Isogeny-based Cryptography using Isomorphisms of Superspecial Abelian Surfaces

Pierrick Gaudry, Julien Soumier, and Pierre-Jean Spaenlehauer

Université de Lorraine, CNRS, Inria

Abstract. We investigate the algorithmic problem of computing isomorphisms between products of supersingular elliptic curves, given their endomorphism rings. This computational problem seems to be difficult when the domain and codomain are fixed, whereas we provide efficient algorithms to compute isomorphisms when part of the codomain is built during the construction. We propose an authentication protocol whose security relies on this asymmetry. Its most prominent feature is that the endomorphism rings of the elliptic curves are not hidden. Furthermore, it does not require a trusted setup.

Quickly after this preprint was published, Benjamin Wesolowski found a way to solve efficiently Problem 5.1 that we assumed to be hard. This kills our authentication protocol.

1 Introduction

Context and problem statement. Isogeny-based cryptography has known a recent fast evolution with the discovery of techniques based on isogenies of abelian varieties of dimension greater than 1. Many recent constructive [4,1,20] and destructive [22,2,16] cryptographic developments involve products of supersingular elliptic curves. 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 $\mathbb{F}_q$. The Deligne-Ogus-Shioda theorem [24] 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 in the case $g = 2$:

Problem 1.1 (Effective Deligne-Ogus-Shioda problem) *Given supersingular elliptic curves E_1, E_2, E_1', E_2' defined over $\mathbb{F}_q$, compute an $\overline{\mathbb{F}_q}$-isomorphism $E_1 \times E_2 \to E_1' \times E_2'$.*

This appears to be a difficult computational problem. In particular, being able to solve this problem would provide non-trivial information about the endomorphism rings of the curves. Indeed, 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.

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. [22,3,5]. 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 explicit isomorphisms is for representing *polarizations* on superspecial abelian varieties. In particular, many principal polarizations on superspecial abelian varieties arise from pullbacks of product polarizations via such isomorphisms. The recent development of isogeny-based cryptography have put the problem of computing endomorphism rings as one of its foundations. Up to our knowledge, all existing isogeny-based cryptosystems would be broken if a polynomial-time algorithm for computing endomorphism rings of elliptic curves is found. In this paper, we propose a cryptographic construction for which all endomorphism rings are public, and which therefore would not be broken by a fast algorithm computing endomorphism rings. This is an attempt to propose a new building block for isogeny-based cryptography.

Contributions. We study the problem of computing an isomorphism between two superspecial surfaces $E_1 \times E_2 \to E'_1 \times E'_2$, 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 contributions are polynomial-time algorithms to compute isomorphisms, in two special cases:

1. when we do not require control over E'_2: the input is E_1, E_2, E'_1, and the output is E'_2 together with an isomorphism $E_1 \times E_2 \to E'_1 \times E'_2$;
2. when we know subrings of $\mathrm{End}(E_1)$ and $\mathrm{End}(E'_1)$ which are isomorphic to low-discriminant imaginary quadratic orders.

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 3.7. 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 4.2.

This criterion is used in our algorithms for both special cases. In the first case, when we have only partial control over the codomain, we actually build the kernel of φ_{21} in order to enforce the conditions of the criterion. In the low-discriminant case, we use the fact that we can solve efficiently norm equations in low-discriminant imaginary quadratic orders to find endomorphisms; this allows to apply our criterion.

In both special cases, we use Wesolowski's heuristic-free variant [30] of KLPT algorithm [13] as an important subroutine. For cryptographic purposes, we will use the randomized version [6, Algo. 5] which relies on some heuristics.

The general problem of computing isomorphisms between superspecial abelian surfaces seems to be hard. Indeed, the techniques that we developed for the special cases require more degrees of freedom that what is available in the general case. Furthermore, randomly constructed isogenies for the first column of the matrix have no chance to produce a valid input for our criterion in Theorem 4.2. We therefore propose a cryptographic construction built on the difficulty of this problem. The main interest of this construction is that most algebraic computations can be done in the quaternion algebra $\mathscr{B}_{p,\infty}$ since the endomorphism rings and their embedding in $\mathscr{B}_{p,\infty}$ are public. This is a significant difference compared to other isogeny-based cryptographic protocols where the knowledge of the endomorphism ring in a quaternion algebra is usually sufficient to break the cryptosystem. The security of this cryptosystem relies on heuristic assumptions which are similar to a heuristic used for the security of SQIsign [6]. In particular, given a product of supersingular curves $E_1 \times E_2$, we can use the algorithm with partial control over the codomain to generate a secret isomorphism $E_1 \times E_2 \to E_1' \times E_2'$ where the pair of j-invariants $(j(E_1'), j(E_2'))$ is heuristically undistinguishable from the uniform distribution on pairs of j-invariants of supersingular elliptic curves. Combining this with a masking technique using automorphisms provides us with an authentication protocol.

Finally, we provide a proof-of-concept implementation in the computer algebra software `Magma`, which demonstrates 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}, that lead to 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 [1,19].

Organization of the paper. Section 2 describes the background on Deuring correspondence, superspecial abelian varieties and efficient representations of isogenies. In Section 3, we develop theoretical and computational tools that will be required in the main algorithms. Section 4 is devoted to the computation of isomorphisms between superspecial abelian surfaces in some special cases, and provided that we know their endomorphism rings. Finally, in Section 5, we

propose a new authentication protocol whose security relies of the difficulty of computing isomorphisms between superspecial abelian surfaces.

Acknowledgements. We thank Jean Kieffer and Damien Robert for fruitful discussions. 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.

2 Background

When nothing else is specified, 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 will also assume, for simplicity, that the characteristic p of the fields discussed later is strictly greater than 3.

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 [29] 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 $\mathrm{End}(E)$ are *kernel ideals*, see [29, Thm. 3.15] for the cases where $\mathrm{End}(E)$ has rank 1 or 4, and [10, 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.

2.1 Deuring correspondence

We recall key concepts of the Deuring correspondence. For a more comprehensive study of the subject, we refer to [15] and [28].

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 $\mathbb{Q}$; a $\mathbb{Q}$-basis is $1, i, j, k$, where

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

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 2.1 (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 2.2 *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 $\mathbb{Z}[i, \frac{1+k}{2}]$ [13, Lem. 2], which is maximal.*

Definition 2.3 (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 [28, Lem. 16.2.8]), we say that I is an integral ideal.

Integral ideals in maximal orders are actually locally principal [28, 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 will give more details in Section 3.5.

Remark 2.4 *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 2.5 (Ideal norm) *[28, 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 2.6 *[28, 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 $\mathrm{Nrd}(I \cdot J) = \mathrm{Nrd}(I) \cdot \mathrm{Nrd}(J)$.*

The correspondence. Endomorphism rings of superspecial elliptic curves can be regarded as 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 2.7 *[28, Thm. 42.1.9] Let E be a supersingular elliptic curve defined over $\overline{\mathbb{F}_p}$. Then the endomorphism ring $\mathrm{End}_{\overline{\mathbb{F}_p}}(E)$ 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 $\mathrm{End}_{\overline{\mathbb{F}_q}}(E)$ of a supersingular elliptic curve E defined over $\overline{\mathbb{F}_q}$. We will implicitly use the isomorphism $\mathrm{End}_{\overline{\mathbb{F}_q}}(E) \to \mathscr{O}$ 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 [28, 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 $\mathrm{End}_{\overline{\mathbb{F}_q}}(E)$-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 [28, 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 $\mathrm{End}_{\overline{\mathbb{F}_q}}(E)$-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 [15, Table 2.1] — we summarize the main dictionary in the Deuring correspondence.

