orders in $\mathscr{B}_{p,\infty}$ up to conjugation. Moreover, for a left-ideal $J \subset \mathscr{O}$ and $\psi : E \to E'$, we have that $J = I_{\varphi_J}$ and $\psi \cong \varphi_{I_\psi}$. In particular we have a bijection between isomorphism classes (i.e. isogenies up to post-composition by isomorphisms) of isogenies from E, and left-ideals I in $\mathscr{O}$.

In Table 1 — which is adapted from [20, Table 2.1] — we summarize the main dictionary in the Deuring correspondence.

2.2. Efficient representations of isogenies

In order to implement the constructions of this work, we have to define what is a good representation of an isogeny. We will use the notion of *efficient representation* designed in [21, 22].

Supersingular j-invariants over $\mathbb{F}_{p^2}$ $j(E)$ up to Galois conjugacy	Isomorphism class of maximal order in $\mathscr{B}_{p,\infty}$ $\mathscr{O} \cong \mathrm{End}(E)$
Isomorphism class of $\varphi : E \to E'$	I_φ integral left $\mathscr{O}$-ideal
$\alpha \in \mathrm{End}(E)$	principal ideal of $\mathscr{O}$ generated by the image of α
$\deg(\varphi)$	$\mathrm{Nrd}(I_\varphi)$
$\widehat{\varphi}$	$\overline{I_\varphi}$
Composition $\psi_2 \circ \psi_1 : E_1 \to E_2 \to E_3$	$I_{\psi_2 \circ \psi_1} = I_{\psi_1} I_{\psi_2}$

Table 1: Summary of the Deuring correspondence.

A *representation* of an isogeny $\varphi : E \to E'$ between elliptic curves defined over $\mathbb{F}_q$, is a set of data that contains the domain, the codomain, the degree $\deg(\varphi)$, and an algorithm to evaluate φ on any point $P \in E(\mathbb{F}_{q'})$ for any finite extension $\mathbb{F}_{q'}/\mathbb{F}_q$. Notice that a bound on the degree (instead of the actual degree) would be sufficient since the degree can then be recovered via the CRT by using the Weil pairing in small torsion subgroups [22, Lem. 6.2]. We say that a representation is *efficient* if this data enable us to compute the image of a point $P \in E(\mathbb{F}_{q'})$ in time polynomial in both $\log(\deg(\varphi))$ and $\log(q')$. We say that it is *compact* if the space needed to store the data is polynomial in $\log(\deg(\varphi))$ and $\log(q')$.

The representation we will use is the *ideal representation* which relies on the Deuring correspondence.

2.2.1. Ideal representation.

The core idea of the ideal representation is to represent an isogeny $\varphi : E \to E'$ via the ideal $I_\varphi \subset \mathrm{End}(E)$ of all endomorphisms whose kernel contains $\ker \varphi$, seen as an ideal in a maximal order of $\mathscr{B}_{p,\infty}$ isomorphic to $\mathrm{End}(E)$. In order to use this representation, we first need to fix an embedding $\mathrm{End}(E) \hookrightarrow \mathscr{B}_{p,\infty}$. Although this only encodes the isomorphism class of φ, knowing the codomain E' enables us to determine φ up to post-composition by automorphisms. Consequently, in order to have a full representation of φ, we need a bit more data to discriminate these automorphisms. We can disregard this subtlety in the present work: the order of $\mathrm{Aut}(E')$ is at most 24, so we can use exhaustive search on the automorphism group when needed without harming the asymptotic complexity. However, for efficient implementation and optimization, it might be useful to add to the data structure representing the isogenies some information to remove the ambiguity, for instance the action of the isogenies on some small torsion subgroup. Note that if $j(E') \neq 0, 1728$ then the only automorphisms of E' are ± 1 [23, Appendix A, Prop. 1.2.(c)].

Theorem 2.10. *Given an efficient representation of a $\mathbb{Z}$-basis of* $\mathrm{End}(E)$ *and its image via an embedding* $\mathrm{End}(E) \hookrightarrow \mathscr{B}_{p,\infty}$*, then a $\mathbb{Z}$-basis of the ideal I_φ provides a compact representation of φ. Assuming GRH, this representation is efficient.*

For more details, see [22, Sec. 4.2 and C.1]. In this paper, we will work with 2×2 matrices whose entries are isogenies, which can conveniently be encoded via efficient representations.

Proposition 2.11. *Let $E_1, E_2, E_1', E_2', E_1'', E_2''$ be elliptic curves defined over $\mathbb{F}_q$. Let $M = (\varphi_{ij})_{i,j \in \{1,2\}}$ (resp. $N = (\psi_{ij})_{i,j \in \{1,2\}}$) be a 2×2 matrix of isogenies, where $\varphi_{ij} : E_j \to E_i'$*

(resp. $\psi_{ij} : E'_j \to E''_i$). Then M (resp. N) represents the isogeny $E_1 \times E_2 \to E'_1 \times E'_2$ (resp. $E'_1 \times E'_2 \to E''_1 \times E''_2$) defined as $\phi_M(P,Q) = (\varphi_{11}(P) + \varphi_{12}(Q), \varphi_{21}(P) + \varphi_{22}(Q))$ (resp. $\phi_N(P,Q) = (\psi_{11}(P) + \psi_{12}(Q), \psi_{21}(P) + \psi_{22}(Q))$). Moreover, the matrix product $N \cdot M = (\sum_{k\in\{1,2\}} N_{ik} \circ M_{kj})_{i,j\in\{1,2\}}$ represents an isogeny $E_1 \times E_2 \to E''_1 \times E''_2$ and efficient representations of the entries of $N \cdot M$ can be computed in polynomial-time from efficient representations of the entries of M and N.

Proof. The only thing that we need to prove is that we can compute efficient representations of compositions and sums of isogenies encoded with efficient representations. Algorithms for doing so are described in [22, Sec. 6.1]. □

2.2.2. Knowing the endomorphism ring of a curve.

Throughout this paper, we often say that the endomorphism ring of a supersingular elliptic curve E is "known" or "given". By this, we mean that efficient representations of a $\mathbb{Z}$-basis $b_1, \dots, b_4$ of $\mathrm{End}(E)$ is given, and that we also have access to elements $\beta_1, \dots, \beta_4 \in \mathscr{B}_{p,\infty}$ such that the $\mathbb{Z}$-module $\mathscr{O}$ generated by $\beta_1, \dots, \beta_4$ in $\mathscr{B}_{p,\infty}$ is a maximal order and the map $\mathrm{End}(E) \to \mathscr{O}$ sending b_i to β_i is a ring isomorphism.

2.3. Superspecial Abelian varieties

The key theoretical result we rely on is the following existential statement.

Theorem 2.12. *(Deligne/Ogus/Shioda theorem) [8, Thm. 3.5] Let k be an algebraically closed field of characteristic $p > 0$. Let $E_1, \dots, E_g$ and $E'_1, \dots, E'_g$ be supersingular elliptic curves, where $g \geq 2$. Then there exists an isomorphism:*

$$E_1 \times \cdots \times E_g \cong E'_1 \times \cdots \times E'_g.$$

In other words, Theorem 2.12 states that there is only one superspecial abelian variety of dimension $g \geq 2$, up to isomorphisms. We emphasize that we do not take into account the *polarizations* of the abelian varieties.

Definition 2.13. *An abelian variety $\mathscr{A}$ is called superspecial when it is isomorphic to a product of supersingular elliptic curve.*

When $p \equiv 3 \bmod 4$, there is a convenient supersingular elliptic curve defined over $\mathbb{F}_p$ by the equation $y^2 = x^3 + x$. We denote this special curve by E_0 throughout this paper. A useful feature of this curve is that $\mathrm{End}(E_0)$ contains a subring isomorphic to $\mathbb{Z}[i]$. A direct consequence of Deligne/Ogus/Shioda theorem is that any superspecial variety of dimension g defined over $\overline{\mathbb{F}_p}$ is $\overline{\mathbb{F}_p}$-isomorphic to E_0^g.

Remark 2.14. *Theorem 2.12 is false for $g = 1$, since for instance the curve defined by $E : y^2 = x^3 + 142x + 23$ is isogenous to E_0 over $\mathbb{F}_{307^2}$, but not isomorphic to E_0. However, $E_0^2 \cong E^2$.*

If E_1, E_2, E'_1, E'_2 are supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, Theorem 2.12 implies that $E_1 \times E_2$ and $E'_1 \times E'_2$ are $\overline{\mathbb{F}_p}$-isomorphic. In fact, when E_1, E_2, E'_1, E'_2 are maximal, this isomorphism is defined over $\mathbb{F}_{p^2}$, see [19, Lem. 5.2].

In this work, we explore the problem of computing explicit isomorphisms between products of supersingular elliptic curves. Moreover, as explained in Remark 2.2, we can choose maximal models for the supersingular elliptic curves we work with. The goal of this article is thus to find an $\mathbb{F}_{p^2}$-isomorphism between the products $E_1 \times \cdots \times E_g$ and $E'_1 \times \cdots \times E'_g$, where the curves are maximal over $\mathbb{F}_{p^2}$.

Remark 2.15. *If the supersingular input curves are not maximal, we can start by computing $\overline{\mathbb{F}_p}$-isomorphic maximal curves. This can be done efficiently and it does not have any impact on our complexity bounds, see [18, Lem. 4].*

3. Main Results

Our main algorithmic result is:

Theorem 3.1. *Let $E_1, \dots, E_g$ and $E'_1, \dots, E'_g$ be maximal elliptic curves over $\mathbb{F}_{p^2}$ of known endomorphism rings, where $g \geq 2$. Assuming GRH, we give a probabilistic Las Vegas algorithm which computes in linear time in g and polynomial time in $\log(p)$ an $\mathbb{F}_{p^2}$-isomorphism of unpolarized abelian varieties:*

$$E_1 \times \cdots \times E_g \cong E'_1 \times \cdots \times E'_g.$$

In fact, the key point is to prove the following theorem.

Theorem 3.2. *Let E_1, E_2 and E'_1, E'_2 be maximal elliptic curves over $\mathbb{F}_{p^2}$ of known endomorphism rings. Assuming GRH, we give a probabilistic Las Vegas algorithm which computes in polynomial time in $\log(p)$ an $\mathbb{F}_{p^2}$-isomorphism of unpolarized abelian surfaces:*

$$E_1 \times E_2 \cong E'_1 \times E'_2.$$

The rest of the paper will be dedicated to the proof of Theorem 3.2. Let us explain how to deduce Theorem 3.1 from Theorem 3.2.

Proof that Theorem 3.2 implies Theorem 3.1. We provide a proof by induction on g, assuming that the result is true for $g = 2$ by Theorem 3.2.

