A Note on Splittings and Endomorphisms

Péter Kutas[1,2] and Min-Yi Shen[3]

[1] Eötvös Loránd University, Hungary
[2] University of Birmingham, United Kingdom
[3] No Affiliation

Changes:

1. A more clear definition of the Splitting problem and the correction of Proposition 3.
2. Section 4 is incorrect (see p. 10), but we keep it in the current version for future work.

Abstract. Finding a nontrivial endomorphism of a given supersingular elliptic curve is a hardness assumption of isogeny-based cryptography. We prove the reduction from it to the problem of finding a splitting of a given principally polarized abelian surface. By using this new reduction, we also prove the heuristic equivalence of the splitting problem with a degree restriction and the endomorphism ring problem in dimension two.

Keywords: endomorphism rings · splittings · reductions

1 Introduction

Computing the endomorphism ring of a given supersingular elliptic curve (`EndRing` problem) is a well-studied problem in computational number theory, and it also forms a hardness assumption of one-dimensional isogeny-based cryptography. One can show that `EndRing` is equivalent to finding a single non-scalar endomorphism of the supersingular elliptic curve (`OneEnd` problem) [PW24]. There exist several methods to solve the latter problem by finding a non-trivial cycle in the one-dimensional ℓ-isogeny graph, for example, [DG16, FIK+25].

In dimension two, finding an isogeny between two given superspecial principally polarized abelian surfaces (PPAS) A and B is also a hard algorithmic problem (as 1-dimensional isogeny finding naturally reduces it). The best known attack, the Costello-Smith algorithm [CS20], works as follows: First find two splitting isogenies (i.e., a polarized isogeny to a product of two supersingular elliptic curves) $F_A\colon A \to E_1 \times E_2$ and $F_B\colon B \to E_3 \times E_4$, and seeking an ℓ^a-isogenies $\phi\colon E_1 \to E_3$ and an ℓ^b-isogeny $\psi\colon E_2 \to E_4$. If $a \equiv b \mod 2$, then one can combine ϕ and ψ to a two-dimensional path between A and B [CS20, Lemma 3]. The most costly step in the Costello-Smith algorithm is walking to a product surface, which has $O(p)$ runtime, that is essentially the total asymptotic runtime of the full algorithm. This motivates the algorithmic problem of finding a splitting isogeny which is formalized as `Splitting` (Remark 5) in this paper. Note that the Costello-Smith algorithm is also the best method for g-dimensional path-finding ($g \geqslant 2$), so one can also consider the higher dimensional splitting problems.

E-mail: kutasp@gmail.com (Péter Kutas), min.yi.shen0403106@gmail.com (Min-Yi Shen)

This work is licensed under a "CC BY 4.0" license.
Date of this document: 2026-10-12.

In most constructions, one tends to consider chains of good isogenies, that is $\ker(f_{i+1}) \cap \ker(\tilde{f}_i) = \{0\}$ where $\tilde{f}_i$ is the adjoint isogeny of f_i (see Subsection 2.2); otherwise, the constructions might be insecure, e.g., the collision attack [FT19] on the first 2-dimensional CGL-hash function [Tak17]. Hence, it's natural to consider good splittings. In [KS26], Kunzweiler and Shen proved the reductions from `OneEnd` and `Isogeny` to `GoodSplitting` (Definition 13), that is to find a good (w.r.t. a given isogeny) isogeny from a given Jacobian of a genus-2 curve to a product of elliptic curves. As an application of the ideas and algorithms, they also pointed out a potential connection between the splitting problem and finding a nontrivial endomorphism of a given superspecial PPAS.

One drawback of [KS26] is that best known algorithms for `OneEnd` have heuristic complexity $O(\sqrt{p})$ whereas the best known algorithm for finding a splitting (a straightforward random walk, until one hits a product surface) has heuristic complexity $O(p)$. Thus one questions whether there exist faster algorithms for `Splitting` than $O(p)$ which would have a major impact on 2-dimensional endomorphism ring computations. Furthermore, [KS26] requires a very specific oracle (that produces a good splitting), so it is also natural to ask whether one could also provide reductions with a less restrictive oracle.

Our contribution

In this work, we show the four reductions — the teal arrows in Figure 1. The first two reductions are from `OneEnd` to `Splitting` (Proposition 3) and from `Isogeny` to `Splitting` (Proposition 4) which eliminates the requirement of a good extension in [KS26]. Second, we prove that `EndRing2` is equivalent to ℓ-`Splitting` under GRH and the assumptions of KLPT^2 (Proposition 5 and Proposition 6). Note that the best known algorithm [CS20] for `EndRing2` has complexity $O(p)$ which matches the best known complexity of `Splitting` (for a survey on the problem, see [FIK+25]).

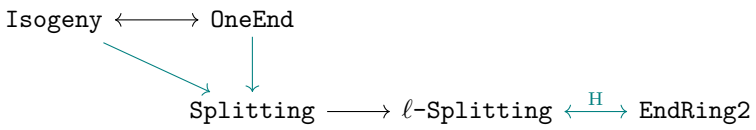

Figure 1: Relation among different hardness assumptions in isogeny-based cryptography. The word 'H' means GRH and the assumptions of KLPT^2.

Outline

In Section 2, we recall the results from literature regarding endomorphisms, the hardness assumptions and KLPT^2. In Section 3, we define more general splitting problems and show that we can remove the 'good' restriction used in [KS26]. In Section 4, we prove the equivalence of `EndRing2` and ℓ-`Splitting` under GRH and KLPT^2 assumptions.