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.

Remark 2.8 *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 [28, 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 [7, Lem. 4] and [9, 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 [9, Lem. 5.7].*

2.2 Efficient representations of isogenies

Recent advances in cryptography have provided new techniques for representing and computing with isogenies [14,21,23]. We use the notion of *efficient representation* of an isogeny designed in [21,23].

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 would actually be sufficient since the degree can then be recovered via the CRT by using the Weil pairing in small torsion subgroups [23, 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 two representations we will use are the *ideal* and the *HD* representations, and both are compact. The latter is always effective, while the former is effective provided that we have an effective representation of a basis of the endomorphism ring of E, according to [23].

Ideal representation. The core idea of the ideal representation is to represent an isogeny $\varphi : E \to E'$ by using 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. Note that if $j(E') \neq 0, 1728$ then the only automorphisms of E' are ± 1 [25, Appendix A, Prop. 1.2.(c)]. 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.

Theorem 2.9 *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 and efficient representation of φ.*

For more details, see [23, Sec. 4.2 and C.1].

HD representation. The successive attacks on SIDH have led to new constructive applications. One of the most significant for us is that we can now evaluate an isogeny using calculations performed in higher dimensions, given only the image of certain torsion points. And to work with such points, we may need to deal with high degree extensions of $\mathbb{F}_q$. But to keep efficient computation we can not work in too big finite fields.

Theorem 2.10 *[23, Thm. 5.19] Let $\varphi : E \to E'$ be an isogeny of degree n. Let $N = \prod \ell_i > n$ be a smooth integer coprime to n, with $\max(\ell_i) = \log^{O(1)} N$. For*

each i, let (P_i, Q_i) be a $\mathbb{Z}$-basis of $E[\ell_i]$, such that $\langle \bigoplus_i P_i, \bigoplus_i Q_i \rangle = E[N]$. The data of n, E, E' and the interpolation data $(P_i, \varphi(P_i), Q_i, \varphi(Q_i))_i$ gives a compact and efficient representation of φ, called an HD representation.

Note that this representation is *universal*, meaning that any efficient representation can be efficiently converted into an HD representation. An interesting feature for cryptographic applications is that the interpolation data does not reveal any information about the way the isogeny was constructed.

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 [23, Sec. 6.1]. □

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 $b_1, \ldots, b_4$ of $\mathrm{End}(E)$ is given, and that we also have access to elements $\beta_1, \ldots, \beta_4 \in \mathscr{B}_{p,\infty}$ such that the $\mathbb{Z}$-module $\mathscr{O}$ generated by $\beta_1, \ldots, \beta_4$ 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) [24, Thm. 3.5] Let k be an algebraically closed field of characteristic $p > 0$. Let $C_1, \ldots, C_g$ and $C_1', \ldots, C_g'$ be supersingular elliptic curves, where $g \geq 2$. Then there exists an isomorphism:*

$$C_1 \times \cdots \times C_g \cong C_1' \times \cdots \times C_g'.$$

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 in play.

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 $\mathrm{End}_{\overline{\mathbb{F}_p}}(E_0)$ 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 (resp. minimal), i.e. they have $(p+1)^2$ (resp. $(p-1)^2$) $\mathbb{F}_{p^2}$-rational points, this isomorphism is defined over $\mathbb{F}_{p^2}$, see [9, Lem. 5.2].

In this work, we explore the problem of finding explicit isomorphisms between superspecial abelian surfaces. We specialize to the case of superspecial abelian surfaces given as products of supersingular elliptic curves over $\mathbb{F}_{p^2}$. The goal of this article is thus to find an isomorphism between the products $E_1 \times E_2$ and $E_1' \times E_2'$.

3 Tools

In this section, we develop tools which will be useful for computing isomorphisms in Section 4. In Section 3.1, we study algorithms for dividing endomorphisms by isogenies. Section 3.2 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 3.3, 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. In Section 3.4, we describe families of easily constructible automorphisms of products of elliptic curves; these automorphisms are useful for hiding secret data in cryptographic constructions, see Section 5. Finally, in Section 3.5, we design algorithms for finding the generator of the localization of a left-ideal in a maximal order of $\mathscr{B}_{p,\infty}$.

3.1 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 [23, Cor. 6.8]. A detailed complexity analysis is provided in [17, 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 3.1 (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 3.2 *If $\mathrm{Nrd}(I)$ and $\mathrm{Nrd}(J)$ are coprime, then [1, 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 3.1 is unambiguous.

Lemma 3.3 *The solution of Problem 3.1 is unique.*

Proof. Let J_1 and J_2 be two solutions of Problem 3.1. 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 [28, 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 $J_1 = J_2$. □

For technical reasons we will first address the slightly different problem below. We first show that we can factor (on both sides) a principal ideal generated by an integer. In other words, we first deal with the case $\mu \in \mathbb{Z}$.

Problem 3.4 (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 3.5 *The same argument as in the proof of Lemma 3.3 shows the unicity of the solution of Problem 3.4. 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 3.4 and 3.1 are equivalent: the solution J of Problem 3.1 with input $\mathscr{O}_1, \mathscr{O}_2, \mu, I$ equals the solution of Problem 3.1 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 3.4.

Proposition 3.6 *With the same notation as in Problem 3.4, $J = \{s \in \mathscr{O}_1 \cap \mathscr{O}_2 : Is \subset \mathscr{O}_1 d\}$.*

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 3.6 reduces Problem 3.4 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 $\{x_i\}_{0 \le i \le 3}$, $\{y_{ij}\}_{0 \le i,j \le 3}$:

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

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 $\{(x_0^{(i)}, \ldots, x_3^{(i)})\}_{1 \le i \le 16}$. Finally, writing $a^{(j)} = (a_0^{(j)}, \ldots, a_3^{(j)})$, the set $\{\sum_{0 \le i \le 3} a_i^{(j)} v_i\}_{0 \le j \le 3}$ is a $\mathbb{Z}$-basis for J.