By Deligne-Ogus-Shioda theorem, an isomorphism $E_1 \times \cdots \times E_g \to E'_1 \times \cdots \times E'_g$ can be factored as a composition

$$E_1 \times \cdots \times E_g \to E'_1 \times \cdots \times E'_{g-1} \times E_g \to E'_1 \times \cdots \times E'_g.$$

This boils down to computing one $(g-1)$-dimensional isomorphism $E_1 \times \cdots \times E_{g-1} \to E'_1 \times \cdots \times E'_{g-1}$ and one 2-dimensional isomorphism $E'_{g-1} \times E_g \to E'_{g-1} \times E'_g$. By induction, this proves that computing a g-dimensional isomorphism can be reduced to computing $g-1$ isomorphisms in dimension 2. □

4. Tools

In this section, we develop tools which will be useful for computing isomorphisms in Section 5. In Section 4.1, we study algorithms for dividing endomorphisms by isogenies. Section 4.2 proves a slight improvement of Kani's formula for the degree of an isogeny between products of elliptic curves; this is useful for proving that an isogeny is an isomorphism. In Section 4.3, we show how to "transpose" isogenies between products of elliptic curves: we provide an easy way to construct an isogeny $E'_1 \times E'_2 \to E_1 \times E_2$ from an isogeny $E_1 \times E_2 \to E'_1 \times E'_2$, while preserving the degree. Finally, in Section 4.4, we design algorithms for finding the generator of the localization of a left-ideal in a maximal order of $\mathscr{B}_{p,\infty}$.

4.1. Division of principal ideals in quaternion orders

The first tool that we need is a method for dividing efficiently an endomorphism by an isogeny. More precisely, given an endomorphism $\phi \in \mathrm{End}(E_1)$, which factors by an isogeny $f : E_1 \to E_2$, we wish to compute an isogeny $g : E_2 \to E_1$ (which is uniquely defined up to composition by automorphisms) such that $\phi = g \circ f$. A general method when isogenies are given via efficient representations is described in [22, Cor. 6.8]. A detailed complexity analysis is provided in [24, Sec. 4] when g is a scalar multiplication. We propose here an explicit complete algebraic solution to the quaternionic version of the problem, i.e. when all isogenies are represented as ideals in $\mathscr{B}_{p,\infty}$. This factorization problem is formalized in quaternion algebras as follows:

Problem 4.1 (Principal ideal division)**.** *Let $\mathscr{O}_1, \mathscr{O}_2, \subset \mathscr{B}_{p,\infty}$ be two maximal orders. Let $\mu \in \mathscr{O}_1$, $I \in \mathrm{Conn}(\mathscr{O}_1, \mathscr{O}_2)$, and J be a left $\mathscr{O}_2$-ideal such that $\mathscr{O}_1\mu = I \cdot J$. Given μ and $\mathbb{Z}$-bases of $\mathscr{O}_1, \mathscr{O}_2, I$, find a $\mathbb{Z}$-basis of J.*

Remark 4.2. *If* $\mathrm{Nrd}(I)$ *and* $\mathrm{Nrd}(J)$ *are coprime, then [6, Lem. 6] allows us to recover I more easily. However here we need to compute J, and the assumption that* $\mathrm{Nrd}(I)$ *and* $\mathrm{Nrd}(J)$ *are coprime is too strong for our setting: in theory (and in experiments), this hypothesis is not always satisfied. Therefore, we design a general algorithm which does not require any such assumption on the input.*

First we remark that Problem 4.1 is unambiguous.

Lemma 4.3. *The solution of Problem 4.1 is unique.*

Proof. Let J_1 and J_2 be two solutions of Problem 4.1. Then we have $I \cdot J_1 = I \cdot J_2$. By multiplying on the left by $\overline{I}$, we obtain that $\mathrm{Nrd}(I) \cdot \mathscr{O}_R(I) \cdot J_1 = \mathrm{Nrd}(I) \cdot \mathscr{O}_R(I) \cdot J_2$, see [17, Sec. 16.6]. Moreover $\mathscr{O}_R(I) = \mathscr{O}_L(J_1) = \mathscr{O}_L(J_2) = \mathscr{O}_2$, and J_1, J_2 are left-ideals in $\mathscr{O}_2$. Therefore, $\mathrm{Nrd}(I) \cdot J_1 = \mathrm{Nrd}(I) \cdot J_2$, which implies $J_1 = J_2$. □

We first address the special case where $\mu \in \mathbb{Z}$.

Problem 4.4 (Integer ideal division)**.** *Let $\mathscr{O}_1, \mathscr{O}_2, \subset \mathscr{B}_{p,\infty}$ be two maximal orders. Let $d \in \mathbb{Z}$, $I \in \mathrm{Conn}(\mathscr{O}_1, \mathscr{O}_2)$, and J a left $\mathscr{O}_2$-ideal be such that $\mathscr{O}_1 d = I \cdot J$. Given d and $\mathbb{Z}$-bases of $\mathscr{O}_1, \mathscr{O}_2, I$, find a $\mathbb{Z}$-basis of J.*

Remark 4.5. *The same argument as in the proof of Lemma 4.3 shows the unicity of the solution of Problem 4.4. Moreover we can swap the roles of I and J via conjugation since $I \cdot J = d\mathscr{O}_1 = \overline{J} \cdot \overline{I} = d\mathscr{O}_1$. It is easy to check that Problems 4.4 and 4.1 are equivalent: the solution J of Problem 4.1 with input $\mathscr{O}_1, \mathscr{O}_2, \mu, I$ equals the solution of Problem 4.1 with input $\mu^{-1}\mathscr{O}_1\mu$, $\mathscr{O}_2$, $\mathrm{Nrd}(\mu)$, $\overline{\mu}I$.*

Now we propose an efficient method to solve Problem 4.4.

Proposition 4.6. *With the same notation as in Problem 4.4, $J = \{s \in \mathscr{O}_1 \cap \mathscr{O}_2 : Is \subset \mathscr{O}_1 d\}$.*

Proof. Set $S := \{s \in \mathscr{O}_1 \cap \mathscr{O}_2 : Is \subset \mathscr{O}_1 d\}$. We must show that S is a left-ideal in $\mathscr{O}_2$ and that $IS = \mathscr{O}_1 d$.

First we show that S is a left-ideal of $\mathscr{O}_2$. Let $s \in S, x \in \mathscr{O}_2$. First, we notice that I is a right-ideal in $\mathscr{O}_2$, thus $Ix \subset I$. Since $s \in S$, we get $Ixs \subset Is \subset \mathscr{O}_1 d$, hence $xs \in S$.

Finally, we prove that $IS = \mathscr{O}_1 d$. Notice that $IS \subset \mathscr{O}_1 d$ by construction. In order to prove the other inclusion, we notice that J is included in S; hence, $\mathscr{O}_1 d = IJ \subset IS$. □

Proposition 4.6 reduces Problem 4.4 to $\mathbb{Z}$-linear algebra. Let $(e_0, \ldots, e_3)$, $(u_0, \ldots, u_3)$, $(v_0, \ldots, v_3)$ be $\mathbb{Z}$-bases of $\mathscr{O}_1, I, \mathscr{O}_1 \cap \mathscr{O}_2$ respectively. We need to solve the following system over the integers of 4 equations in 20 unknowns $\{x_i\}_{0\leq i\leq 3}$, $\{y_{ij}\}_{0\leq i,j\leq 3}$:

$$(E_j) : u_j \sum_{0\leq i\leq 3} x_i v_i = d \sum_{0\leq i\leq 3} y_{ij} e_i.$$

Let $b^{(1)}, \ldots, b^{(16)} \in \mathbb{Z}^{20}$ be a $\mathbb{Z}$-basis of the solutions of this system. Then, writing $b^{(i)} = (x_0^{(i)}, \ldots, x_3^{(i)}, y_{00}^{(i)}, \ldots, y_{33}^{(i)})$, we compute a basis $a^{(1)}, \ldots, a^{(3)}$ of the lattice generated by $\{(x_0^{(i)}, \ldots, x_3^{(i)})\}_{1\leq i\leq 16}$. Finally, writing $a^{(j)} = (a_0^{(j)}, \ldots, a_3^{(j)})$, the set $\{\sum_{0\leq i\leq 3} a_i^{(j)} v_i\}_{0\leq j\leq 3}$ is a $\mathbb{Z}$-basis for J.

Proposition 4.7. *With the same notation as in Problem 4.4, let γ be the maximum of the numerators and denominators of the coefficients of the elements in the bases of $\mathscr{O}_1, \mathscr{O}_2, I$, when written in the canonical basis $1, i, j, ij$ of $\mathscr{B}_{p,\infty}$. Then a $\mathbb{Z}$-basis of J (written in the basis $1, i, j, ij$) can be computed in quasi-linear complexity $\widetilde{O}(\log \gamma)$.*

Proof. A $\mathbb{Z}$-basis for J is obtained via linear algebra over the integers from the input $\mathbb{Z}$-bases. It can be computed via a sequence of Hermite Normal Forms of matrices with dimensions bounded above by a constant. Our proposition follows from the fact that the Hermite Normal Form of a nonzero matrix (A_{ij}) with integer entries can be computed with complexity quasi-linear in $\max_{ij}(\log|A_{ij}|)$, see [25, Chap. 6]. □

Remark 4.8. *The reduction in Remark 4.5 shows that Problem 4.1 can also be solved in quasi-linear complexity.*

4.2. An improvement of Kani's formula for the degree of isogenies between products of elliptic curves

The following statement is a slight improvement of Kani's formula [26, Cor. 63] for the degree of an isogeny between products of elliptic curves. This formula involves absolute values, and our improvement shows that they are in fact unnecessary. In the following statement, we use the convention that the zero morphism, that is not an isogeny, has degree 0.

Proposition 4.9. *Let E_1, E_2, E_1', E_2' be elliptic curves defined over $\overline{\mathbb{F}_p}$. For $i, j \in \{1, 2\}$, let $\varphi_{ij} \in \mathrm{Hom}(E_j, E_i')$ be a morphism of degree $d_{ij} \in \mathbb{Z}_{\geq 0}$. Let $\phi \in \mathrm{Hom}(E_1 \times E_2, E_1' \times E_2')$ be the morphism defined as $\phi(x_1, x_2) = (\varphi_{11}(x_1) + \varphi_{12}(x_2), \varphi_{21}(x_1) + \varphi_{22}(x_2))$. Then*

$$\deg(\phi) = (d_{11} + d_{21})(d_{12} + d_{22}) - \deg(\widehat{\varphi}_{12}\varphi_{11} + \widehat{\varphi}_{22}\varphi_{21}).$$

Proof. Set $\mu := \widehat{\varphi}_{12}\varphi_{11}$ and $\nu := \widehat{\varphi}_{22}\varphi_{21}$. [26, Cor. 64] states that $\deg(\phi) = |(d_{11} + d_{21})(d_{12} + d_{22}) - \deg(\mu + \nu)|$. Therefore, the only thing that we need to prove is that $\deg(\mu + \nu) \leq (d_{11} + d_{21})(d_{12} + d_{22})$, so that the absolute value is not required.