Acknowledgments. Péter Kutas is partly supported by EPSRC through grant number EP/V011324/1 and by the Hungarian Ministry of Innovation and Technology NRDI Office within the framework of the Quantum Information National Laboratory Program. Kutas is also supported by the grant "EXCELLENCE-151343". Min-Yi Shen thanks Péter Kutas for everything, and he also thanks Mohammed Alshawki, Kouider Fatna, Péter Ligeti, Ádám Nagy, István Seres and Viktória Villányi for the welcoming atmosphere at ELTE.

2 Preliminaries

Throughout this paper, we focus on supersingular elliptic curves and superspecial principally polarized abelian surfaces. $p \notin \{2, 3\}$ is a prime and q is a p-power.

2.1 Elliptic Curves and Deuring Correspondence

Elliptic curve is itself a fruitful area, we refer to [Sil09] for a complete introduction.

Definition 1. An *elliptic curve* E defined over $\mathbb{F}_q$ is a smooth projective curve of genus one with a point at infinity 0_E. Given two elliptic curves E_1 and E_2, an *isogeny* is a nonconstant morphism $\phi\colon E_1 \to E_2$ such that $\phi(0_{E_1}) = 0_{E_2}$. The *degree* of ϕ is its degree as a rational map; if an isogeny has degree d, we call it a *d-isogeny*.

Concretely, every elliptic over $\mathbb{F}_q$ of characteristic $p > 3$ admits a *short Weierstraß equation* $y^2 = x^3 + Ax + B$ for some $A, B \in \mathbb{F}_q$. The *j-invariant* is defined as

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Two elliptic curves are isomorphic over $\overline{\mathbb{F}_q}$ if and only if they have the same j-invariant [Sil09, III Proposition 1.4].

An isogeny from E to itself is called an *endomorphism*. The set containing all endomorphism of E and the zero map is denoted by $\mathrm{End}(E)$. One can prove that $\mathrm{End}(E)$ is a ring, and therefore call it the *endomorphism ring*. Note that $\mathrm{End}(E)$ always contains the multiplication-by-n map $[n]$ for every $n \in \mathbb{Z}$; its kernel, denoted by $E[n]$ is called the *n-torsion group*. By [Sil09, V.3 Theorem 3.1], $E[p^r]$ is either trivial or $\mathbb{Z}/p^r\mathbb{Z}$ for $r \geqslant 1$; for the former (resp. latter) case, E is said to be *ordinary* (resp. *supersingular*). In this paper, we focus on supersingular elliptic curves.

An important object studied in one-dimensional isogeny-based cryptography is *ℓ-isogeny graph*: the vertices are isomorphic representatives of supersingular elliptic curves (could be j-invariants) and the edges are ℓ-isogenies for some prime $\ell \neq p$. The best known algorithms (e.g. [DG16, FIK+25]) to find a nontrivial endomorphism of an elliptic curve rely on different methods to find a nontrivial circle in an ℓ-isogeny graph.

Because supersingular elliptic curves have a strong connection with quaternion world, we briefly recall some definitions in quaternion algebra, we refer to [EPSV23] for the detailed descriptions of quaternions, Deuring correspondence and KLPT algorithm.

A *quaternion algebra* $\mathfrak{B}_{\alpha,\beta}$ over $\mathbb{Q}$ is a four-dimensional central simple algebra over $\mathbb{Q}$; it has a $\mathbb{Q}$-basis $\{1, i, j, ij\}$ where $i^2 = -\alpha$, $j^2 = -\beta$ and $ij = -ji$. There is a well-known involution, called *conjugation* $\bar{\cdot}$, and it is defined as $\bar{\alpha} = w - xi - yj - zij$ where $\alpha = w + xi + yj + zij$. We also define the *reduced norm* as $\mathrm{nrd}(\alpha) = \alpha\bar{\alpha}$.

An *order* is a subring in a quaternion algebra which has full rank as a $\mathbb{Z}$-module. An *ideal* is a rank-4 $\mathbb{Z}$-module in a quaternion algebra. Given an order $\mathcal{O}$ and an ideal I, the *left order* of I is defined as $\mathfrak{O}_L(I) \coloneqq \{\beta \in \mathfrak{B} \mid \beta I \subseteq I\}$, and the *right order* $\mathfrak{O}_R(I)$ is defined similarly. We say I is a *left (resp. right) $\mathcal{O}$-ideal* if $\mathcal{O} \subseteq \mathfrak{O}_L(I)$ (resp. $\mathcal{O} \subseteq \mathfrak{O}_R(I)$). Two left $\mathcal{O}$-ideal I and J are equivalent if there is a nonzero $\beta \in \mathfrak{B}_{p,\infty}$ such that $J = I\beta$. The *norm* of an ideal I is defined as $n(I) \coloneqq \gcd\{\mathrm{nrd}(u) \mid u \in I\}$.

In dimension one, finding an isogeny between two given elliptic curves and finding the endomorphism ring of a given elliptic curve are the well-known hardness assumptions. The quaternion analog of the former assumption was solved thanks to *Deuring correspondence* [Deu41] and *KLPT* algorithm [KLPT14].

Recall that $\mathrm{End}(E)$ of a supersingular $E/\mathbb{F}_{p^2}$ is isomorphic to a maximal order in $\mathfrak{B}_{p,\infty}$. Moreover, the degree of an endomorphism matches the reduced norm of the corresponding quaternion.