Proposition 3.7 *With the same notation as in Problem 3.4, 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 [26, Chap. 6]. □

Remark 3.8 *The reduction in Remark 3.5 shows that Problem 3.1 can also be solved in quasi-linear complexity.*

3.2 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 [11, 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 3.9 *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 $\nu := \widehat{\varphi}_{22}\varphi_{21}$. [11, 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 3.9 in order to compute degrees of isogenies between superspecial abelian surfaces. 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 3.10 *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 3.9, we have

$$\deg(\mu + \nu) = (d_{11} + d_{21})(d_{12} + d_{22}) - \deg(\phi).$$

Therefore, we obtain the equality

$$\deg(\mu+\nu)-\deg(\mu)-\deg(\nu)=\frac{d_{11}}{d_{21}}\deg(\nu)+\frac{d_{21}}{d_{11}}\deg(\mu)-\deg(\phi). \tag{3.1}$$

By multiplying (3.1) by $d_{11}d_{21}$, we obtain

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

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

3.3 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 3.11 *With the same notation as in Proposition 3.9, let* $\widetilde{\phi}\in\operatorname{Hom}(E_1'\times E_2', E_1\times E_2)$ *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 3.9 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, $\deg(\phi)=\deg(\widetilde{\phi})$. □

3.4 Automorphisms of products $E_1\times E_2$

In this section we prove that the data of an isogeny $\varphi: E_1\to E_2$ between elliptic curves allows us to compute families of non-trivial automorphisms of $E_1\times E_2$. We shall use such automorphisms in cryptographic applications (Section 5) in order to hide secret data.

Proposition 3.12 *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 3.9,

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

□

Remark 3.13 *Direct computations show that the inverse of the automorphism $F = \begin{pmatrix} a & b\widehat{\varphi} \\ c\varphi & d \end{pmatrix}$ is $F^{-1} = \begin{pmatrix} d & -b\widehat{\varphi} \\ -c\varphi & a \end{pmatrix}$.*

3.5 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 $\mathcal{O}$ is a maximal order in a quaternion algebra over $\mathbb{Q}$ not ramified at ℓ, then $\mathcal{O} \otimes \mathbb{Z}_\ell$ 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 3.14 *[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 3.15 *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 3.15 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 3.15.

4 Computing isomorphisms in special cases

In this section, which contains our main algorithms, we start by giving a criterion for an isomorphism to exist, if we fix already 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 in two special cases. However, this does not solve the general isomorphism question of Problem 5.1, that we believe to be a hard problem.

4.1 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 4.1 *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

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

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. □

We are now ready to state the main theoretical result of the paper.

Theorem 4.2 *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 3.10, there exist isogenies $\varphi_{12} : E_2 \to E_1'$, $\varphi_{22} : E_2 \to E_2'$ such that $\phi = (\varphi_{ij})_{i,j\in\{1,2\}} \in \operatorname{Hom}(E_1 \times E_2, E_1' \times E_2')$ 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 4.1 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 $\tau \in \operatorname{Hom}(E_1/K, E_2)$. 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 $\phi = (\varphi_{ij})_{i,j\in\{1,2\}} \in \operatorname{Hom}(E_1 \times E_2, E_1' \times E_2')$ is an isomorphism if and only if there exists $\tau \in \operatorname{Hom}(E_1/K, E_2)$ with $\deg(\tau) = 1$, *i.e.* if and only if E_1/K and E_2 are isomorphic. □

Theorem 4.2 is actually effective, provided that we know the endomorphism rings of the curves. Algorithm 1 computes such an isomorphism.

Proposition 4.3 *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 4.2. An isogeny associated to the ideal I_ψ plays the role of ψ in the proof of Theorem 4.2. The ideals I_{11}, I_{21} correspond to the isogenies $\varphi_{11}, \varphi_{21}$ in Theorem 4.2, and the ideals J_{11} and J_{21} play the same role as in the proof of Theorem 4.2. We now prove that the endomorphism ξ computed in Step 5 satisfies the requirements of σ in the proof of Theorem 4.2, namely that $\mathrm{Nrd}(\xi) = d_{11}d_{21}\,\mathrm{Nrd}(I_\psi)$. By the same argument as in the proof of Theorem 4.2, 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 4.2 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 [18, 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 $|\mathrm{Aut}(E)| \leq 24$ [25, Appendix A, Prop. 1.2.(c)]. Converting the ideal representation to an efficient representation can be done in polynomial-time, see e.g. [23, Appendix C]. □

4.2 Building isomorphisms when the codomain is not constrained

In this section, we propose a fast algorithm for the following problem: upon input of supersingular elliptic curves E_1, E_2, E_1' and their endomorphism rings, we wish to compute a curve E_2' together with an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$. We believe that the problem of computing isomorphisms from $E_1 \times E_2$ is difficult (even when the endomorphism rings are given) when the codomain is fixed, whereas it is computationally easy when the codomain is not constrained. This asymmetry will be instrumental for designing an authentication procotol in Section 5.

Theorem 4.4 *Algorithm 2 is correct. It is a probabilistic Las Vegas algorithm which computes a supersingular elliptic curve* E_2' *and isogenies* $\varphi_{21} : E_1 \to E_2'$, $\varphi_{12} : E_2 \to E_1'$ *and* $\varphi_{22} : E_2 \to E_2'$, *such that* (φ_{ij}) *is an isomorphism. Assuming GRH, for* ℓ_1, ℓ_2 *fixed, the expected running time of Algorithm 2 is polynomial in* $\log(p)$ *and in the input size.*

Algorithm 1: IsomorphismCompletion

Input: Four supersingular curves E_1, E_1', E_2, E_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 $I_{11}, I_{21} \subset \mathscr{O}_1$ corresponding 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 [12, 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. 3.7 and Remark 3.8`

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 3.9, find a matrix among them which is an isomorphism and return it;

Algorithm 2: IsomAndCodomain

Input: Supersingular elliptic curves E_1, E_2, E_1' defined over $\mathbb{F}_{p^2}$, maximal orders $\mathscr{O}_1, \mathscr{O}_2, \mathscr{O}_1'$ together with isomorphisms $\mathscr{O}_1 \cong \mathrm{End}(E_1)$, $\mathscr{O}_2 \cong \mathrm{End}(E_2)$, $\mathscr{O}_1' \cong \mathrm{End}(E_1')$, and two small distinct primes $\ell_1, \ell_2 \neq p$.

Output: Returns an elliptic curve E_2' and an efficient representation of an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$.

1 Compute a left $\mathscr{O}_1$-ideal I_{11} with reduced norm $\ell_1^{m_1}$ for a positive integer m_1, such that $E_1/E_1[I_{11}] \simeq E_1'$;
`// use KLPT [13] or [30, Algo. 5]`

2 Compute a left $\mathscr{O}_R(I_{11})$-ideal J with reduced norm $\ell_2^{m_2}$ for a positive integer m_2, such that $E_1'/E_1'[J] \simeq E_2$;
`// use KLPT [13] or [30, Algo. 5]`

3 Compute a $\mathbb{Z}$-basis of the left $\mathscr{O}_1$-ideal $I_{21} := \{x \in \mathscr{O}_1 : \ell_1^{m_1}x \subset I_{11}J\}$;
`// This is linear algebra over` $\mathbb{Z}$.

4 Using the fact that $\mathrm{Nrd}(I_{21}) = \ell_2^{m_2}$ and hence I_{21} corresponds to a composition of m_2 isogenies of degree ℓ_2, compute a curve E_2' such that $E_2' \cong E_1/E_1[I_{21}]$;

5 Return E_2' and IsomorphismCompletion$(E_1, E_2, E_1', E_2', \mathscr{O}_1, \mathscr{O}_2, I_{11}, I_{21})$;

Proof. Throughout this proof, for Steps 1 and 2, we use the heuristic-free algorithm [30, Algo. 5], whose correctness and complexity are proved under GRH.