We start with the following computation:

$$\begin{aligned} 0 &\leq \deg(d_{21}\mu - d_{11}\nu) \\ &= (d_{21}\mu - d_{11}\nu)(d_{21}\widehat{\mu} - d_{11}\widehat{\nu}) \\ &= d_{21}^2 \deg(\mu) + d_{11}^2 \deg(\nu) - d_{11}d_{21}(\nu\widehat{\mu} + \mu\widehat{\nu}). \end{aligned}$$

Next, we notice that $\deg(\mu+\nu)-\deg(\mu)-\deg(\nu) = (\mu+\nu)(\widehat{\mu}+\widehat{\nu})-\deg(\mu)-\deg(\nu) = \nu\widehat{\mu}+\mu\widehat{\nu}$. Replacing $\nu\widehat{\mu}+\mu\widehat{\nu}$ in the previous inequality, we obtain

$$d_{21}^2 \deg(\mu) + d_{11}^2 \deg(\nu) \geq d_{11}d_{21}(\deg(\mu+\nu) - \deg(\mu) - \deg(\nu)).$$

Finally, we replace $\deg(\mu)$ and $\deg(\nu)$ by their respective values $d_{12}d_{11}$ and $d_{22}d_{21}$ to obtain

$$d_{21}^2 d_{12}d_{11} + d_{11}^2 d_{22}d_{21} \geq d_{11}d_{21}(\deg(\mu+\nu) - d_{12}d_{11} - d_{22}d_{21}).$$

By dividing this inequality by $d_{11}d_{21}$ and by rearranging terms, we obtain the desired inequality $\deg(\mu+\nu) \leq (d_{11}+d_{21})(d_{12}+d_{22})$. □

We shall use Proposition 4.9 in order to compute degrees of isogenies between products of elliptic curves. An important special case is that it can be used to check if such an isogeny has degree 1, i.e. if it is an isomorphism. More precisely, a 2-dimensional isogeny between products of elliptic curves can be given as a matrix of isogenies $(\varphi_{ij}) = \begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix}$. Such an isogeny is an isomorphism if and only if

$$(d_{11}+d_{21})(d_{12}+d_{22}) - \deg(\widehat{\varphi}_{12}\varphi_{11} + \widehat{\varphi}_{22}\varphi_{21}) = 1.$$

We can reformulate this statement to obtain the following necessary and sufficient condition:

Proposition 4.10. *Let E_1, E_2, E_1', E_2' be four elliptic curves defined over $\overline{\mathbb{F}_p}$, and $\varphi_{ij} : E_j \to E_i'$, $i,j \in \{1,2\}$ be four isogenies. Set $\mu = \widehat{\varphi}_{12}\varphi_{11}, \nu = \widehat{\varphi}_{22}\varphi_{21}$, and write $d_{ij} = \deg(\varphi_{ij})$. Then $\deg(d_{21}\mu - d_{11}\nu) = d_{11}d_{21}$ if and only if $\phi = (\varphi_{ij})_{i,j\in\{1,2\}} \in \mathrm{Hom}(E_1 \times E_2, E_1' \times E_2')$ is an isomorphism.*

Proof. By Proposition 4.9, we have $\deg(\mu+\nu) = (d_{11}+d_{21})(d_{12}+d_{22}) - \deg(\phi)$. Therefore, we obtain the equality

$$\deg(\mu+\nu) - \deg(\mu) - \deg(\nu) = \frac{d_{11}}{d_{21}}\deg(\nu) + \frac{d_{21}}{d_{11}}\deg(\mu) - \deg(\phi). \tag{4.1}$$

By multiplying (4.1) by $d_{11}d_{21}$, we obtain

$$\begin{aligned} & d_{11}d_{21}\deg(\phi) \\ = \; & d_{11}(d_{11}+d_{21})\deg(\nu) + d_{21}(d_{11}+d_{21})\deg(\mu) - d_{11}d_{21}\deg(\mu+\nu) \\ = \; & d_{11}^2\deg(\nu) + d_{21}^2\deg(\mu) - d_{11}d_{21}\,\mathrm{Trd}(\mu\widehat{\nu}) \\ = \; & \deg(d_{21}\mu - d_{11}\nu), \end{aligned}$$

hence $\deg(\phi) = 1$ if and only if $\deg(d_{21}\mu - d_{11}\nu) = d_{11}d_{21}$. □

4.3. Transposing isogenies

In this section, we show how an isogeny $\phi : E_1 \times E_2 \to E_1' \times E_2'$ can be transformed into a transposed isogeny $\widetilde{\phi} : E_1' \times E_2' \to E_1 \times E_2$ of the same degree. Since we have not fixed any polarization on the product surface, this transposed isogeny is not a dual of ϕ in the usual sense. In particular, the composed endomorphism $\widetilde{\phi}\cdot\phi$ need not be the multiplication by an integer. Still, the degree is preserved, i.e. $\deg(\phi) = \deg(\widetilde{\phi})$.

Corollary 4.11. *With the same notation as in Proposition 4.9, let* $\widetilde{\phi} \in \mathrm{Hom}(E_1' \times E_2', E_1 \times E_2)$ *denote the morphism defined as* $\widetilde{\phi}(x_1', x_2') = (\widehat{\varphi}_{11}(x_1') + \widehat{\varphi}_{21}(x_2'), \widehat{\varphi}_{12}(x_1') + \widehat{\varphi}_{22}(x_2'))$*, i.e. in matrix notation*

$$\widetilde{\phi} = \begin{bmatrix} \widehat{\varphi}_{11} & \widehat{\varphi}_{21} \\ \widehat{\varphi}_{12} & \widehat{\varphi}_{22} \end{bmatrix}.$$

Then $\deg(\phi) = \deg(\widetilde{\phi})$.

Proof. Set $d_{ij} = \deg(\varphi_{ij})$ and $\psi := \varphi_{21}\widehat{\varphi}_{11} + \varphi_{22}\widehat{\varphi}_{12}$, then

$$\phi\widetilde{\phi} = \begin{pmatrix} (d_{11} + d_{12}) & \widehat{\psi} \\ \psi & (d_{21} + d_{22}) \end{pmatrix}.$$

Applying Proposition 4.9 to the composed endomorphism $\phi\widetilde{\phi}$, we get

$$\deg(\phi)\deg(\widetilde{\phi}) = \deg(\phi\widetilde{\phi}) = ((d_{11} + d_{12})(d_{21} + d_{22}) - \deg(\psi))^2 = \deg(\widetilde{\phi})^2.$$

Therefore, $\deg(\phi) = \deg(\widetilde{\phi})$. $\square$

4.4. Localization

In this section, we investigate algorithmic aspects of the ring $\mathrm{M}_2(\mathbb{Z}_\ell)$ and of its left-ideals. This will be useful during the study of localizations of quaternion algebras: when $\mathscr{O}$ is a maximal order in a quaternion algebra over $\mathbb{Q}$ not ramified at ℓ, then $\mathscr{O} \otimes \mathbb{Z}_\ell$ is isomorphic to $\mathrm{M}_2(\mathbb{Z}_\ell)$. The first thing to notice is that $\mathrm{M}_2(\mathbb{Z}_\ell)$ is left-principal, and its left-ideals correspond to matrices in Hermite Normal Form.

Proposition 4.12. *[27, Chap. II, Thm. 2.3] The left-ideals in* $\mathrm{M}_2(\mathbb{Z}_\ell)$ *are the (all distinct) ideals of the form*

$$\mathrm{M}_2(\mathbb{Z}_\ell) \cdot \begin{pmatrix} \ell^n & r \\ 0 & \ell^m \end{pmatrix},$$

where $n, m \in \mathbb{Z}_{\geq 0}$ *are positive integers, and* $r \in \{0, \ldots, \ell^{m-1}\}$.

As $\mathrm{M}_2(\mathbb{Z}_\ell)$ is left-principal, we can define the *right-gcd* of matrices $A_1, A_2 \in \mathrm{M}_2(\mathbb{Z}_\ell)$ as the Hermite Normal Form of a generator of the ideal $\mathrm{M}_2(\mathbb{Z}_\ell) \cdot A_1 + \mathrm{M}_2(\mathbb{Z}_\ell) \cdot A_2$. We now consider the problem of computing this right-gcd, assuming that A_1 and A_2 are given in Hermite Normal Form.

Proposition 4.13. *Let* $A_1, A_2 \in \mathrm{M}_2(\mathbb{Z}_\ell)$ *be two matrices in Hermite Normal Form:*

$$A_i = \begin{pmatrix} \ell^{n_i} & r_i \\ 0 & \ell^{m_i} \end{pmatrix}, \quad i \in \{1, 2\}.$$

We assume without loss of generality that $n_2 \geq n_1$. *Set* $m = \min(m_1, m_2, \mathrm{val}_\ell(r_2 - \ell^{n_2 - n_1} r_1))$ *(with the convention that* $\mathrm{val}_\ell(0) = \infty$*). Then the* right-gcd *of* A_1 *and* A_2 *is*

$$\mathrm{rgcd}(A_1, A_2) = \begin{pmatrix} \ell^{n_1} & (r_1 \bmod \ell^m) \\ 0 & \ell^m \end{pmatrix}.$$

Proof. We have to prove that

$$\mathrm{M}_2(\mathbb{Z}_\ell)\cdot A_1 + \mathrm{M}_2(\mathbb{Z}_\ell)\cdot A_2 = \mathrm{M}_2(\mathbb{Z}_\ell)\cdot \begin{pmatrix} \ell^{n_1} & (r_1 \bmod \ell^m) \\ 0 & \ell^m \end{pmatrix}.$$

We notice that the left-ideal generated by a matrix correspond to the $\mathbb{Z}_\ell$-module generated by its rows.

First we prove the inclusion

$$\mathrm{M}_2(\mathbb{Z}_\ell)\cdot A_1 + \mathrm{M}_2(\mathbb{Z}_\ell)\cdot A_2 \supset \mathrm{M}_2(\mathbb{Z}_\ell)\cdot \begin{pmatrix} \ell^{n_1} & (r_1 \bmod \ell^m) \\ 0 & \ell^m \end{pmatrix}.$$

The vector $(0,\ell^m)$ clearly belongs to the $\mathbb{Z}_\ell$-module generated by the rows of A_1 and A_2 since $(0,\ell^{m_1}),(0,\ell^{m_2})$ and $(0, r_2 - \ell^{n_2-n_1}r_1)$ belongs to it. Hence, $(\ell^{n_1}, r_1 \bmod \ell^m)$ also lies in this $\mathbb{Z}_\ell$-module.