The Deuring correspondence builds an equivalence between the following two categories: category of supersingular elliptic curves over $\overline{\mathbb{F}_p}$ (up to Galois conjugation), and category of maximal orders in $\mathfrak{B}_{p,\infty}$ (up to isomorphism). An isogeny $\varphi\colon E_0 \to E_1$ corresponds to an ideal $I \subseteq \mathfrak{B}_{p,\infty}$ which is a left (resp. right) ideal of $\mathcal{O}_0 \cong \mathrm{End}(E_0)$ (resp. $\mathcal{O}_1 \cong \mathrm{End}(E_1)$). Under such correspondence, there is a quaternion analog of isogeny-finding problem: given two maximal orders, connected by an ideal I, in $\mathfrak{B}_{p,\infty}$, can one find an ideal J equivalent to I (together with a norm restriction)? This problem was addressed by the KLPT algorithm and its generalizations (e.g. [DFKL+20]).

2.2 Principally Polarized Abelian Varieties and Isogenies

Abelian variety is also a huge topic, for the details, we refer to [Mil08] and [Mum74].

A complete connected group variety is called an *abelian variety*, one can show that its group structure is commutative (by using rigidity) and it is projective. Given an abelian variety A, denote by $\hat{A} \cong \mathrm{Pic}^0(A)$, consisting of divisor classes whose divisors are algebraically equivalent to 0, its *dual abelian variety*.

Definition 2. An *isogeny* $\phi\colon A \to B$ between two abelian varieties is a morphism (between abelian varieties) such that it is surjective and its kernel is finite.

Definition 3. Consider an abelian variety A, a *polarization* is an isogeny $\lambda\colon A \to \hat{A}$ defined by $P \mapsto [t_{-P}(D) - D]$ where D is an ample divisor and t_{-P} is the translation-by-$-P$ map. The *degree* of a polarization is its degree as an isogeny. A polarization is said to be *principal* if it is of degree one.

We need the higher-dimensional analog of 'supersingularity of elliptic curve", one can find the discussion in [CDS20, Section 2] for the notion of superspeciality and supersingularity in higher dimensions. As a result, we focus on *superspecial* PPAV which is defined as follows.

Definition 4. A g-dimensional abelian variety is said to be *superspecial* if it is isomorphic to a product of g supersingular elliptic curves as an unpolarized variety.

An isogeny between abelian varieties is defined above, but we also need isogenies which are compatible with the polarizations.

Definition 5. An isogeny $f\colon (A, \lambda_A) \to (B, \lambda_B)$ between PPAV is said to be *polarized* if there exists $N \in \mathbb{N}$ such that the following diagram commutes

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle [N]\lambda_A}\downarrow & & \downarrow{\scriptstyle \lambda_B} \\ \hat{A} & \xleftarrow[\hat{f}]{} & \hat{B} \end{array}$$

This N is called the *reduced degree* of f and denoted by $\mathrm{rdeg}(f)$. Two principal polarizations λ_1 and λ_2 on an abelian variety A are said to be *equivalent* if there exists a polarized $\alpha \in \mathrm{Aut}(A)$ such that $\hat{\alpha}\lambda_1\alpha = \lambda_2$.

Every isogeny $\phi\colon A \to B$ between abelian varieties admits a *dual isogeny* $\hat{\phi}\colon \hat{B} \to \hat{A}$. Regarding an isogeny $\psi\colon (A, \lambda) \to (B, \lambda_B)$ between PPAV, we can define the *adjoint isogeny* $\tilde{\psi}\colon B \to A$ by $\lambda_A^{-1} \circ \hat{\psi} \circ \lambda_B$. We have $\psi\tilde{\psi} = [\mathrm{rdeg}\,\psi]_B$ and $\hat{\psi}\psi = [\mathrm{rdeg}\,\psi]_A$. Note that in dimension one, the two definitions match via the canonical polarization, but this fails in higher dimensions. Thus, for a higher-dimensional isogeny between PPAV, we fix $\tilde{\cdot}$ for its adjoint isogeny, and $\hat{\cdot}$ for its dual isogeny.

In dimension two, we know (see, e.g., [Rü90, p. 354]) that we have two flavors of PPAS defined over an algebraically closed field: products of elliptic curves (*reducible*) and Jacobians of genus-2 curves (*irreducible*).

Let $f\colon A \to B$ be an isogeny bewteen PPAS. We say f is an (N,N)-*isogeny* if $\ker(f) \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. We also note that an isogeny is determined by its kernel up to isomorphism. Consider an (N_1,N_1)-isogeny $f_1\colon A \to B$ and an (N_2,N_2)-isogeny $f_2\colon B \to C$ between PPAS, we say f_2 is a *good extension of* f_1 if $f_2 \circ f_1$ is an (N_1N_2, N_1N_2)-isogeny.

2.3 Hardness Assumptions

In this subsection, We define most hardness assumptions discussed in this paper. To make 'find' concrete, we admit the definitions of *representation* from [ABI+25].

Definition 6. Let $\varphi\colon A \to B$ be an isogeny between two AV defined over $\mathbb{F}_q$. An *efficient representation* of φ with respect to a given algorithm is some data $D_\varphi \in \{0,1\}^*$ such that, on input D_φ and $P \in A(\mathbb{F}_q)$, the algorithm returns the evaluation $\varphi(P)$ in polynomial time in length of D_φ and $\log q$.

To address polarizations, we also consider the following definition from [Mon26], which is slightly different from the original form in [ABI+25].