In order to prove the correctness, the crucial point that we need to show is that the ideal I_{21} constructed at Step 3 satisfies the assumptions of Theorem 4.2, i.e. that the direct sum of the kernels of the isogenies corresponding to I_{11} and I_{21} is the kernel of an isogeny $E_1 \to E_2$. By Lemma 4.1, this amounts to showing that $\mathrm{Nrd}(I_{21}) = \ell_2^{m_2}$ and $I_{11}J = \ell_1^{m_1} I_{21} + \ell_2^{m_2} I_{11}$. Indeed, applying Lemma 4.1 to $\varphi_{I_{21}}$, $\varphi_{I_{21}}$ and $\psi = \mathrm{Id}_{E_1}$ yields to the fact that $\mathrm{Nrd}(I_{21})I_{11} + \ell_1^{m_1} I_{21}$ correspond to $\mathrm{Hom}(E_1/K, E_1)\pi_K$ for $K = \ker(\varphi_{I_{21}}) \oplus \ker(\varphi_{I_{11}})$. But if $\mathrm{Nrd}(I_{21}) = \ell_2^{m_2}$ and $I_{11}J = \ell_1^{m_1} I_{21} + \ell_2^{m_2} I_{11}$, then $\mathrm{Hom}(E_1/K, E_1)\pi_K$ also correspond to $I_{11}J$. Thus as left $\mathscr{O}_1$-ideals, $I_{11}J = I_{\pi_K}$. Hence $E_1/E[I_{11}J] = E_1/E[I_{\pi_K}]$ and $E_1'/E_1'[J] \simeq E_1/K$. Finally by assumption on J, $E_2 \simeq E_1/K$.

First we show that $I_{11}J = \ell_1^{m_1} I_{21} + \ell_2^{m_2} I_{11}$. We notice that $\ell_2^{m_2} I_{11} \subset I_{11}J$, which implies that $\ell_1^{m_1} I_{21} + \ell_2^{m_2} I_{11} \subset I_{11}J$ by definition of I_{21}. Conversely, let $x_{11} \in I_{11}$ and $x_J \in J$, we want to show that $x_{11}x_J \in \ell_1^{m_1} I_{21} + \ell_2^{m_2} I_{11}$. Since ℓ_1 and ℓ_2 are coprime, there exists $u, v \in \mathbb{Z}$ such that $1 = \ell_1^{m_1} u + \ell_2^{m_2} v$. Thus $x_{11}x_J = \ell_1^{m_1} u x_{11}x_J + \ell_2^{m_2} v x_{11}x_J$. Finally we remark that $v x_{11}x_J \in I_{11}$ so that $\ell_2^{m_2} v x_{11}x_J \in \ell_2^{m_2} I_{11}$, and $u x_{11}x_J \in I_{21}$ because $\ell_1^{m_1} u x_{11}x_J \in I_{11}J$. Hence we conclude that $x_{11}x_J \in \ell_1^{m_1} I_{21} + \ell_2^{m_2} I_{11}$.

Now we prove that $\mathrm{Nrd}(I_{21}) = \ell_2^{m_2}$. First remark that $\ell_2^{m_2} \in I_{21}$ by definition, thus $\mathrm{Nrd}(I_{21}) \mid \ell_2^{m_2}$. Conversely, let $x_{21} \in I_{21}$, so that $\ell_1^{m_1} x_{21} \in I_{11}J$. Then $\mathrm{Nrd}(I_{11}J) = \ell_1^{m_1}\ell_2^{m_2} \mid \ell_1^{m_1} \mathrm{Nrd}(x_{21})$. By coprimality we deduce that $\ell_2^{m_2} \mid \mathrm{Nrd}(x_{21})$.

Finally Algorithm 2 terminates in heuristic probabilistic polynomial time in $\log(p)$ and the size of the inputs. This follows from [30, Thm. 6.4] for the first two steps (m_1 and m_2 are chosen to be sufficiently large), from Proposition 4.3 for the last step, and from usual $\mathbb{Z}$-linear algebra algorithms for the other steps. □

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`. For this proof-of-concept implementation, we reduced to the special case where $E_1 = E_2 = E_0$. First we let the user choose the following parameters: a lower bound for the prime p, a little prime ℓ and an exponent m that $\ell^m > 2p$. Then we build two random ideals, first I_{11} with norm $d_{11} := \ell^m$, then J with norm d_J coprime to d_{11} and such that $I_{11}J$ is a principal left $\mathscr{O}_0$-ideal. With $\mathbb{Z}$-linear algebra we are able to recover the ideal I_{21} as in Step 3 with a call to FindI21.mgm. It determines (the isomorphism class of) E_2', since $\mathscr{O}_2'$ is now the right order of I_{21}. We conclude as in Algorithm 2 by computing the ideals I_{12} and I_{22}, with a call to Algorithm 1, presented in IsomorphismCompletion_SpecialCase.mgm. We can finally check that the ideals I_{ij} represent an isomorphism.

Example 4.5 *We set the seed to be* 12345*. If we set the lower bound* $l_b := 1000$*, then* $p = 1019$*. We denote by* i_q, j_q, k_q *the usual generators of* $\mathscr{B}_{p,\infty}$*. If we set* $\ell := 3$*,* $m := 8$*, an instance of our algorithm is given by* $I_{11} =$

$\langle 6561, 6561\,i_q, 5727/2 + 5303\,i_q + k_q/2, 5303 + 7395\,i_q/2 + j_q/2\rangle$ *of norm* 3^8*, and*

$$I_{21} = \langle 13003094501, 13003094501\,i_q, 7379255027/2 + 4184616424\,i_q + k_q/2, \\ 4184616424 + 18626933975\,i_q/2 + j_q/2\rangle$$

of norm 13003094501*. Then* IsomorphismCompletion_SpecialCase *returns*

$$\begin{aligned}
I_{12} = \langle & 37613191543109 - 246780149714338149\,k_q, \\
& - 37613191543109\,i_q/6561 - 95650346094126187\,j_q/2187 \\
& - 1400185132743770581754\,k_q/6561, \\
& 29921922947917 - 18751589796940\,i_q/6561 - 47685292856404658\,j_q/2187 \\
& - 198608558098789375835\,k_q/6561, \\
& 35439812151471 - 35805775615792\,i_q/6561 - 91054087390959056\,j_q/2187 \\
& - 2858470143362188506697\,k_q/6561\rangle. \\
I_{22} = \langle & 189939937316853583931789/2 \\
& - 24698069544450635318455875049922 89\,k_q/2, \\
& - 189939937316853583931789\,i_q/26006189002 \\
& - 2948662288363563014156316022054933\,j_q/26006189002 \\
& - 5562420807416308194134180760499769417126 52\,k_q/13003094501, \\
& 8126557187854449202689 5 - 28046700416508535541985\,i_q/26006189002 \\
& - 435402101313904500613719060222547\,j_q/26006189002 \\
& - 1382255601325640315842323112787458821862636 4\,k_q/13003094501, \\
& 72080406466220369649903 - 8232575935895622879723 2\,i_q/13003094501 \\
& - 1278040128957694099074362135894704\,j_q/13003094501 \\
& - 1266957330904376960832762488955069388010545 6\,k_q/13003094501\rangle.
\end{aligned}$$

The function RepresentIsomorphism *returns* TRUE *on input* $(I_{11}, I_{12}, I_{21}, I_{22})$.