Let us now prove the other inclusion:

$$\mathrm{M}_2(\mathbb{Z}_\ell)\cdot A_1 + \mathrm{M}_2(\mathbb{Z}_\ell)\cdot A_2 \subset \mathrm{M}_2(\mathbb{Z}_\ell)\cdot \begin{pmatrix} \ell^{n_1} & (r_1 \bmod \ell^m) \\ 0 & \ell^m \end{pmatrix}.$$

The only non-trivial thing that we need to prove is that (ℓ^{n_2}, r_2) belongs to the $\mathbb{Z}_\ell$-module generated by (ℓ^{n_1}, r_1) and $(0,\ell^m)$. We notice that $\mathrm{val}_\ell(r_2 - \ell^{n_2-n_1}r_1) \geq m$, hence there exists $x \in \mathbb{Z}_\ell$ such that $r_2 - \ell^{n_2-n_1}r_1 = x\,\ell^m$. Therefore $(\ell^{n_2}, r_2) = \ell^{n_2-n_1}\cdot(\ell^{n_1}, r_1) + x\cdot(0,\ell^m)$, which concludes the proof. ☐

The main application of Proposition 4.13 shall appear in the following setting. Let $\mathscr{O} \subset \mathscr{B}_{p,\infty}$ be a maximal order, and $I \subset \mathscr{O}$ be a left-ideal given by a $\mathbb{Z}$-basis $b_1, b_2, b_3, b_4 \in \mathscr{O}$. Assume that we can compute an isomorphism $\phi : \mathscr{O}\otimes\mathbb{Z}_\ell \to \mathrm{M}_2(\mathbb{Z}_\ell)$. Then a generator of $I \otimes \mathbb{Z}_\ell$ is $\phi^{-1}(\mathrm{rgcd}(\phi(b_1), \phi(b_2), \phi(b_3), \phi(b_4)))$, so we can compute this generator by using Proposition 4.13.

5. Computing 2-dimensional isomorphisms

In this section, which contains our main algorithms, we start by noticing that the problem of finding automorphisms of surfaces is pretty easy to solve. Then, in the general case, we give a criterion for an isomorphism to exist, if we fixed two isogenies of its matrix representation. This criterion can be made effective, and it will then be used to compute (in polynomial time) isomorphisms between product of curves.

5.1. The case of automorphisms

Proposition 5.1. *Let E_1, E_2 be two elliptic curves defined over $\overline{\mathbb{F}_p}$, $\varphi : E_1 \to E_2$ be an isogeny, and $a,b,c,d \in \mathbb{Z}$ be integers such that $ad - bc\deg(\varphi) = \pm 1$. Then the endomorphism $F = \begin{pmatrix} a & b\widehat{\varphi} \\ c\varphi & d \end{pmatrix} \in \mathrm{End}(E_1 \times E_2)$ is an automorphism.*

Proof. By Proposition 4.9,

$$\begin{aligned} \deg(F) &= (a^2 + c^2\deg(\varphi))(b^2\deg(\varphi) + d^2) - \deg(b\varphi a + dc\varphi) \\ &= (a^2 + c^2\deg(\varphi))(b^2\deg(\varphi) + d^2) - (ba+dc)^2\deg(\varphi) \\ &= a^2d^2 + c^2b^2\deg(\varphi)^2 - 2abcd\deg(\varphi) \\ &= (ad - bc\deg(\varphi))^2 \\ &= 1. \end{aligned}$$

$\square$

Remark 5.2. *Direct computations show that the inverse of the automorphism* $F = \begin{pmatrix} a & b\widehat{\varphi} \\ c\varphi & d \end{pmatrix}$ *is* $F^{-1} = \begin{pmatrix} d & -b\widehat{\varphi} \\ -c\varphi & a \end{pmatrix}$.

Proposition 5.1 implies that if we are able to compute an isogeny $\varphi : E_1 \to E_2$, then the 2-dimensional morphism $\begin{pmatrix} 1+\deg(\varphi) & \widehat{\varphi} \\ \varphi & 1 \end{pmatrix}$ is an isomorphism. Thus knowing the endomorphism rings of E_1 and E_2 is enough to compute automorphisms of the surface $E_1 \times E_2$, thanks to [9, Algo. 5].

5.2. Completion of matrices of isogenies

In this section, we investigate the following question: given two isogenies $\varphi_{11}, \varphi_{21}$, can we compute isogenies $\varphi_{12}, \varphi_{22}$ such that the matrix (φ_{ij}) is an isomorphism. First, we give a necessary and sufficient criterion for the existence of such isogenies $\varphi_{12}, \varphi_{22}$. When this criterion is satisfied, we provide an algorithm to compute them. First we state a useful lemma.

Lemma 5.3. *Let F, E, E_1, E_2 be elliptic curves over $\overline{\mathbb{F}_p}$, $\psi : F \to E$ be a (non-necessarily separable) isogeny, and $\varphi_1 : E \to E_1$, $\varphi_2 : E \to E_2$ be separable isogenies of coprime degrees. Write $K := \ker(\varphi_1) \oplus \ker(\varphi_2)$. Then*

$$\deg(\varphi_2)\operatorname{Hom}(E_1, F)\varphi_1\psi + \deg(\varphi_1)\operatorname{Hom}(E_2, F)\varphi_2\psi = \operatorname{Hom}(E/K, F)\pi_K\psi.$$

where $\pi_K : E \to E/K$ is the canonical separable isogeny with kernel K.

Proof. Set $d_1 := \deg(\varphi_1)$, $d_2 := \deg(\varphi_2)$, $I_1 := d_2 \operatorname{Hom}(E_1, F)\varphi_1\psi$, $I_2 := d_1 \operatorname{Hom}(E_2, F)\varphi_2\psi$ and $I_K := \operatorname{Hom}(E/K, F)\pi_K\psi$. Direct computations show that

$$\begin{array}{rlcl} & \ker(d_2\varphi_1\psi) \cap \ker(d_1\varphi_2\psi) & = & \psi^{-1}(\ker(d_2\varphi_1)) \cap \psi^{-1}(\ker(d_1\varphi_2)) \\ = & \psi^{-1}\left(\ker(d_2\varphi_1) \cap \ker(d_2\varphi_1)\right) & = & \psi^{-1}\left((\ker\varphi_1 + E[d_2]) \cap (\ker\varphi_2 + E[d_1])\right) \\ = & \psi^{-1}(\ker\varphi_1 \oplus \ker\varphi_2) & = & \psi^{-1}(\ker(\pi_K)) \\ = & \ker(\pi_K\psi). & & \end{array}$$

Noticing that $I_1 + I_2 = I_{\ker(d_2\varphi_1\psi)\cap\ker(d_1\varphi_2\psi)}$ and $\operatorname{Hom}(E/K, F)\pi_K\psi = I_{\ker(\pi_K\psi)}$ concludes the proof. $\square$

We are now ready to state a key result of the paper.

Theorem 5.4. *Let E_1, E_2, E_1', E_2' be four isogenous elliptic curves defined over $\overline{\mathbb{F}_p}$, and $\varphi_{11} : E_1 \to E_1'$, $\varphi_{21} : E_1 \to E_2'$ be separable isogenies with coprime degrees. There exist isogenies $\varphi_{12} : E_2 \to E_1'$, $\varphi_{22} : E_2 \to E_2'$ such that $\phi = (\varphi_{ij})_{i,j\in\{1,2\}} \in \operatorname{Hom}(E_1 \times E_2, E_1' \times E_2')$ is an isomorphism if and only if $E_1/\left(\ker(\varphi_{11}) \oplus \ker(\varphi_{21})\right)$ and E_2 are isomorphic.*

Proof. Let $\psi : E_1 \to E_2$ be an isogeny. Let K denote the subgroup $\ker(\varphi_{11}) \oplus \ker(\varphi_{21})$ of E_1. Let $\pi_K : E_1 \to E_1/K$ be the associated canonical isogeny. Set $J_{11} := \operatorname{Hom}(E_1', E_2)\varphi_{11}\widehat{\psi}$, $J_{21} := \operatorname{Hom}(E_2', E_2)\varphi_{21}\widehat{\psi}$, and $J_K := \operatorname{Hom}(E_1/K, E_2)\pi_K\widehat{\psi}$, which are left-ideals in $\operatorname{End}(E_2)$.

By Proposition 4.10, there exist isogenies $\varphi_{12} : E_2 \to E_1'$, $\varphi_{22} : E_2 \to E_2'$ such that $\phi = (\varphi_{ij})_{i,j\in\{1,2\}} \in \mathrm{Hom}(E_1 \times E_2, E_1' \times E_2')$ is an isomorphism if and only if there exist isogenies $\mu, \nu : E_1 \to E_2$ which factors respectively by φ_{11} and φ_{21} and such that $\deg(d_{21}\mu - d_{11}\nu) = d_{11}d_{21}$, where $d_{11} = \deg(\varphi_{11})$ and $d_{21} = \deg(\varphi_{21})$. Equivalently, $\deg((d_{21}\mu - d_{11}\nu)\widehat{\psi}) = d_{11}d_{21}\deg(\psi)$, with $\mu\widehat{\psi} \in J_{11}, \nu\widehat{\psi} \in J_{21}$. Since Lemma 5.3 implies that $J_K = d_{21}J_{11} + d_{11}J_{21}$, it is equivalent to the existence of a $\sigma \in J_K$ such that $\deg(\sigma) = d_{11}d_{21}\deg(\psi)$. Remark that by definition, such a $\sigma \in J_K$ would factor as $\sigma = \tau\pi_K\widehat{\psi}$ for some $\tau \in \mathrm{Hom}(E_1/K, E_2)$. Thus the equation $\deg(\sigma) = d_{11}d_{21}\deg(\psi)$ is equivalent to $\deg(\tau)\deg(\pi_K)\deg(\psi) = d_{11}d_{21}\deg(\psi)$ by multiplicativity of the degree, which reduces to $\deg(\tau) = 1$, since $\deg(\pi_K) = d_{11}d_{21}$.

We conclude that there exist isogenies $\varphi_{12} : E_2 \to E_1'$, $\varphi_{22} : E_2 \to E_2'$ such that $\phi = (\varphi_{ij})_{i,j\in\{1,2\}} \in \mathrm{Hom}(E_1 \times E_2, E_1' \times E_2')$ is an isomorphism if and only if there exists $\tau \in \mathrm{Hom}(E_1/K, E_2)$ with $\deg(\tau) = 1$, *i.e.* if and only if E_1/K and E_2 are isomorphic. □

Theorem 5.4 is actually effective, provided that we know the endomorphism rings of the curves. Algorithm 1 computes such an isomorphism.