Definition 7. A *good representation* for an isogeny $\varphi\colon (A,\lambda_A) \to (B,\lambda_B)$ between PPAV is a tuple $(r, r^\dagger, D, r^*)$ where r is an efficient representation of φ, $r^\dagger$ is an efficient representation of $\varphi^\dagger = \lambda_A^{-1} \circ \hat{\varphi} \circ \lambda_B$, D is an integer such that $\mathrm{tr}(\varphi \circ \varphi^\dagger) \leqslant D$, and r^* is a matrix representing the $\mathbb{F}_q$-linear map $H^0(B,\Omega_B) \to H^0(A,\Omega_A)$ by φ w.r.t. any bases of these vector spaces.

We define the following one-dimensional hardness assumptions.

Definition 8. (`Isogeny`) Given two supersingular elliptic curves E and E', find an efficient representation of an isogeny from E to E'.

Definition 9. (`OneEnd`) Given a supersingular elliptic curve E, find an efficient representation of a nontrivial endomorphism of E.

Definition 10. (`EndRing`) Given a supersingular elliptic curve E find efficient representations of 4 endomorphisms of E that generate $End(E)$ as a $\mathbb{Z}$-lattice.

Remark 1. Assume GRH, given a supersingular E, there is a polynomial time algorithm to compute a good representation of $\mathrm{End}(E)$ from an efficient representation of it [Mon26, Lemma 2.19].

Remark 2. Computing endomorphism rings for supersingular elliptic curves can usually mean two things. The algebraic version (called MaxOrder in [Wes22]) asks to compute the maximal order in $B_{p,\infty}$ that is isomorphic to the endomorphism ring of the given supersingular elliptic curve. In Definition 10 we chose the geometric definition of the endomorphism ring problem. As it turns out the two problems are polynomial-time equivalent [Wes22].

`OneEnd` and `EndRing` are indeed equivalent by [PW24]. More precisely, if one is provided with an oracle for `OneEnd` that can be called on any supersingular elliptic curve, then one can also compute the endomorphism ring of any supersingular elliptic curve. If one is only given one elliptic curve with one non-scalar endomorphism, then there is still no known polynomial-time algorithm that computes the full endomorphism ring (which underlies the security of CSIDH [CLM+18] and other group-action protocols [DEF+25], [FFK+23],[CLP24],[ABE+25]).

Next we will define the endomorphism ring problem for principally polarized superspecial abelian surfaces. Here we will concentrate on the geometric version and much later we will define an algebraic version.

Definition 11. (`EndRing2`) Given a principally polarized superspecial abelian surface, compute a collection of endomorphisms with a good representation that generate the endomorphism ring as $\mathbb{Z}$-lattice.

Regarding the endomorphism ring of a given PPAS, we refer to [ABI+25] for a complete and detailed analysis for all cases.

Naturally, there is also an analogue of finding isogenies between superspecial surfaces:

Definition 12. (`IsogenyPath2`) Given two principally polarized superspecial surfaces, find a chain of (ℓ, ℓ)-isogenies connecting the two surfaces.

A heuristic polynomial-time equivalence between `EndRing2` and `IsogenyPath2` was proven in [CDK+25]. The best algorithm for computing a chain of (ℓ, ℓ)-isogenies between two PPASs is to find a path to a product surface from both abelian surfaces. Finding a chain of (ℓ, ℓ)-isogenies between two products can essentially be accomplished via 1-dimensional pathfinding algorithms. This approach is extensively studied in [CS20].

In [CS20] they take a random walk to find a problem which has complexity $O(p)$ as the density of products among all superspecial surfaces is $O(1/p)$. This naturally motivates the question whether there exists a more conceptual algorithm to find a path to a product. This would have natural consequences for `IsogenyPath2` and `EndRing2` as this is asymptotically the slowest step of the Costello-Smith algorithm [CS20].

2.4 Endomorphisms via Splittings

Finding an isogeny to a product is called the `Splitting` problem. The complexity of `Splitting` is studied in [KS26]. In this paper, the authors assume that they have an oracle that can compute a splitting isogeny from any superspecial surface. Due to technical reasons (which will be evident a bit later) one naturally has to enforce restrictions on this splitting oracle. In [KS26] the authors restrict to an oracle that returns a "good splitting":

Definition 13. (`GoodSplitting`) Given a principally polarized abelian surface A and a maximal m-isotropic group $K \subset A[m]$ for some integer $m \in \mathbb{N}$, find an efficient representation of a good (N, N)-splitting $F \colon A \to E_1 \times E_2$ for some N. By 'good', we mean that $K \cap \ker(F) = \{0\}$.

The main result of [KS26] is that finding a good splitting is at least as hard as `OneEnd` (which is equivalent to `EndRing`). Now we briefly recall the main idea of [KS26]. First, by applying a suitable automorphism of $E \times E'$ [KS26, Lemma 3.2], one could construct a $(2, 2)$-gluing isogeny $f \colon E \times E' \to A$ where A is irreducible, and $E \times E'$ is the same surface but with a different theta structure. Suppose we find a good (N, N)-splitting isogeny $g \colon A \to E_1 \times E_2$, then by Kani's lemma, there is an explicit correspondence between the matrix form of the $(2N, 2N)$-product isogeny $F := g \circ f \colon E \times E' \to E_1 \times E_2$ and a commutative diagram.

$$F := \begin{pmatrix} \phi_1 & \hat{\psi}_2 \\ -\phi_2 & \hat{\psi}_1 \end{pmatrix}, \qquad \begin{array}{ccc} E & \xrightarrow{\phi_1} & E_1 \\ \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \psi_2} \\ E_2 & \xrightarrow{\psi_1} & E' \end{array}$$

Under this construction, $\psi_2 \circ \phi_1$ is nonzero [KS26, Proposition 4.8], i.e., a solution to `Isogeny`. In particular, when $E = E'$, $\psi_2 \circ \phi_1$ is nontrivial [KS26, Proposition 4.10], i.e., a solution to `OneEnd`.