4.3 Computing isomorphisms $E_0^2 \to E_1' \times E_0$

In this section, we focus on a special case of Problem 1.1: we assume that the endomorphism rings of all curves are known, and that we also know subrings of $\mathrm{End}(E_1)$ and $\mathrm{End}(E_1')$ which are isomorphic to a low-discriminant imaginary quadratic order. In this case, we provide a fast algorithm to solve Problem 1.1. 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 4.15. 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 summary, our objective in this section is to provide a fast algorithm for the following problem:

Problem 4.6 (Low-discriminant Deligne-Ogus-Shioda problem) *Given a supersingular elliptic curve E_1' defined over $\mathbb{F}_q$ and its endomorphism ring, compute an $\overline{\mathbb{F}_q}$-isomorphism $E_0 \times E_0 \to E_1' \times E_0$.*

The following statement gives sufficient conditions to use the strategy of Theorem 4.2.

Proposition 4.7 *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 4.7 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 4.7. As explained above, we specialize to the case $E = E_0$, and $p \equiv 3 \mod 4$, 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 3 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 4.7 is actually related to computing a generator of a localization of the ideal I associated to φ at a prime ℓ.

Lemma 4.8 *Let $\mathcal{O} \subset \mathcal{B}_{p,\infty}$ be a maximal order, $I \subset \mathcal{O}$ be a left ideal, $\alpha \in \mathcal{O}$ 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 $x \in \mathcal{O}$, such that $\alpha x \in I$ and $\mathrm{Nrd}(x)$ is not divisible by ℓ;
(b) There exists an invertible $y \in \mathcal{O} \otimes \mathbb{Z}_\ell$ such that $\alpha y \in I \otimes \mathbb{Z}_\ell$.

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

We now prove *(b)⇒(a)*. Let y be as in *(b)*. Let $b_1, \ldots, b_4$ 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 $z_1, \ldots, z_4 \in \mathbb{Z}_\ell$. Next, pick integers $z_1', \ldots, z_4' \in \mathbb{Z}$ such that $z_i' \equiv z_i \bmod \ell^e$, where e is the ℓ-valuation of $\mathrm{Nrd}(\alpha)$. Then set $y' = \alpha^{-1}(z_1' \cdot b_1 + \cdots + z_4' \cdot b_4) \in \mathcal{B}_{p,\infty}$. 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 $\mathcal{O}$. Notice that x clearly belongs to localized orders $\mathcal{O} \otimes \mathbb{Z}_{\ell'}$ for primes $\ell' \neq \ell$, so we only have to prove that $x \in \mathcal{O} \otimes \mathbb{Z}_\ell$. To do so, we use the fact that $z_i \equiv z_i' \bmod \ell^e$, hence there exists $z_1'', \ldots, z_4'' \in \mathbb{Z}_\ell$ 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 $x \in \mathcal{O} \otimes \mathbb{Z}_\ell$. 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 4.9 *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 $I \subset \mathcal{O}$ be a left-ideal of a maximal order in $\mathcal{B}_{p,\infty}$, and $\ell \neq p$ be a prime number. By [27, Cor. I.2.4], $\mathcal{O} \otimes \mathbb{Z}_\ell$ 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 $\mathcal{O} \otimes \mathbb{Z}_\ell \cong \mathrm{M}_2(\mathbb{Z}_\ell)$. If $\alpha \in \mathcal{O}$ is an element in a maximal order, its ℓ-type is defined as the ℓ-type of the left-ideal $\mathcal{O}\alpha$.

Proof. The only thing that we need to prove is that the definition of the ℓ-type of a left ideal $I \subset \mathcal{O} \otimes \mathbb{Z}_\ell \cong \mathrm{M}_2(\mathbb{Z}_\ell)$ 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 4.10 *With the same notation as in Lemma 4.8, the ℓ-types of I and α are the same if and only if there exists an invertible $y \in \mathcal{O} \otimes \mathbb{Z}_\ell$ such that $\alpha y \in I \otimes \mathbb{Z}_\ell$.*

Proof. In this proof, we fix an isomorphism $\mathcal{O} \otimes \mathbb{Z}_\ell \cong \mathrm{M}_2(\mathbb{Z}_\ell)$ 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 $y \in (\mathcal{O} \otimes \mathbb{Z}_\ell)^\times$ 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. □

Lemma 4.11 *With the same notation as in Lemma 4.8, if $\alpha \in \mathcal{O}$ has ℓ-type (i, j), then there exists $\alpha' \in \mathcal{O}$ with ℓ-type $(0, j - i)$ such that $\alpha = \ell^i \, \alpha'$. Similarly,*

if $I \subset \mathcal{O}$ is a left-ideal which has ℓ-type (i,j), there exists a left-ideal $I' \subset \mathcal{O}$ with ℓ-type $(0, j-i)$ and $I = \ell^i \cdot I'$.

Proof. Using 4.9, 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 $M = \ell^i M'$. □

We are now ready to prove the main algorithmic result of this section.

Algorithm 3: LocalGenerator

Input: A prime ℓ, a left ideal $I \subset \mathcal{O}_0$ not divisible by ℓ with reduced norm $\mathrm{Nrd}(I) = \ell^m \gg 2p$.

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

repeat
  Pick at random $\alpha_2, \alpha_3 \in \{-\left\lfloor \sqrt{\ell^m/(2p)} \right\rfloor, \ldots, \left\lfloor \sqrt{\ell^m/(2p)} \right\rfloor\}$ not both divisible by ℓ;
  Set $N := \ell^m - p(\alpha_2^2 + \alpha_3^2)$;
until N *is a prime congruent to* $1 \bmod 4$;;
Using Cornacchia's algorithm, compute α_0 and α_1 such that $N = \alpha_0^2 + \alpha_1^2$;
Using the isomorphism $\phi : \mathcal{O}_0 \otimes \mathbb{Z}_\ell \to \mathrm{M}_2(\mathbb{Z}_\ell)$, compute $M_\alpha := \phi(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 ij) \bmod \mathbb{Z}/\ell^m\mathbb{Z} \in \mathrm{M}_2(\mathbb{Z}/\ell^m\mathbb{Z})$;
Compute a generator $\beta \in \mathcal{O} \otimes \mathbb{Z}/\ell^m\mathbb{Z}$ 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 3.15`
Set $M_\beta := \phi(\beta) \in \mathrm{M}_2(\mathbb{Z}/\ell^m\mathbb{Z})$;
Using the Smith Normal Form, compute two matrices $S, T \in \mathrm{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z})$ such that $S \cdot M_\alpha \cdot T = M_\beta$;
By lifting coordinates from $\mathbb{Z}/\ell^m\mathbb{Z}$ to representatives in $\mathbb{Z}$, set x an element of $\mathcal{O}$ such that $x \equiv \phi^{-1}(T) \bmod \mathbb{Z}/\ell^m\mathbb{Z}$;
Return $(\alpha, x) \in \mathcal{O}_0^2$;