Proposition 5.5. *Assuming GRH, Algorithm 1 is correct and it runs in time polynomial in* $\log(p)$ *and in the size of the input.*

Proof. First we prove that Algorithm 1 is correct. In fact, Algorithm 1 follows the proof of Theorem 5.4. An isogeny associated to the ideal I_ψ plays the role of ψ in the proof of Theorem 5.4. The ideals I_{11}, I_{21} correspond to the isogenies $\varphi_{11}, \varphi_{21}$ in Theorem 5.4, and the ideals J_{11} and J_{21} play the same role as in the proof of Theorem 5.4. We now prove that the endomorphism ξ computed in Step 5 satisfies the requirements of σ in the proof of Theorem 5.4, namely that $\mathrm{Nrd}(\xi) = d_{11}d_{21}\mathrm{Nrd}(I_\psi)$. By the same argument as in the proof of Theorem 5.4, J_K is a principal left-ideal (because $E_1/K \simeq E_2$) of reduced norm $d_{11}d_{21}\mathrm{Nrd}(I_\psi)$, so it contains an element with this reduced norm; this proves that $\mathrm{Nrd}(\xi) = d_{11}d_{21}\mathrm{Nrd}(I_\psi)$. Theorem 5.4 also asserts that at least one of the matrices computed at Step 8 is an isomorphism.

Let us now prove that the complexity is polynomial with respect to the input size. Most steps reduce to linear algebra over $\mathbb{Z}$; this boils down to computing Hermite Normal Forms, which can be done in time polynomial in the input size. Step 5 involves computing the shortest vector in a lattice of dimension 4, with respect to the positive definite quadratic form $(x_1, x_2, x_3, x_4) \mapsto x_1^2 + x_2^2 + p(x_3^2 + x_4^2)$. This can be achieved in time polynomial in the input size and in $\log(p)$, see [28, Thm. 4.2.1]. The combinatorial factor in Step 8 does not increase the complexity since the number of possible isogenies $E \to E'$ that are represented by the same left-ideal in $\mathrm{End}(E)$ equals the order of $\mathrm{Aut}(E)$. For most elliptic curves, $\mathrm{Aut}(E) = \{1, -1\}$, and in any case $|\mathrm{Aut}(E)| \leq 24$ [23, Appendix A, Prop. 1.2.(c)]. Assuming GRH, converting the ideal representation to an efficient representation can be done in polynomial-time, see e.g. [22, Appendix C]. □

Experiments. Now we present the first part of our experimental results. Those are described in the file ExperimentResults_part1.mgm available at `https://gitlab.inria.fr/superspecial-surfaces-isomorphisms/experiments`. In this proof-of-concept implementation we illustrate Algorithm 1, *i.e* we compute an isomorphism $E_0 \times E \to E_1' \times E_2'$,

Algorithm 1: IsomorphismCompletion

Input: Four maximal curves E_1, E_1', E_2, E_2' over $\mathbb{F}_{p^2}$; $\mathbb{Z}$-bases of maximal orders $\mathscr{O}_1, \mathscr{O}_2 \subset \mathscr{B}_{p,\infty}$ and isomorphisms $\mathscr{O}_1 \cong \mathrm{End}(E_1)$, $\mathscr{O}_2 \cong \mathrm{End}(E_2)$; $\mathbb{Z}$-bases of left-ideals $I_{11}, I_{21} \subset \mathscr{O}_1$ of coprime degrees which correspond to isogenies $\varphi_{11} : E_1 \to E_1'$, $\varphi_{21} : E_1 \to E_2'$ such that $E_2 \cong E_1/\left(\ker(\varphi_{11}) \oplus \ker(\varphi_{21})\right)$.

Output: An efficient representation of a 2×2 matrix of isogenies (φ_{ij}) representing an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$ such that $\mathrm{Hom}(E_2, E_1)\varphi_{11} \cong I_{11}$ and $\mathrm{Hom}(E_2', E_1)\varphi_{21} \cong I_{21}$.

1 Compute $d \in \mathbb{Z}$ such that $d\mathscr{O}_1\mathscr{O}_2 \subset \mathscr{O}_1 \cap \mathscr{O}_2$ and set $I_\psi := d\mathscr{O}_1\mathscr{O}_2$, which is a connecting ideal between $\mathscr{O}_1$ and $\mathscr{O}_2$;
`// see [29, Algo. 3.5]`

2 Compute $\mathbb{Z}$-bases of $J_{11} := \overline{I}_\psi I_{11}$ and $J_{21} := \overline{I}_\psi I_{21}$;

3 Set $d_{11} := \mathrm{Nrd}(I_{11})$ and $d_{21} = \mathrm{Nrd}(I_{21})$;

4 Compute a $\mathbb{Z}$-basis of $J_K = d_{21}J_{11} + d_{11}J_{21}$;

5 Compute an element ξ in J_K whose reduced norm is minimal;
`// Lattice reduction in dimension` 4

6 Using linear algebra over $\mathbb{Z}$, compute $\xi_{11} \in J_{11}, \xi_{21} \in J_{21}$ such that $d_{21}\xi_{11} - d_{11}\xi_{21} = \xi$;

7 Compute left-ideals I_{12} and I_{22} in the right-orders of I_{11} and I_{21} respectively, such that $\overline{I}_\psi I_{11}\overline{I}_{12} = \mathscr{O}_2\xi_{11}$ and $\overline{I}_\psi I_{21}\overline{I}_{22} = \mathscr{O}_2\xi_{21}$;
`// Prop. 4.7 and Remark 4.8`

8 Compute efficient representations of all possible matrices (φ_{ij}) such that $\varphi_{ij} \in \mathrm{Hom}(E_j, E_i')$ and $\mathrm{Hom}(E_i', E_j)\varphi_{ij} \cong I_{ij}$ as $\mathrm{End}(E_j)$ left-modules;

9 Using Proposition 4.9, find a matrix among them which is an isomorphism and return it;

given isogenies $\varphi_{11} : E_0 \to E_1'$ and $\varphi_{21} : E_0 \to E_1'$ of coprime degree. Those isogenies are given by left $\mathscr{O}_0$-ideals, denoted I_{11} and I_{21} respectively.

First we let the user choose the following parameters: a lower bound for the prime p, and the norm of the two ideals I_{11} and I_{21}. Then we randomly compute such ideals, that determine (the isomorphism class of) E according to Theorem 5.4. We then recover the corresponding order $\mathscr{O} \simeq \operatorname{End}(E)$ as the right order of the left $\mathscr{O}_0$-ideal $I_K := d_{11}I_{21} + d_{21}I_{11}$, by application of Lemma 5.3. We conclude by computing the ideals I_{12} and I_{22}, with a call to Algorithm 1. We can finally check that the ideals I_{ij} represent an isomorphism, thanks to the following lemma.

Lemma 5.6. *Let E_1, E_2, E_1', E_2' be elliptic curves defined over $\overline{\mathbb{F}_p}$. For $i, j \in \{1, 2\}$, let $\varphi_{ij} \in \operatorname{Hom}(E_j, E_i')$ be a morphism of degree $d_{ij} \in \mathbb{Z}_{\geq 0}$. Denote $\Phi : E_1 \times E_2 \to E_1' \times E_2'$ the 2-dimensional morphism given by the matrix $(\varphi_{ij})_{ij}$. Let $\psi : E_2 \to E_1$ be a nonzero morphism. Then*

$$\deg \begin{pmatrix} \varphi_{11} \circ \psi & \varphi_{12} \\ \varphi_{21} \circ \psi & \varphi_{22} \end{pmatrix} = \deg(\psi) \deg(\Phi).$$

Proof. This is a direct consequence of Proposition 4.9. □

Example 5.7. *We report on experimental results obtained by running `Magma` version V2.28-3 with seed 12345 on the file ExperimentResults_part1.mgm. In this example, $p = 503$ and $\ell_{11} = 3$, $m_{11} = 6$ and $\ell_{21} = 5$, $m_{21} = 4$. We denote by i_q, j_q, k_q the usual generators of $\mathscr{B}_{p,\infty}$. The input ideals are $I_{11} = \langle 729,\ 729\, i_q, 603/2 + 652\ i_q + k_q/2,\ 652 + 855\, i_q/2 + j_q/2 \rangle$ of norm $\ell_{11}^{m_{11}}$, and $I_{21} = \langle 625,\ 625\, i_q,\ 759/2 + 527\, i_q + k_q/2,\ 527 + 491\, i_q/2 + j_q/2 \rangle$ of norm $\ell_{21}^{m_{21}}$. Then IsomorphismCompletion returns*

$$\begin{aligned}
I_{12} = \langle & 3196396279123748125/2 - 2330172887481212383125\, k_q/2, \\
& 511423404659799700 - 127855851164949925\, i_q/1458 - 300461250237632323 75\, j_q/486 \\
& \quad - 2899534171096409141638 75\, k_q/729, \\
& 11442125762113937/2 - 9726906334344569\, i_q/243 - 2285822988570975740\, j_q/81 \\
& \quad - 755380533918112010241 5\, k_q/486, \\
& 386746255666051731/2 - 9746968804698626\, i_q/729 - 2290537669104179054\, j_q/243 \\
& \quad - 211071083520127178104733\, k_q/1458 \rangle. \\
I_{22} = \langle & 57091554482520078 - 35682221551575048750\, k_q, \\
& 19030518160840026 - 38061036321680052\, i_q/625 - 2767037340586139780 4\, j_q/625 \\
& \quad - 2601892407038186118774 6\, k_q/625, \\
& 30532858451621568 - 4151933667041628\, i_q/625 - 3018455775939278556\, j_q/625 \\
& \quad - 1395427873841377463414 4\, k_q/625, \\
& 43446906184660068 - 31874160047168274\, i_q/625 - 23172514354291335198\, j_q/625 \\
& \quad - 3253553633109502698265 2\, k_q/625 \rangle.
\end{aligned}$$

Then using Lemma 5.6, we check that the four ideals I_{ij} represent an isomorphism.

5.3. *Computing isomorphisms $E_0^2 \to E_1' \times E_0$*

In this section, we focus on a special 2-dimensional instance of Problem 1.1: we assume that the endomorphism rings of all curves are known, and that we also know subrings of $\operatorname{End}(E_1)$ and $\operatorname{End}(E_1')$ which are isomorphic to a low-discriminant imaginary quadratic order. In this case, we provide a fast algorithm to compute the corresponding isomorphism, described in Algorithm 3. In order to simplify the exposition, we assume that $E_1 = E_2 = E_2'$. In fact, this assumption does not lose any generality, see Remark 5.17.