Remark 3. This shows two limitations of [KS26]. Even though `OneEnd` is an established hard problem, the best known algorithm for `OneEnd` have complexity $O(\sqrt{p})$ whereas the

best known algorithm for splitting has complexity $O(p)$. The second problem is that the oracle is very restrictive. In particular, even if endomorphism rings are known, it is not yet clear how one can instantiate a good splitting oracle (a particular limitation of [CDK+25]).

In Section 3 we will show a way how to remove this restriction (and will also demonstrate why some restriction is necessary).

2.5 Rosati Involution and Ibukiyama-Katsura-Oort Matrix

E_0 is a supersingular elliptic curve with known endomorphism ring $\mathrm{End}(E_0)$, which is isomorphic to a maximal order $\mathcal{O}_0$ in the quaternion algebra $\mathfrak{B}_{p,\infty}$. All superspecial abelian surfaces over a finite field are all isomorphic to $A_0 := E_0 \times E_0$ without considering the polarizations. Therefore, their endomorphism rings are all isomorphic. This provides an algebraic difficulty in assigning algebraic objects to principally polarized superspecial surfaces.

The key insight is that you have to incorporate the principal polarization into your algebraic data. As a ring, you can view your endomorphism ring as $M_2(\mathcal{O}_0)$. The additional information is going to be a positive involution on $M_2(\mathcal{O}_0)$ that encodes the principal polarization, called the Rosati involution:

Definition 14. Let (A, λ) be a PPAV, the adjoint operator $\mathrm{Ros}_\lambda \colon \alpha \to \lambda^{-1}\hat{\alpha}\lambda$ defines an involution on $\mathrm{End}(A)$. It is called the *Rosati involution (w.r.t. λ)*.

Given a PPAS (A, λ_A), we know that $(A, \lambda_A) \cong (A_0, \lambda)$ for some λ; in particular, if one knows an unpolarized isomorphism $\varphi \colon A_0 \to A$, then one can set $\lambda = \hat{\varphi}\lambda_A\varphi$. Therefore, classifying principal polarizations on A_0 up to equivalence (Definition 5) is equivalent to classifying superspecial PPAS up to (polarized) isomorphism. The method thanks to Ibukiyama, Katsura and Oort [IKO86] describes a PP λ on A_0 as a matrix with coefficients in $\mathcal{O}_0$: Let λ_0 be the product polarization on A_0, and $\mu \colon \lambda \mapsto \lambda_0^{-1}\lambda$ be a map from the set of PP on A_0 up to equivalence to $\mathrm{End}(A_0) \cong M_2(\mathcal{O}_0)$.

Theorem 1. *([CDK+25, Theorem 2.7]) The map μ defined above is injective, and its image transferred to the quaternion world through Deuring correspondence, is*

$$\mathrm{Mat}(A_0) := \left\{ \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix} \;\middle|\; s, t \in \mathbb{N},\ r \in \mathcal{O}_0,\ st - r\bar{r} = 1 \right\} \subset \mathrm{GL}_2(\mathcal{O}_0).$$

Given a PPAS $(A, \lambda_A) \cong (A_0, \lambda)$, we write $\mu(\lambda) \in \mathrm{Mat}(A_0)$ for its image under μ, and call it the *Ibukiyama-Katsura-Oort (IKO) matrix of A*. Two PP λ and λ' on A_0 are equivalent iff there exists $\gamma \in \mathrm{GL}_2(\mathcal{O}_0)$ such that $\gamma^*\mu(\lambda')\gamma = \mu(\lambda)$. So $\mu(\lambda)$ is only defined up to equivalence in $\mathrm{Mat}(A_0)$.

Remark 4. The IKO correspondence now defines an algebraic version of `EndRing2`. Namely, given a superspecial surface, find a corresponding IKO matrix (note that there are infinitely many options here as a g matrix is only defined up to an equivalence relation).

2.6 KLPT^2

KLPT^2 [CDK+25] is a two-dimensional analog of the KLPT algorithm [KLPT14], which is one of the milestones in isogeny-based cryptography.

We recall the main equation [CDK+25, Subsection 2.3]. Given two PPAS (A_0, λ_1) and (A_0, λ_2), the goal is to find a connecting polarized isogeny φ of reduced degree N. Note that $\varphi \in \mathrm{End}(A_0) \cong M_2(\mathcal{O}_0)$, so we can identify it with $\gamma \in M_2(\mathcal{O}_0)$. Denoted by $g_1, g_2 \in \mathrm{Mat}(A_0)$ the IKO matrices of the two PPAS. Then the property of being polarized isogeny provides the main equation as follows:

$$\hat{\varphi}\lambda_2\varphi = N\lambda_1 \;\Rightarrow\; (\lambda_0^{-1}\hat{\varphi}\lambda_0)\lambda_0^{-1}\lambda_2\varphi = N\lambda_0^{-1}\lambda_1 \;\Rightarrow\; \gamma^* g_2 \gamma = N g_1$$

where $\lambda_0^{-1}\lambda_i = g_i$.

Thus in this setting the algebraic pathfinding problem for superspecial surfaces can be described as follows. One is provided with matrices g_1, g_2 and one has to find $\gamma \in M_2(\mathcal{O})$ such that $\gamma^* g_2 \gamma = N g_1$ for some fixed N. Depending on the application, N is either a power of a small prime ℓ, or is a powersmooth number. The latter is useful in establishing an effective version of the IKO correspondence. Namely, KLPT^2 can be used to translate an IKO matrix into a superspecial surface in polynomial time. In general, [CDK+25] solves the algebraic pathfinding problem in the case where $N > p^{25}$ which has been recently improved by Page, Robert and Soumier [PRS26].