Theorem 4.12 *Algorithm 3 is correct. Assuming that $\ell^m \gg 2p$, and under the heuristic assumption that for any ℓ, m, p, the number $N := \ell^m - p(\alpha_2^2 + \alpha_3^2)$ is prime and congruent to $1 \bmod 4$ with probability $\Omega(1/(m \log \ell))$ (where the constant in the $\Omega()$ does not depend on any other variable, and (α_2, α_3) is picked uniformly at random among the admissible pairs), Algorithm 3 eventually terminates and it requires an expected number of $\widetilde{O}(m \log(\ell))$ bit operations.*

Proof. The fact that Algorithm 3 is correct is a direct consequence of Lemma 4.11 (to prove that the ℓ-types of I and α are the same) and of the proof of Lemma 4.10 which explains how to construct the elements α and x.

The termination of Algorithm 3 is straightforward: if $\ell^m \gg 2p$, then there exist α_2, α_3 not both divisible by ℓ in $\{-\left\lfloor\sqrt{\ell^m/(2p)}\right\rfloor, \ldots, \left\lfloor\sqrt{\ell^m/(2p)}\right\rfloor\}$, and the heuristic assumption implies that there is a positive probability of being such that $\ell^m - p(\alpha_2^2 + \alpha_3^2)$ is prime and congruent to 1 modulo 4.

Finally, the quasi-linear complexity is a consequence of the following ingredients:

- The heuristic assumption implies that the repeat-until loop is expected to be executed $O(m\log(\ell))$ times;
- Cornacchia's algorithm is quasi-linear [8, Rem. 3.4];
- 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 $\widetilde{O}(m\log(\ell))$ [26, Chap. 8].

□

Finally, we put all the pieces together and we give a complete algorithm (Algorithm 4) to compute an isomorphism $E_0^2 \to E_1 \times E_0$ upon input of E_1 and its endomorphism ring.

Algorithm 4: IsomorphismE0

Input: A supersingular 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 $\ell^m \gg 2p$ for some $m \in \mathbb{Z}_{\geq 0}$ such that its right-order is conjugated to $\mathscr{O}_1'$;
`// use KLPT [13] or [30, Algo. 5]`
2 Set $\alpha, \nu_1 :=$ LocalGenerator(ℓ, I_{11});
3 Return IsomorphismCompletion$(E_0, E_1', E_0, E_0, \mathscr{O}_0, \mathscr{O}_1, I_{11}, \mathscr{O}_0\nu_1)$;

Theorem 4.13 *Algorithm 4 is correct and it requires an expected number which is polynomial in* $\log(p)$.

Proof. The correctness is a direct consequence of Theorem 4.2 and Proposition 4.7, together with the correctness of the subroutines, see Theorem 4.12 and Proposition 4.3. The complexity also follows from the complexities of the subroutines (Theorem 4.12 and Proposition 4.3), together with the fact that the output size of Wesolowski's algorithm [30, Algo. 5] is polynomial in $\log(p)$. □

The following corollary shows that by running twice Algorithm 4, we can compute isomorphisms $E_1 \times E_0 \to E_2 \times E_0$.

Corollary 4.14 *Let E_1, E_2 be two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, with known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$. Assuming GRH we can compute an efficient representation of an 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 4 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 3.3, 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 4.15 *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 4.14 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 orientations of E_1, 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 4 we propose in the file ExperimentResults_part2.mgm available at `https://gitlab.inria.fr/superspecial-surfaces-isomorphisms/experiments`. As in the previous experiment paragraph in Section 4.2, 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, as explained above. Those computations allow us to set $I_{21} := \mathcal{O}_0\nu_1$. Finally, as described in Algorithm 4, we recover the two last ideals I_{12} and I_{22} by a call to IsomorphismCompletion_specialCase. The function RepresentIsomorphism ensures us that the computed ideals represent an isomorphism.

Example 4.16 *We set the seed to be* 12345. *If we set the lower bound $l_b := 100$, then $p = 103$. We choose a bound smaller than in Section 4.2, so that the coefficients of the basis fit in one page. We denote by i_q, j_q, k_q the usual generators of $\mathcal{B}_{p,\infty}$. If we set $\ell := 3$, $m := 5$, the ideal I_{11} is given by the basis: $\langle 243, 243\,i_q, 61/2 + 4\,i_q + k_q/2, 4 + 425\,i_q/2 + j_q/2\rangle$. Further computation leads to $\alpha = 6 + i_q + j_q - k_q$, and $\nu_1 = 1075/2 + 1577\,i_q + 244\,j_q + 625\,k_q/2$. The function*

IsomorphismCompletion_specialCase returns the ideals:

$$
\begin{aligned}
I_{21} =&\langle 2270721937/2 - 551785430691\, k_q/2,\\
&- 2270721937\, i_q/486 - 1051344256831\, j_q/486 - 129953416454510\, k_q/243,\\
&50499229/2 - 1/162\,(298530595\, i_q + 138219685087\, j_q + 35163788972983\, k_q)\,,\\
&154335016 - 78843721\, i_q/81 - 36504642823\, j_q/81 - 12062230807231\, k_q/81\rangle.\\
I_{22} =&\langle 5361340538374912 - 1016865998247415258109 44\, k_q,\\
&- 2680670269187456\, i_q/18966637 - 55856914626107754862976\, j_q/18966637\\
&- 16973417607085427459139415869 44\, k_q/18966637,\\
&2136763600071452 - 958438363694345\, i_q/18966637\\
&- 19970904467668410778293\, j_q/18966637\\
&- 13755272629822659210466732305 48\, k_q/18966637,\\
&2914265937452479 - 120604897180148\, i_q/18966637\\
&- 2513034714755866644308\, j_q/18966637\\
&- 11247229404189680062435057944 41\, k_q/18966637\rangle.
\end{aligned}
$$

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

5 An authentication protocol

We propose an authentication protocol whose security is based on the hardness of the general Deligne-Ogus-Shioda problem with known endomorphism rings.

Problem 5.1 *Given E_1, E_2, E_1', E_2', four supersingular elliptic curves over $\mathbb{F}_{p^2}$, with their endomorphism rings, compute an isomorphism $E_1 \times E_2 \to E_1' \times E_2'$.*

Additional heuristic assumptions will be needed, that we will make explicit in the security analysis.

5.1 Generating and masking secret isomorphisms

We start with describing how Algorithm 2 can be turned into a method for generating secret isomorphisms.

Heuristic claim 5.2 (Generating secret isomorphisms) *Let E and F be two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ with their endomorphism rings. Then, we can compute in expected polynomial time two other curves E' and F', their endomorphism rings and an isomorphism from $E \times F$ to $E' \times F'$ such that the distribution of the pair $(j(E'), j(F'))$ is heuristically undistinguishable from the uniform distribution on the pairs of supersingular j-invariants in $\mathbb{F}_{p^2}$.*

Our method for generating E' and F' in Heuristic 5.2 works as follows:

- We pick E' uniformly at random, using a random path of low-degree isogenies from E, and we compute its endomorphism ring from $\mathrm{End}(E)$ and the knowledge of the isogeny path.