Also, for the sake of simplicity, we assume throughout this section that the curve for which we know a subring of endomorphisms isomorphic to a low-discriminant imaginary quadratic order is the curve E_0 defined over $\mathbb{F}_{p^2}$ (with $p \equiv 3 \bmod 4$) by the equation $y^2 = x^3 + x$. Its endomorphism ring contains a subring isomorphic to $\mathbb{Z}[i]$. However, all the results presented in this section can be generalized without any major difficulty to other curves. In particular, when $p \equiv 1 \bmod 4$, a curve with a low-discriminant can also be explicitly computed, see [18, Sec. 3.1].

In summary, our objective in this section is to provide a fast algorithm for the following problem:

Problem 5.8 (Low-discriminant Deligne-Ogus-Shioda problem)**.** *Given a maximal supersingular elliptic curve E_1' defined over $\mathbb{F}_{p^2}$ and its endomorphism ring, compute an $\mathbb{F}_{p^2}$-isomorphism $E_0 \times E_0 \to E_1' \times E_0$.*

The following statement gives sufficient conditions to use the strategy of Theorem 5.4.

Proposition 5.9. *Let E, E_1' be elliptic curves defined over $\overline{\mathbb{F}_p}$ and let $\varphi : E \to E_1'$ be a separable isogeny. Let $\alpha, \nu \in \mathrm{End}(E)$ be endomorphisms of coprime degrees such that $\deg(\alpha) = \deg(\varphi)$ and $\alpha\nu \in \mathrm{Hom}(E_1', E)\varphi$. Then $\ker(\nu) \oplus \ker(\varphi)$ is the kernel of the endomorphism $\alpha\nu : E \to E$.*

Proof. Since $\alpha\nu \in \mathrm{Hom}(E_1', E)\varphi$, we have $\ker(\varphi) \subset \ker(\alpha\nu)$. Consequently, $\ker(\varphi) + \ker(\nu) \subset \ker(\alpha\nu)$. The co-primality of the degrees of ν and φ implies that the intersection of the kernels is trivial. Since α and ν are separable, so is $\alpha\nu$ and therefore $|\ker(\alpha\nu)| = \deg(\alpha)\deg(\nu) = \deg(\varphi)\deg(\nu) = |\ker(\varphi) \oplus \ker(\nu)|$, which shows that the inclusion is in fact an equality. □

Proposition 5.9 tells us that if are able to compute φ, α and ν, then Algorithm 1 can compute an isomorphism $E \times E \to E_1' \times E$. Our strategy will be to first fix φ, then to compute the endomorphisms α and ν that satisfy the conditions of Proposition 5.9. As explained above, we specialize to the case $E = E_0$, and $p \equiv 3 \bmod 4$, to perform those computations. The low-discriminant quadratic order will help us find the endomorphism $\alpha \in \mathrm{End}(E_0)$ of prescribed degree $\deg(\alpha) = \deg(\varphi)$ by solving low-discriminant norm equations with Cornacchia's algorithm. Algorithm 2 provides a fast method for computing such α, ν upon input of the ideal I corresponding to the isogeny φ.

We start with a few technical lemmas which state that computing α, ν in Proposition 5.9 is actually related to computing a generator of a localization of the ideal I associated to φ at a prime ℓ.

Lemma 5.10. *Let $\mathscr{O} \subset \mathscr{B}_{p,\infty}$ be a maximal order, $I \subset \mathscr{O}$ be a left ideal, $\alpha \in \mathscr{O}$ such that $\mathrm{Nrd}(\alpha) = \mathrm{Nrd}(I)$, and $\ell \neq p$ be a prime number. Then the following statements are equivalent:*

(a) There exists $x \in \mathscr{O}$, such that $\alpha x \in I$ and $\mathrm{Nrd}(x)$ is not divisible by ℓ;

(b) There exists an invertible $y \in \mathscr{O} \otimes \mathbb{Z}_\ell$ such that $\alpha y \in I \otimes \mathbb{Z}_\ell$.

Proof. First, we notice that all elements $x \in \mathscr{O}$ with reduced norm not divisible by ℓ are invertible in $\mathscr{O} \otimes \mathbb{Z}_\ell$; Indeed, $x \cdot (\overline{x}/\mathrm{Nrd}(x)) = 1$, hence the inverse of x in $\mathscr{O} \otimes \mathbb{Z}_\ell$ is $x/\mathrm{Nrd}(x)$. This proves the implication *(a)⇒(b)*.

We now prove *(b)⇒(a)*. Let y be as in *(b)*. Let $b_1, \dots, b_4$ be generators of I seen as a free rank-4 $\mathbb{Z}$-module. Then $\alpha y = z_1 \cdot b_1 + \cdots + z_4 \cdot b_4$, with $z_1, \dots, z_4 \in \mathbb{Z}_\ell$. Next, pick integers $z'_1, \dots, z'_4 \in \mathbb{Z}$ such that $z'_i \equiv z_i \bmod \ell^e$, where e is the ℓ-valuation of $\mathrm{Nrd}(\alpha)$. Then set $y' = \alpha^{-1}(z'_1 \cdot b_1 + \cdots + z'_4 \cdot b_4) \in \mathscr{B}_{p,\infty}$. We prove now that $x := \mathrm{Nrd}(\alpha)y'/\ell^e$ satisfies the desired properties. First, we show that $x = \ell^{-e}\overline{\alpha}(z'_1 \cdot b_1 + \cdots + z'_4 \cdot b_4)$ belongs to $\mathscr{O}$. Notice that x clearly belongs to localized orders $\mathscr{O} \otimes \mathbb{Z}_{\ell'}$ for primes $\ell' \neq \ell$, so we only have to prove that $x \in \mathscr{O} \otimes \mathbb{Z}_\ell$. To do so, we use the fact that $z_i \equiv z'_i \bmod \ell^e$, hence there exists $z''_1, \dots, z''_4 \in \mathbb{Z}_\ell$ such that $z_i = z'_i + \ell^e z''_i$, which gives

$$\begin{aligned} x &= \ell^{-e}\overline{\alpha}(z_1 \cdot b_1 + \cdots + z_4 \cdot b_4) - \overline{\alpha}(z''_1 \cdot b_1 + \cdots + z''_4 \cdot b_4) \\ &= y\,\mathrm{Nrd}(\alpha)/\ell^e - \overline{\alpha}(z''_1 \cdot b_1 + \cdots + z''_4 \cdot b_4), \end{aligned}$$

which shows that $x \in \mathscr{O} \otimes \mathbb{Z}_\ell$. Then we notice that $\mathrm{Nrd}(x) = (\mathrm{Nrd}(\alpha)/\ell^e)^2\,\mathrm{Nrd}(y')$ is not divisible by ℓ since $\mathrm{Nrd}(y') \equiv \mathrm{Nrd}(y) \not\equiv 0 \bmod \ell$. Finally, since $\mathrm{Nrd}(\alpha) = \mathrm{Nrd}(I) \in I$, we notice that $\alpha x = \mathrm{Nrd}(\alpha)(z'_1 \cdot b_1 + \cdots + z'_4 \cdot b_4)$ belongs to I, which concludes the proof. □

Definition-Proposition 5.11. *Let $M \in \mathrm{M}_2(\mathbb{Z}_\ell)$ be a matrix. We say that the ℓ-type of M is the pair of valuations (in $\mathbb{Z}^2_{\geq 0}$) of the invariant factors of M, sorted in non-decreasing order. More explicitly, using the* Smith Normal Form*, this means that M has ℓ-type (d_1, d_2) if $d_1 \leq d_2$ and if there exist invertible matrices $S, T \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ such that*

$$S \cdot M \cdot T = \begin{pmatrix} \ell^{d_1} & 0 \\ 0 & \ell^{d_2} \end{pmatrix}.$$

Since $\mathrm{M}_2(\mathbb{Z}_\ell)$ is left-principal, we define the ℓ-type of a left-ideal $I \subset \mathrm{M}_2(\mathbb{Z}_\ell)$ as the ℓ-type of a generator.

Let $I \subset \mathscr{O}$ be a left-ideal of a maximal order in $\mathscr{B}_{p,\infty}$, and $\ell \neq p$ be a prime number. By [27, Cor. I.2.4], $\mathscr{O} \otimes \mathbb{Z}_\ell$ is isomorphic to $\mathrm{M}_2(\mathbb{Z}_\ell)$, so we define the ℓ-type of I as the ℓ-type of $I \otimes \mathbb{Z}_\ell$ regarded as an ideal in $\mathrm{M}_2(\mathbb{Z}_\ell)$; this definition does not depend on the choice of the isomorphism $\mathscr{O} \otimes \mathbb{Z}_\ell \cong \mathrm{M}_2(\mathbb{Z}_\ell)$. If $\alpha \in \mathscr{O}$ is an element in a maximal order, its ℓ-type is defined as the ℓ-type of the left-ideal $\mathscr{O}\alpha$.

Proof. The only thing that we need to prove is that the definition of the ℓ-type of a left ideal $I \subset \mathscr{O} \otimes \mathbb{Z}_\ell \cong \mathrm{M}_2(\mathbb{Z}_\ell)$ does not depend on the choice of the isomorphism. In fact, this is a consequence of the fact that automorphisms of $\mathrm{M}_2(\mathbb{Z}_\ell)$ preserve the ℓ-type of matrices in $\mathrm{M}_2(\mathbb{Z}_\ell)$, which can be seen on the Smith Normal Form since automorphisms act as conjugations by invertible matrices. □

Lemma 5.12. *With the same notation as in Lemma 5.10, the ℓ-types of I and α are the same if and only if there exists an invertible $y \in \mathscr{O} \otimes \mathbb{Z}_\ell$ such that $\alpha y \in I \otimes \mathbb{Z}_\ell$.*

Proof. In this proof, we fix an isomorphism $\mathscr{O} \otimes \mathbb{Z}_\ell \cong \mathrm{M}_2(\mathbb{Z}_\ell)$ and we use it implicitly. Let $\beta \in \mathrm{M}_2(\mathbb{Z}_\ell)$ be a generator of $I \otimes \mathbb{Z}_\ell$.

To prove the "only if" part of the statement, we notice that if the matrices α and β have the same invariant factors then there exist invertible matrices $U, V \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ such that $U \cdot \beta = \alpha \cdot V$. This implies that $\alpha \cdot V$ belongs to the left-ideal generated by β. Writing $y \in (\mathscr{O} \otimes \mathbb{Z}_\ell)^\times$ for the element corresponding to the matrix $V \in \mathrm{GL}_2(\mathbb{Z}_\ell)$, we obtain that $\alpha y \in I \otimes \mathbb{Z}_\ell$.