Furthermore, [CDK+25] also contains results relevant to this paper outside of algebraic pathfinding. Namely, given a superspecial surface with its IKO matrix and a polarized isogeny, one can compute the corresponding γ matrix in polynomial time assuming the degree of the polarized isogeny is smooth [CDK+25, Algorithm 6]. This is called the `IsogenyToMatrix` algorithm which is the 2-dimensional analogue of the isogeny-to-ideal algorithm for supersingular elliptic curves. Note that even in the 1-dimensional case, there is no known classical polynomial-time algorithm for this problem (but there is a quantum polynomial-time one [CII+23]).

2.7 Endomorphism Rings and IKO Matrices

As mentioned before, the two-dimensional endomorphism ring problem for superspecial abelian surfaces can be stated in a geometric and algebraic manner. The geometric way requires a representation of a $\mathbb{Z}$-basis of the endomorphism ring that one can evaluate efficiently whereas the algebraic version requires finding the associated IKO matrix.

In the 1-dimensional setting such an equivalence is almost automatic from the KLPT algorithm. In higher dimensions, there are some technical difficulties that have to be handled. This was recently accomplished in concurrent work by Montessinos [Mon26] and Page, Robert, Soumier [PRS26]. Here is the appropriate theorem from [Mon26]:

Proposition 1. *([Mon26, Theorem 6.9 and Proposition 4.2]) Given a superspecial PPAS A. Under GRH and KLPT^2 heuristics, computing its IKO matrix is equivalent to computing a good representation of* $\mathrm{End}(A)$.

In Section 3 we will encounter a situation where we have two elliptic curves E_1, E_2 of known endomorphism ring and our goal is finding the IKO matrix associated to $E_1 \times E_2$ (with respect to the product polarization). Now Proposition 1 implies that is enough to find an generators of $End(E_1 \times E_2)$ that one can evaluate efficiently. This is luckily handled by the following lemma:

Proposition 2. *([Mon26, Proposition 4.1]) Under GRH, there is a polynomial time algorithm taking supersingular E_1, E_2 and an efficient representation of* $\mathrm{End}(E_1 \times E_2)$ *as input, and returns a good representation of* $\mathrm{End}(E_1 \times E_2)$.

3 Removing the 'Good' Restriction

Kunzweiler et al. [KS26] proved the reductions from `OneEnd` and `Isogeny` to `GoodSplitting` by using the idea introduced in Subsection 2.4. However, to invoke Kani's lemma, the results are based on good isogenies. The 'good' restriction is not that artificial, but it restricts the usage and applications of the reductions. In this subsection, we prove that the reductions to the more general `Splitting` are possible.

We now define a more general `Splitting` problem. First, we would like to exclude the 'trivial' splittings — the splittings which can be generated without additional information. Given a supersingular elliptic curve E, one can construct many polarized product isogenies

from $E \times E$ without any oracle: Consider two isogeny $\varphi_1 \colon E \to E_1$ and $\varphi_2 \colon E \to E_2$ of the same degree, we can construct a polarized product isogeny

$$\begin{pmatrix} a\varphi_1 & \pm b\varphi_1 \\ b\varphi_2 & \mp a\varphi_2 \end{pmatrix} : E \times E \to E_1 \times E_2, \tag{1}$$

where $a, b \in \mathbb{Z}$ cannot be zero simultaneously. Regarding $E \times E'$, one can also construct $\left(\begin{smallmatrix} a\varphi_1 & 0 \\ 0 & a\varphi_2 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & b\varphi_1 \\ b\varphi_2 & 0 \end{smallmatrix}\right)$ for some φ_1, φ_2 of the same degree.

Therefore, we define a new splitting problem as follows:

Definition 15. (ℓ-`Splitting`) Given a principally polarized abelian surface B and a maximal m-isotropic group $K \subset B[m]$ for some integer $m \in \mathbb{N}$ which defines the adjoint of $f \colon A \to B$, find an efficient representation of a splitting $g \colon B \to E_1 \times E_2$ consisting of (ℓ, ℓ)-isogenies. The composition $g \circ f$ satisfies the following conditions for any $M \in \mathbb{Z}$.

1. If A is reducible, then $g \circ f$ is not of the form (1).
2. If A is irreducible, then there is no more restriction on g.

Remark 5. The general `Splitting` problem is defined as Definition 15 without the degree restriction. Clearly, we have a reduction from `Splitting` to ℓ-`Splitting`.

3.1 `OneEnd` to `Splitting`

Given a supersingular elliptic curve E, we still consider $E \times E$. To reduce the length of the whole chain, we use the explicit method developed in [KS26] to obtain a $(2,2)$-gluing $f \colon E \times E \to A$. Now by running the `Splitting` oracle, we obtain a splitting $g \colon A \to E_1 \times E_2$ which is not necessary to be a good extension of f. The product isogeny $F := g \circ f$ still has a matrix form as follows:

$$\begin{pmatrix} \phi_1 & \phi_2 \\ \phi_3 & \phi_4 \end{pmatrix} : E \times E \to E_1 \times E_2.$$

Note that $\hat{\phi}_2 \circ \phi_1$ and $\hat{\phi}_4 \circ \phi_3$ are endomorphisms of E. However, they are the same map: $\tilde{F} \circ F = \left(\begin{smallmatrix} d & 0 \\ 0 & d \end{smallmatrix}\right)$ for some $d \in \mathbb{Z}$, the bottom left entry forces $\hat{\phi}_2 \circ \phi_1 = \hat{\phi}_4 \circ \phi_3$.