- We run Algorithm 2 with input E, F, E' (and their endomorphism rings) to compute efficiently F' and an isomorphism from $E \times F$ to $E' \times F'$.
- The ring $\mathrm{End}(F')$ can be computed efficiently from the isomorphism $E \times F$ to $E' \times F'$.
- In the first two steps of Algorithm 2, we can use the randomized version of KLPT from [6, Algo. 5] at the cost of some heuristics. The curve F' is then obtained from a randomized isogeny. By using heuristics similar to those in SQIsign, we can assume F' is heuristically undistinguishable from uniformly random, see [6, Pb. 2], and that the algorithm runs in heuristic probabilistic polynomial time, see [6, Prop. 9].

Definition 5.3 (Height of an isomorphism) *Let E_1, E_2, E_1', E_2' be four supersingular elliptic curves over $\mathbb{F}_{p^2}$ and let φ be an isomorphism from $E_1 \times E_2$ to $E_1' \times E_2'$ given by a 2×2-matrix of isogenies (φ_{ij}). Then the* height *of φ, denoted by $\mathrm{ht}(\varphi)$ is the maximum degree of the defining isogenies:*

$$\mathrm{ht}(\varphi) = \max_{i,j \in \{1,2\}} \deg(\varphi_{ij}).$$

Lemma 5.4 *Let φ and ψ be two composable isomorphisms. Then*

$$\mathrm{ht}(\varphi\psi) \leq 4\,\mathrm{ht}(\varphi)\ \mathrm{ht}(\psi).$$

Proof. Composing the isomorphisms amounts to computing the product of the associated matrices. Each entry is of the form $\varphi_{i,1}\psi_{1,k} + \varphi_{i,2}\psi_{2,k}$. The degree of the composition of two isogenies is the product of their degrees. By the Cauchy-Schwartz inequality, the degree of the sum of two isogenies is bounded by 4 times the sum of their degrees. Therefore, each entry has a degree at most $4\,\mathrm{ht}(\varphi)\,\mathrm{ht}(\psi)$. □

In our protocol, we will need to transform an isomorphism of a given height into an isomorphism of a target (approximate) height, in such a way that is undistinguishable from a random isomorphism of this height.

Heuristic claim 5.5 (Masking with automorphisms) *Let E_1, E_2, E_1', E_2' be four supersingular elliptic curves over $\mathbb{F}_{p^2}$ of known endomorphism rings and let φ be an isomorphism from $E_1 \times E_2$ to $E_1' \times E_2'$ of height $\mathrm{ht}(\varphi) = H_\varphi$, given via an efficient representation. Let $H \gg H_\varphi$ be a target height. Then we can compute an efficient representation of another isomorphism ψ with the same domain and codomain, such that*

- $\mathrm{ht}(\psi) \approx H$,
- *ψ is undistinguishable from a uniform randomly chosen isomorphism of approximate height H, with the same domain and codomain.*

The construction supporting this claim is based on composing φ with a random automorphism of $E_1 \times E_2$ of appropriate height, namely $H/4H_\varphi$. By Lemma 5.4, the resulting automorphism is of height bounded by H, and we

expect it to be close to H. If not, we can try with another automorphism, possibly slightly increasing the height.

In order to produce such automorphisms, we can use the construction of Proposition 3.12, of the form $\begin{pmatrix} a & b\widehat{\iota} \\ c\iota & d \end{pmatrix}$, where ι is an isogeny from E_1 to E_2, and a, b, c, d are integers such that $ad - bc\deg(\iota) = \pm 1$. We call them *basic* automorphisms.

Since we know the ring of endomorphisms of E_1 and E_2, we can use [30, Algo. 5] to compute an isogeny ι whose degree is a power of a prime ℓ, that is a bounded by a power of p^κ for some constant κ. Then, for any μ, we can freely pick b and c in $O(\mu)$ and a and d of size in $O(\mu \deg(\iota))$ such that the condition holds. The resulting automorphism has height in $O(\mu \deg(\iota))$. We suggest to take μ polynomial in $\log p$.

Such automorphisms are very special, since their diagonal entries are integers. We will therefore compose a polynomial number of such automorphisms, changing ℓ, a, b, c, d, until we reach the height $H/4H_\varphi$. We remark that when two basic automorphisms are constructed from different ι isogenies, then their composition no longer has integral diagonal elements.

To conclude, we see that the target height H must be large enough compared to H_φ, so that we have room for composing φ with a polynomial number of basic automorphisms of heights that can not be smaller than what is obtained from [30, Algo. 5].

The isogenies forming the resulting automorphism ψ are obtained as sum of products of other isogenies, and we expect them to be random-looking, so that ψ is undistinguishable from random ones with the same height. In particular, we emphasize that efficient representations only give access to interpolation data, which do not reveal how the isogeny was constructed.

5.2 Protocol

We present an authentication protocol, where a prover can create a public key / secret key pair, then publish the public part, and subsequently can convince a verifier that they know the corresponding secret part. This protocol must be understood as a prototype, which does not really claims efficiency, except that it runs in polynomial time. The goal is to illustrate that Problem 5.1 opens new perspectives.

Therefore, we seek for simplicity. We follow the classical Sigma protocol structure, that we turn into a non-interactive one using the Fiat-Shamir transform.

Key generation. The prover starts by producing two random supersingular elliptic curves E_1 and E_2, together with their ring of endomorphisms. For this, they can create isogeny paths from the canonical curve E_0 to E_1 (resp. E_2) and transport the knowledge of the ring of endomorphisms.

Then, the prover applies Heuristic 5.2 to compute a pair of curves (E_1', E_2') with their endomorphism rings, and an isomorphism φ from $E_1 \times E_2$ to $E_1' \times E_2'$.

Public key: The 4 curves E_1, E_2, E'_1, E'_2, together with their endomorphism rings.
Secret key: The isomorphism $\varphi : E_1 \times E_2 \to E'_1 \times E'_2$.

Basic interactive protocol. This is a classical Sigma protocol, with the three phases: commit, challenge, response, that we describe in turn.
Commit phase:

The prover applies Heuristic 5.2 to produce two curves E_3 and E_4 with their endomorphism rings, and an isomorphism $\varphi_0 : E_1 \times E_2 \to E_3 \times E_4$.

The prover applies again Heuristic 5.2 to produce two curves E'_3 and E'_4 with their endomorphism rings, and an isomorphism $\varphi_1 : E'_1 \times E'_2 \to E'_3 \times E'_4$.

Finally, the prover computes the composition of the transpose of φ_0, φ and φ_1, and masks it using automorphisms. This produces an isomorphism $\psi : E_3 \times E_4 \to E'_3 \times E'_4$.

The prover sends E_3, E_4, E'_3 and E'_4 with their endomorphism rings, together with ψ, to the verifier.
Challenge phase:

The verifier picks a random bit b and sends it to the prover.
Response phase:

The prover masks φ_b with automorphisms and sends it to the verifier.