We now prove the "if" part of the statement. Under the fixed isomorphism, the assumption $\alpha y \in I \otimes \mathbb{Z}_\ell$ translates to the existence of $U \in \mathrm{M}_2(\mathbb{Z}_\ell)$ such that $\alpha y = U\beta$. By the multiplicativity of the determinant, we deduce that $U \in \mathrm{GL}_2(\mathbb{Z}_\ell)$. Therefore $\beta = U^{-1}\alpha y$ and hence β and α have the same invariant factors. $\square$

Lemma 5.13. *With the same notation as in Lemma 5.10, if $\alpha \in \mathscr{O}$ has ℓ-type (i, j), then there exists $\alpha' \in \mathscr{O}$ with ℓ-type $(0, j-i)$ such that $\alpha = \ell^i \alpha'$. Similarly, if $I \subset \mathscr{O}$ is a left-ideal which has ℓ-type (i, j), there exists a left-ideal $I' \subset \mathscr{O}$ with ℓ-type $(0, j-i)$ and $I = \ell^i \cdot I'$.*

Proof. Using 5.11, we just need to prove this property for matrices in $\mathrm{M}_2(\mathbb{Z}_\ell)$. Let $M \in \mathrm{M}_2(\mathbb{Z}_\ell)$ be a matrix with ℓ-type (i, j), i.e. there exists $S, T \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ such that

$$S \cdot M \cdot T = \begin{pmatrix} \ell^i & 0 \\ 0 & \ell^j \end{pmatrix}.$$

Then set $M' = S^{-1} \cdot \begin{pmatrix} 1 & 0 \\ 0 & \ell^{j-i} \end{pmatrix} \cdot T^{-1}$. By construction, M' has ℓ-type $(0, j-i)$ and $M = \ell^i M'$. $\square$

We are now ready to prove the main algorithmic result of this section. It will relies on the fact that we can efficiently solve norm equations in $\mathscr{O}_0$, if we assume that the norm to reach is big enough.

Algorithm 2: LocalGenerator

Input: A prime ℓ, a left ideal $I \subset \mathscr{O}_0$ not divisible by ℓ, with reduced norm $\mathrm{Nrd}(I) = \ell^m$.

Output: Returns elements $\alpha, x \in \mathscr{O}_0$ such that $\mathrm{Nrd}(\alpha) = \ell^m$ and αx generates $I \otimes \mathbb{Z}_\ell$.

1 Check that $m \log(\ell) > \log(p)^c$ and compute $\alpha \in \mathscr{O}_0$ such that $\mathrm{Nrd}(\alpha) = \ell^m$;
`// Use [9, Corollary 5.8]; the constant` c `is the one of this reference.`
2 Using the isomorphism $\phi : \mathscr{O}_0 \otimes \mathbb{Z}_\ell \to \mathrm{M}_2(\mathbb{Z}_\ell)$, compute $M_\alpha := \phi(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 ij) \bmod \mathbb{Z}/\ell^m\mathbb{Z} \in \mathrm{M}_2(\mathbb{Z}/\ell^m\mathbb{Z})$;
3 Compute a generator $\beta \in \mathscr{O} \otimes \mathbb{Z}/\ell^m\mathbb{Z}$ of $I \otimes \mathbb{Z}/\ell^m\mathbb{Z}$;
`// This is done by computing the right-gcds of the four generators of` $I \otimes \mathbb{Z}/\ell^m\mathbb{Z} \cong \mathrm{M}_2(\mathbb{Z}/\ell^m\mathbb{Z})$`, see Proposition 4.13`
4 Set $M_\beta := \phi(\beta) \in \mathrm{M}_2(\mathbb{Z}/\ell^m\mathbb{Z})$;
5 Using the Smith Normal Form, compute two matrices $S, T \in \mathrm{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z})$ such that $S \cdot M_\alpha \cdot T = M_\beta$;
6 By lifting coordinates from $\mathbb{Z}/\ell^m\mathbb{Z}$ to representatives in $\mathbb{Z}$, set x an element of $\mathscr{O}$ such that $x \equiv \phi^{-1}(T) \bmod \mathbb{Z}/\ell^m\mathbb{Z}$;
7 Return $(\alpha, x) \in \mathscr{O}_0^2$;

Theorem 5.14. *Assuming GRH, there exists a constant $c > 0$ such that on input an ideal I with $\log(\mathrm{Nrd}(I)) > \log(p)^c$, Algorithm 2 is correct and terminates in expected polynomial time in $\log(p)$ and $\log(\mathrm{Nrd}(I))$.*

Proof. Let c be the constant given by [9, Corollary 5.8], so that the corresponding algorithm can be run on input $\mathrm{Nrd}(I)$. In [9], the algorithm is proved to be correct and polynomial time under GRH. Therefore α can be correctly computed at Step 1.

Hence the correctness of Algorithm 2 is a direct consequence of Lemma 5.13 (to prove that the ℓ-types of I and α are the same) and of the proof of Lemma 5.12 which explains how to construct x.

The complexity is a consequence of the polynomial time computation of α, and of the fact that computing the Hermite Normal Forms (for computing the generator of $I \otimes \mathbb{Z}/\ell^m\mathbb{Z}$) and Smith Normal Forms of matrices in $\mathrm{M}_2(\mathbb{Z}/\ell^m\mathbb{Z})$ can be done in quasi-linear complexity $\widetilde{O}(m\log(\ell))$ [25, Chap. 8]. □

Finally, we put all the pieces together and we give a complete algorithm (Algorithm 3) to compute an isomorphism $E_0^2 \to E_1 \times E_0$ upon input of E_1 and its endomorphism ring. In the following, c_0 will denote the constant given by Theorem 5.14.

Algorithm 3: LowDiscriminantIsomorphism

Input: A maximal elliptic curve E_1' defined over $\mathbb{F}_{p^2}$, a maximal order $\mathscr{O}_1'$ together with an isomorphism $\mathscr{O}_1' \cong \mathrm{End}(E_1')$, a prime $\ell \neq p$.

Output: Returns an efficient representation of an isomorphism $E_0^2 \to E_1' \times E_0$.

1 Compute a left $\mathscr{O}_0$-ideal I_{11} with norm ℓ^m for some $m \in \mathbb{Z}_{\geq 0}$ such that its right-order is conjugated to $\mathscr{O}_1'$ and that $m\log(\ell) > \log(p)^{c_0}$;
`// use KLPT [10] or [9, Algo. 5]`

2 Set $\alpha, \nu_1 := \textsc{LocalGenerator}_{c_0}(\ell, I_{11})$;

3 Return $\textsc{IsomorphismCompletion}(E_0, E_1', E_0, E_0, \mathscr{O}_0, \mathscr{O}_1, I_{11}, \mathscr{O}_0\nu_1)$;

Theorem 5.15. *Algorithm 3 is correct and, under GRH, it requires an expected number of operations which is polynomial in* $\log(p)$.

Proof. The correctness is a direct consequence of Theorem 5.4 and Proposition 5.9, together with the correctness of the subroutines, see Theorem 5.14 and Proposition 5.5. The complexity also follows from the complexities of the subroutines (Theorem 5.14 and Proposition 5.5), together with the fact that the output size of Wesolowski's algorithm [9, Algo. 5] is polynomial in $\log(p)$. □

The following corollary shows that by running twice Algorithm 3, we can compute isomorphisms $E_1 \times E_0 \to E_2 \times E_0$.

Corollary 5.16. *Let E_1, E_2 be two maximal elliptic curves defined over $\mathbb{F}_{p^2}$, with known endomorphism rings $\mathscr{O}_1 \cong \mathrm{End}(E_1)$ and $\mathscr{O}_2 \cong \mathrm{End}(E_2)$. Assuming GRH we can compute an efficient representation of an $\mathbb{F}_{p^2}$-isomorphism from $E_1 \times E_0$ to $E_2 \times E_0$ with a Las Vegas probabilistic algorithm running in expected polynomial time.*

Proof. Running twice Algorithm 3 provides us with efficient representations of two isomorphisms $\xi_1 : E_0^2 \to E_1 \times E_0$ and $\xi_2 : E_0^2 \to E_2 \times E_0$. By transposing ξ_2 as in Section 4.3, we get an efficient representation of an isomorphism $\xi_2' : E_2 \times E_0 \to E_0^2$. Finally, computing a efficient representation of $\xi_1 \circ \xi_2'$ provides the desired isomorphism. □

Remark 5.17. *In fact, all results in this section generalize if we replace E_0 by an elliptic curve E for which we know a subring of $\mathrm{End}(E)$ isomorphic to a low-discriminant imaginary quadratic order. Corollary 5.16 can actually be generalized as follows: given E_1, E_2, E_1', E_2' supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ with their endomorphism rings, and given low-discriminant endomorphisms in $\mathrm{End}(E_1)$ and $\mathrm{End}(E_1')$, we can efficiently compute an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$ by computing isomorphisms $E_1 \times E_2 \to E_1^2$, $E_1^2 \to E_1 \times E_1'$, $E_1 \times E_1' \to (E_1')^2$, and $(E_1')^2 \to E_1' \times E_2'$. Each isomorphism can be computed by using the low-discriminant technique described in this section.*

Experiments. Let us describe an implementation of instances of Algorithm 3 we propose in the file ExperimentResults_part2.mgm available at `https://gitlab.inria.fr/superspecial-surfaces-isomorphisms/experiments`. As in the previous experiment paragraph, the user can choose the parameters p, ℓ and m. Then we build a random ideal I_{11} such that $\mathrm{Nrd}(I_{11}) = \ell^m$. Next we recover α and ν_1 with the function LocalGenerator, where we compute α thanks to Cornacchia's algorithm. Those computations allow us to set $I_{21} := \mathscr{O}_0 \nu_1$. Finally, as described in Algorithm 3, we recover the two last ideals I_{12} and I_{22} by a call to IsomorphismCompletion. The function RepresentIsomorphism ensures us that the computed ideals represent an isomorphism.