Algorithm 1 `OneEnd` to `Splitting`

Input: a supersingular elliptic curve E
Output: a nontrivial endomorphism of E

1: Compute the $(2,2)$-gluing $f \colon E \times E \to A$
2: Run the `Splitting` oracle on input $(A, \ker(\hat{f}))$ to obtain a suitable $g \colon A \to E_1 \times E_2$ and denote $g \circ f$ by $\left(\begin{smallmatrix} \phi_1 & \phi_2 \\ \phi_3 & \phi_4 \end{smallmatrix}\right)$
3: **return:** $\hat{\phi}_2 \circ \phi_1$

Proposition 3. *`OneEnd` reduces to `Splitting`.*

Proof. The reduction is sketched in Algorithm 1, and it remains to show that $\hat{\phi}_2 \circ \phi_1$ is nontrivial. We first write $\phi_1 = [a]\phi_i'$, $\phi_2 = [b]\phi_2'$, $\phi_3 = [c]\phi_3'$ and $\phi_4 = [d]\phi_4'$ where $a, b, c, d \in \mathbb{N}$ and ϕ_i''s are cyclic. Note that if $\hat{\phi}_2 \circ \phi_1$ is constant, then $\phi_2' = \pm\phi_1'$.

Case 1. Assume $\hat{\phi}_2 \circ \phi_1$ is a non-zero constant, we can rewrite the product isogeny as

$$\begin{pmatrix} [a]\phi_1' & [v]\phi_1' \\ [c]\phi_3' & [w]\phi_3' \end{pmatrix}$$

where $v = \pm b$ and $w = \pm d$. Because it is polarized, we have

$$\begin{pmatrix} a\phi'_1 & v\phi'_1 \\ c\phi'_3 & w\phi'_3 \end{pmatrix} \begin{pmatrix} a\hat{\phi}'_1 & c\hat{\phi}'_3 \\ v\hat{\phi}'_1 & w\hat{\phi}'_3 \end{pmatrix} = \begin{pmatrix} (a^2+v^2)\deg\phi'_1 & (ac+vw)\phi'_1\hat{\phi}'_3 \\ (ac+vw)\phi'_3\hat{\phi}'_1 & (c^2+w^2)\deg\phi'_3 \end{pmatrix} = \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix}$$

for some D. Notice that $ac + vw = 0$, we then rewrite the product as

$$\begin{pmatrix} a\phi'_1 & -b\phi'_1 \\ bk\phi'_3 & ak\phi'_3 \end{pmatrix} \text{ or } \begin{pmatrix} a\phi'_1 & b\phi'_1 \\ bk\phi'_3 & -ak\phi'_3 \end{pmatrix}$$

for some $k \in \mathbb{Z}$. Because the two diagonal elements must be the same, we have $(a^2 + b^2)\deg\phi'_1 = k^2(a^2 + b^2)\deg\phi'_3$ which means $\deg\phi'_1 = k^2\deg\phi'_3 = \deg(k\phi'_3)$. In other words, the product isogeny is exactly of the form (1), which contradicts the restriction in Definition 15.

Case 2. Assume $\hat{\phi}_2 \circ \phi_1$ is zero. It implies that at least one of ϕ_2 and ϕ_1 is the zero map. Since the two compositions are equal, the same must hold for ϕ_3 and ϕ_4. Then we have the following possibilities:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \phi_1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \phi_1 & 0 \\ \phi_3 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \phi_2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \phi_2 \\ 0 & \phi_4 \end{pmatrix}, \begin{pmatrix} \phi_1 & 0 \\ 0 & \phi_4 \end{pmatrix}, \begin{pmatrix} 0 & \phi_2 \\ \phi_3 & 0 \end{pmatrix}.$$

An isogeny has a finite kernel, so the first five possibilities are not isogenies. By the same computation as in Case 1, the last two maps are polarized isogenies if the degrees of the two nonzero isogenies are the same, i.e., the matrices are of the form (1). □

3.2 Isogeny to Splitting

Using a similar strategy as in the previous subsection, we are also able to prove the reduction from `Isogeny` to `Splitting`.

Algorithm 2 `Isogeny` to `Splitting`

Input: two supersingular elliptic curves E and E'
Output: an isogeny $\phi\colon E \to E'$

1: Compute the $(2,2)$-gluing $f\colon E \times E' \to A$
2: Run the `Splitting` oracle on input $(A, \ker(\hat{f}))$ to obtain a suitable $g\colon A \to E_1 \times E_2$ and denote $g \circ f$ by $\left(\begin{smallmatrix} \phi_1 & \phi_2 \\ \phi_3 & \phi_4 \end{smallmatrix}\right)$
3: **return:** $\hat{\phi}_2 \circ \phi_1$

Proposition 4. *`Isogeny` reduces to `Splitting`.*

Proof. The reduction is sketched in Algorithm 2. It remains to prove that $\hat{\phi}_2 \circ \phi_1$ is non-zero. The cases are exactly the second case in the proof of Proposition 3. □

4 ℓ-Splitting and EndRing2

WARNING

The original purpose of this section was to prove the equivalence between ℓ-`Splitting` and `EndRing2`, but our proof was wrong. Indeed, the first subsection (`EndRing2` → ℓ-`Splitting`) is incorrect, with an ℓ-`Splitting` oracle, we are not able to compute $\mathrm{End}(E_1 \times E_2)$ because we cannot recover the $\mathrm{Hom}(E_1, E_2)$ and $\mathrm{Hom}(E_2, E_1)$. The second subsection (ℓ-`Splitting` → `EndRing2`) still holds because it is a result (Algorithm 4) of [CDK+25] and [Mon26].