The verifier checks that the following holds:

- ψ is indeed an isomorphism between $E_3 \times E_4$ and $E'_3 \times E'_4$;
- φ_b is indeed an isomorphism between the products of curves corresponding to the challenge bit b.

Overall protocol. The basic protocol provides only one bit of soundness. It is then repeated λ times, where λ is a security parameter.

The overall protocol is obtained by combining these λ repetitions in a single non-interactive protocol with the Fiat-Shamir transform: the prover produces λ independent commits, then the challenge is computed as the result of hashing all these commits together with the context of the proof, and then the prover computes the corresponding responses.

5.3 Security analysis

We conclude with a brief security analysis of the presented protocol. In the first part we show that the soundness essentially relies on the computational hardness of Problem 5.1. Then we will describe a simulator to establish the zero-knowledge property, under some heuristics.

Soundness. The basic protocol has the special soundness property: for a given commit, if the prover is able to answer to the two possible challenges, then by computing the composition of φ_0, ψ, and the transpose of φ_1, it can get an isomorphism between $E_1 \times E_2$ and $E'_1 \times E'_2$.

Therefore, if Problem 5.1 is hard, then the protocol is sound.

Zero-knowledge. Let us consider the following simulator S. It starts by picking a bit b uniformly at random. If $b = 0$ (resp. $b = 1$), then S applies Heuristic 5.2 to the pair (E_1, E_2) (resp. (E'_1, E'_2)) to produce a new pair of curves (E_3, E_4) (resp. (E'_3, E'_4)) with their ring of endomorphisms, and an isomorphism φ_b. Then, it applies again Heuristic 5.2 to (E_3, E_4) (resp. (E'_3, E'_4)) to produce (E'_3, E'_4) (resp. (E_3, E_4)) with their ring of endomorphisms, and an isomorphism ψ between those two products of curves.

If $b = 1$, then ψ is replaced by its transpose, so that in both cases, we have an isomorphism from (E_3, E_4) to (E'_3, E'_4).

Finally, S masks φ_b and ψ so that they have the expected height, and returns the transcript corresponding to this data.

The assumptions under which this transcript is undistinguishable from one of a real run of the protocols are the following:

- Both curves output by the algorithm from Heuristic 5.2 are undistinguishable from uniformly random.
- The masking by automorphisms strategy indeed produces an isomorphism that is undistinguishable from uniformly random.

References

1. Basso, A., Dartois, P., Feo, L.D., Leroux, A., Maino, L., Pope, G., Robert, D., Wesolowski, B.: SQIsign2D-West: The fast, the small, and the safer. In: ASIACRYPT 2024. pp. 339–370 (2024)
2. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Advances in Cryptology – EUROCRYPT 2023. pp. 423–447 (2023)
3. Dartois, P.: Fast computation of 2-isogenies in dimension 4 and cryptographic applications. Cryptology ePrint Archive, Paper 2024/1180 (2024), `https://eprint.iacr.org/2024/1180`
4. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQIsignHD: New dimensions in cryptography. In: Advances in Cryptology – EUROCRYPT 2024. pp. 3–32 (2024)
5. Dartois, P., Maino, L., Pope, G., Robert, D.: An algorithmic approach to (2, 2)-isogenies in the theta model and applications to isogeny-based cryptography. In: Advances in Cryptology – ASIACRYPT 2024. pp. 304–338 (2025)
6. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: compact post-quantum signatures from quaternions and isogenies. In: ASIACRYPT 2020. pp. 64–93 (2020)
7. Eriksen, J., Panny, L., Sotáková, J., Veroni, M.: Deuring for the people: Supersingular elliptic curves with prescribed endomorphism ring in general characteristic. Contemporary Mathematics **796**, 339–373 (2024)
8. Fité, F., Sutherland, A.V.: Sato-Tate groups of $y^2 = x^8 + c$ and $y^2 = x^7 - cx$. Frobenius distributions: Lang-Trotter and Sato-Tate conjectures **663**, 103–126 (2016)
9. Jordan, B.W., Keeton, A.G., Poonen, B., Rains, E.M., Shepherd-Barron, N., Tate, J.T.: Abelian varieties isogenous to a power of an elliptic curve. Compositio Mathematica **154**(5), 934–959 (2018)
10. Kani, E.: Products of CM elliptic curves. Collectanea mathematica **62**(3), 297–339 (2011)

11. Kani, E.: The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. Journal of Number Theory **139**, 138–174 (2014)
12. Kirschmer, M., Voight, J.: Algorithmic enumeration of ideal classes for quaternion orders. SIAM Journal on Computing **39**(5), 1714–1747 (2010)
13. Kohel, D., Lauter, K., Petit, C., Tignol, J.P.: On the quaternion ℓ-isogeny path problem. LMS Journal of Computation and Mathematics **17**, 418–432 (2014)
14. Leroux, A.: A new isogeny representation and applications to cryptography. In: ASIACRYPT 2022. pp. 3–35 (2022)
15. Leroux, A.: Quaternion algebras and isogeny-based cryptography. Ph.D. thesis (2022)
16. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Advances in Cryptology – EUROCRYPT 2023. pp. 448–471 (2023)
17. Merdy, A.H.L., Wesolowski, B.: The supersingular endomorphism ring problem given one endomorphism. arXiv preprint arXiv:2309.11912 (2023)
18. Nguyen, P.Q., Stehlé, D.: Low-dimensional lattice basis reduction revisited. ACM Transactions on algorithms (TALG) **5**(4), 1–48 (2009)
19. Onuki, H., Nakagawa, K.: Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign. In: Advances in Cryptology – ASIACRYPT 2024. pp. 243–271 (2025)
20. Page, A., Robert, D.: Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time. Cryptology ePrint Archive, Paper 2023/1766 (2023), `https://eprint.iacr.org/2023/1766`
21. Page, A., Wesolowski, B.: The supersingular endomorphism ring and one endomorphism problems are equivalent. In: EUROCRYPT 2024. pp. 388–417 (2024)
22. Robert, D.: Breaking SIDH in polynomial time. In: EUROCRYPT 2023. pp. 472–503 (2023)
23. Robert, D.: On the efficient representation of isogenies. In: NUTMIC 2024: Number-Theoretic Methods in Cryptology (2024)
24. Shioda, T.: Supersingular K3 surfaces. In: Algebraic Geometry, Summer meeting. pp. 564–591 (1979)
25. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate texts in mathematics, Springer (2009)
26. Storjohann, A.: Algorithms for matrix canonical forms. Ph.D. thesis, ETH Zurich (2000)
27. Vignéras, M.F.: Arithmétique des algèbres de quaternions. Springer (1980)
28. Voight, J.: Quaternion Algebras. Springer (2021)
29. Waterhouse, W.C.: Abelian varieties over finite fields. Annales scientifiques de l'École normale supérieure **2**(4), 521–560 (1969)
30. Wesolowski, B.: The supersingular isogeny path and endomorphism ring problems are equivalent. In: FOCS 2021. pp. 1100–1111. IEEE (2021)