Example 5.18. *We report on experimental results obtained by running* `Magma` *version V2.28-3 with seed* 12345 *on the file* ExperimentResults_part2.mgm. *In this example, $p = 103$, $\ell = 3$, $m = 5$. We choose a prime smaller than in previous experiments, so that the coefficients of the basis fit in one page. We denote by i_q, j_q, k_q the usual generators of $\mathscr{B}_{p,\infty}$. The input ideal I_{11} has norm ℓ^m and is given by the basis: $\langle 243, 243\, i_q, 61/2 + 4\, i_q + k_q/2, 4 + 425\, i_q/2 + j_q/2\rangle$. Computations give $\alpha = 6 + i_q + j_q - k_q$, and $\nu_1 = 1075/2 + 1577\, i_q + 244\, j_q + 625\, k_q/2$. We set $I_{21} := \mathscr{O}_0 \nu_1$. Then the function* IsomorphismCompletion *returns the ideals:*

$$
\begin{aligned}
I_{12} =& \langle 27765012061574622102876796822 79/2 - 67468979309626331709990616279 3797/2\, k_q, \\
& - 2776501206157462210287679682279/243\, i_q - 1285520058450905003363195692895177/243\, j_q \\
& \quad - 31779832805678312458952781643 3654340/243\, k_q, \\
& 41028316571489821819779875437 9 - 3374039621204859851194289602 9/486\, i_q \\
& \quad - 15621803446178501111029560861913/486\, j_q - 261577735275145661792003105870744 75/243\, k_q, \\
& 10674275265076830057879907202 83/2 - 98953672687555676747083214852 5/243\, i_q \\
& \quad - 458155504543382783338995284767075/243\, j_q - 2895552755291046290181979594825700 63/486\, k_q\rangle.
\end{aligned}
$$

$$
\begin{aligned}
I_{22} =& \langle 4627639113435172228906591486 5/2 - 87770751231526734698152227631 7359005/2\, k_q, \\
& - 15425463711450574096355304955/37933274\, i_q - 3214191687438624078504018772782 43555/37933274\, j_q \\
& \quad - 48835330545288251675472404924651 80139329460/18966637\, k_q, \\
& 41759783165084856705939206451/2 - 74483148464488136463672586 82/18966637\, i_q \\
& \quad - 155199948038581060493609428604527415/18966637\, j_q \\
& \quad - 24454605381976538232598154967499148986000315/37933274\, k_q, \\
& 15145446823711167882959064733 - 14521079224050332265634834729/37933274\, i_q \\
& \quad - 302574580626278073443494629377735133/37933274\, j_q \\
& \quad - 100455366748893602912121729741692324481158 92/18966637\, k_q\rangle
\end{aligned}
$$

We finally check that RepresentIsomorphism *returns* TRUE *on those inputs.*

5.4. Computing an isomorphism in the general case

For simplicity, we focus on the case $p \equiv 3 \bmod 4$ where we can use the curve E_0 defined over $\mathbb{F}_{p^2}$ by the equation $y^2 = x^3 + x$ which admits a low-discriminant endomorphism. If

$p \equiv 1 \bmod 4$, we can use instead the construction described in [18, Sec. 3.1].

First we provide an algorithm to solve a special case of Theorem 3.2.

Algorithm 4: IsomorphismE0

Input: Two maximal elliptic curves E_1, E_2 defined over $\mathbb{F}_{p^2}$, maximal orders $\mathscr{O}_1, \mathscr{O}_2$ together with isomorphisms $\mathscr{O}_1 \cong \mathrm{End}(E_1)$, $\mathscr{O}_2 \cong \mathrm{End}(E_2)$

Output: Returns an efficient representation of an isomorphism $E_0^2 \to E_1 \times E_2$.

1 Compute isogenies $\varphi_1 : E_0 \to E_1$ and $\varphi_2 : E_0 \to E_2$ of coprime degree, and their ideals I_1, I_2 ;
`// use KLPT [10] or [9, Algo. 5]`

2 Set $I_K := \deg(\varphi_1) I_2 + \deg(\varphi_2) I_1$, and compute its right order $\mathscr{O}_3$ along with an elliptic curve E_3 such that $\mathrm{End}(E_3) \cong \mathscr{O}_3$;
`// Lemma 5.3 ensures that` $E_3 \simeq E_0/(\ker(\varphi_1) \oplus \ker(\varphi_2))$

3 Compute an isomorphism $F : E_0 \times E_3 \to E_1 \times E_2$ by running IsomorphismCompletion$(E_0, E_3, E_1, E_2, \mathscr{O}_0, \mathscr{O}_3, I_1, I_2)$;

4 Choose a prime $\ell \neq p$, and compute an isomorphism $G : E_0^2 \to E_0 \times E_3$ by running LowDiscriminantIsomorphism$(E_3, \mathscr{O}_3, \ell)$, and post-composing by the isomorphism $(P, Q) \mapsto (Q, P)$;

5 Return the composition $F \circ G : E_0^2 \to E_1 \times E_2$;

Theorem 5.19. *Algorithm 4 is correct and assuming GRH it requires an expected number of operations which is polynomial in* $\log(p)$.

Proof. First we prove that the algorithm is correct. Since we know the endomorphism rings of E_0, E_1, E_2 we can compute the isogenies $\varphi_i : E_0 \to E_i$ of coprime degree by [9, Algo. 5]. Applying Lemma 5.3 with $\psi = Id_{E_0}$ leads to the construction of the ideal I_K representing an isogeny $E_0 \to E_0/(\ker(\varphi_1) \oplus \ker(\varphi_2))$. The correctness is then a consequence of Proposition 5.5 and Theorem 5.15.

The complexity follows from the same results, using the fact that [9, Algo. 5] requires polynomial time assuming GRH, and that constructing I_K is standard $\mathbb{Z}$-linear algebra. □

We finally present a proof of Theorem 3.2.

Proof of Theorem 3.2. By two calls to Algorithm 4, we compute two isomorphisms $\Phi : E_1 \times E_2 \to E_0^2$ and $\Psi : E_1' \times E_2' \to E_0^2$. Then by Corollary 4.11 we compute the tranposed isomorphism $\widetilde{\Psi} : E_0^2 \to E_1' \times E_2'$. Computing the composition $\widetilde{\Psi} \circ \Phi$ leads to the desired isomorphism $E_1 \times E_2 \to E_1' \times E_2'$. □

References

[1] D. Lubicz, D. Robert, Computing isogenies between abelian varieties, Compositio Mathematica 148 (5) (2012) 1483–1515. `doi:10.1112/s0010437x12000243`.
URL `http://dx.doi.org/10.1112/S0010437X12000243`

[2] P. Dartois, L. Maino, G. Pope, D. Robert, An algorithmic approach to (2, 2)-isogenies in the theta model and applications to isogeny-based cryptography, in: Advances in Cryptology – ASIACRYPT 2024, 2025, pp. 304–338.

[3] W. Castryck, T. Decru, An efficient key recovery attack on SIDH, in: Advances in Cryptology – EUROCRYPT 2023, 2023, pp. 423–447.

[4] L. Maino, C. Martindale, L. Panny, G. Pope, B. Wesolowski, A direct key recovery attack on SIDH, in: Advances in Cryptology – EUROCRYPT 2023, 2023, pp. 448–471.

[5] D. Robert, Breaking SIDH in polynomial time, in: EUROCRYPT 2023, 2023, pp. 472–503.

[6] A. Basso, P. Dartois, L. D. Feo, A. Leroux, L. Maino, G. Pope, D. Robert, B. Wesolowski, SQIsign2D-West: The fast, the small, and the safer, in: ASIACRYPT 2024, 2024, pp. 339–370.

[7] A. Basso, G. Borin, W. Castryck, M. C.-R. Santos, R. Invernizzi, A. Leroux, L. Maino, F. Vercauteren, B. Wesolowski, PRISM: Simple and compact identification and signatures from large prime degree isogenies, to appear in PKC 2025 (2025).

[8] T. Shioda, Supersingular K3 surfaces, in: Algebraic Geometry, Summer meeting, 1979, pp. 564–591.

[9] B. Wesolowski, The supersingular isogeny path and endomorphism ring problems are equivalent, in: FOCS 2021, IEEE, 2021, pp. 1100–1111.

[10] D. Kohel, K. Lauter, C. Petit, J.-P. Tignol, On the quaternion ℓ-isogeny path problem, LMS Journal of Computation and Mathematics 17 (2014) 418–432.

[11] H. Onuki, K. Nakagawa, Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign, in: Advances in Cryptology – ASIACRYPT 2024, 2025, pp. 243–271.

[12] P. Dartois, Fast computation of 2-isogenies in dimension 4 and cryptographic applications, Cryptology ePrint Archive, Paper 2024/1180 (2024).
URL `https://eprint.iacr.org/2024/1180`

[13] W. Castryck, T. Decru, P. Kutas, A. Laval, C. Petit, Y. B. Ti, KLPT$^{\mathbf{2}}$: Algebraic pathfinding in dimension two and applications, Cryptology ePrint Archive, Paper 2025/372 (2025).
URL `https://eprint.iacr.org/2025/372`

[14] D. Boneh, D. Glass, D. Krashen, K. Lauter, S. Sharif, A. Silverberg, M. Tibouchi, M. Zhandry, Multiparty non-interactive key exchange and more from isogenies on elliptic curves, Journal of Mathematical Cryptology 14 (1) (2020) 5–14.

[15] W. C. Waterhouse, Abelian varieties over finite fields, Annales scientifiques de l'École normale supérieure 2 (4) (1969) 521–560.

[16] E. Kani, Products of CM elliptic curves, Collectanea mathematica 62 (3) (2011) 297–339.

[17] J. Voight, Quaternion Algebras, Springer, 2021.

[18] J. Eriksen, L. Panny, J. Sotáková, M. Veroni, Deuring for the people: Supersingular elliptic curves with prescribed endomorphism ring in general characteristic, Contemporary Mathematics 796 (2024) 339–373.

[19] B. W. Jordan, A. G. Keeton, B. Poonen, E. M. Rains, N. Shepherd-Barron, J. T. Tate, Abelian varieties isogenous to a power of an elliptic curve, Compositio Mathematica 154 (5) (2018) 934–959.

[20] A. Leroux, Quaternion algebras and isogeny-based cryptography, Ph.D. thesis, École Polytechnique (2022).

[21] A. Page, B. Wesolowski, The supersingular endomorphism ring and one endomorphism problems are equivalent, in: EUROCRYPT 2024, 2024, pp. 388–417.

[22] D. Robert, On the efficient representation of isogenies, in: NUTMIC 2024: Number-Theoretic Methods in Cryptology, 2024, pp. 3–84.

[23] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate texts in mathematics, Springer, 2009.

[24] A. H. L. Merdy, B. Wesolowski, The supersingular endomorphism ring problem given one endomorphism, arXiv preprint arXiv:2309.11912 (2023).

[25] A. Storjohann, Algorithms for matrix canonical forms, Ph.D. thesis, ETH Zurich (2000).

[26] E. Kani, The moduli spaces of Jacobians isomorphic to a product of two elliptic curves, Journal of Number Theory 139 (2014) 138–174.

[27] M.-F. Vignéras, Arithmétique des algèbres de quaternions, Springer, 1980.

[28] P. Q. Nguyen, D. Stehlé, Low-dimensional lattice basis reduction revisited, ACM Transactions on algorithms (TALG) 5 (4) (2009) 1–48.

[29] M. Kirschmer, J. Voight, Algorithmic enumeration of ideal classes for quaternion orders, SIAM Journal on Computing 39 (5) (2010) 1714–1747.