In this section, we prove the equivalence of ℓ-Splitting and EndRing2 under GRH and the KLPT^2 heuristics. To use IsogenyToMatrix, we consider ℓ-Splitting in this section.

We leave the equivalence between EndRing2 and the general Splitting for future work. Also as in [Mon26], we leave the relaxation of KLPT^2 heuristics for future work.

4.1 EndRing2 to ℓ-Splitting

We consider the irreducible case in the Algorithm 3, and discuss the stronger result for reducible case in Remark 6. The idea is to use Proposition 1 and the equivalence between OneEnd and EndRing to compute the IKO matrix of the codomain, and then compute the IKO matrix of the given PPAS via the connecting isogeny given by ℓ-Splitting oracle.

Algorithm 3 EndRing2 to ℓ-Splitting

Input: an irreducible superspecial PPAS A
Output: End(A)
1: Running the ℓ-Splitting oracle, we have $\phi\colon A \to E_1 \times E_2$
2: **for** $i = 1, 2$ **do**
3: Run the ℓ-Splitting oracle, we are able to find a non-scalar endomorphism of E_i by Proposition 3. Repeating it polynomial many times, we recover End(E_i)
4: **end for**
5: Compute End$(E_1 \times E_2)$ from the knowledge of End(E_1) and End(E_2)
6: Compute the IKO matrix g_{12} of $E_1 \times E_2$ from End$(E_1 \times E_2)$
7: With the help of $\tilde{\phi}$, we are able to find the IKO matrix g_A of A
8: With g_A, we can compute a good representation of End(A)
9: **return:** a good representation of End(A)

Remark 6. Regarding the reducible case, say $E \times E'$, we have a stronger result as follows. To compute End$(E \times E')$, one only needs End(E) and End(E'), which can be computed by assuming Splitting, and use Step 5. Note that Step 5 only relies only on GRH. Moreover, IsogenyToMatrix is not necessary in this case, so we have: *Given a superspecial $E \times E'$, computing its endomorphism ring reduces to Splitting under GRH.*

Proposition 5. *EndRing2 reduces to ℓ-Splitting under GRH and the KLPT^2 heuristics.*

Proof. The reduction is sketched in Algorithm 3. The splitting-finding in Step 3 can be randomized by taking a random walk first, and this step efficiently provides an efficient representation of End(E_i) thanks to Proposition 3 and [PW24]. By Proposition 2, Step 5 is efficient. We use IsogenyToMatrix in Step 7 to compute the IKO matrix of A. Step 6 and Step 8 are heuristically efficient by Proposition 1. □

4.2 ℓ-Splitting to EndRing2

An anonymous reviewer of [KS26] pointed out this reduction. But we also note that GoodSplitting, which is the main role in [KS26], cannot reduce to EndRing2 to our knowledge since the current KLPT^2 algorithm doesn't generate a chain of good isogenies in general. Assume an EndRing2 oracle, we have the IKO matrices of the two PPAS, a connecting isogeny can therefore be computed by KLPT^2 algorithm.

Proposition 6. *ℓ-Splitting reduces to EndRing2 under GRH and the KLPT^2 heuristics.*

Proof. The reduction is sketched in Algorithm 4. Given a superspecial PPAS A, by knowing End(A) and Proposition 1, the computation of the IKO matrix of A is efficient under GRH and KLPT^2 heuristics. With the knowledge of the IKO matrices of A and E^2 for some E,

Algorithm 4 ℓ-`Splitting` to `EndRing2`

Input: a superspecial PPAS A
Output: $\phi\colon A \to E_0 \times E_0$
1: Run the `EndRing2` oracle on A to obtain $\mathrm{End}(A)$
2: Compute the IKO matrix of A
3: Using KLPT^2 to find an isogeny ϕ from A to $E_0 \times E_0$
4: **return:** ϕ

the KLPT^2 algorithm efficiently finds a connecting isogeny under the assumptions of the algorithm. □

5 Conclusion

In this work we showed that `EndRing2` and ℓ-`Splitting` are polynomial-time equivalent (assuming heuristics from [CDK+25]) which significantly strengthens the results of [KS26]. Our results do not yet extend to arbitrary splittings but only because current `IsogenyToMatrix` algorithms require the degree of the isogeny to be smooth. Hence, if one could find a polynomial-time algorithm for `IsogenyToMatrix` for arbitrary degree isogenies given by an isogeny representation, then our results naturally extend to that case as well.

The methods of this paper likely extend to g-dimensional superspecial abelian varieties as long as a higher dimensional analog of [CDK+25] is established. This shows that finding a reducible abelian variety in the Costello-Smith algorithm will always naturally be the bottleneck of the algorithm as expected.

References

[ABE+25] Bill Allombert, Jean-François Biasse, Jonathan Komada Eriksen, Péter Kutas, Chris Leonardi, Aurel Page, Renate Scheidler, and Márton Tot Bagi. Faster SCALLOP from Non-Prime Conductor Suborders in Medium Sized Quadratic Fields. In *Public-Key Cryptography-PKC 2025*, volume 15676, pages 333–363. Springer Nature Switzerland, 2025.

[ABI+25] Samuele Anni, Gaetan Bisson, Annamaria Iezzi, Elisa Lorenzo García, and Benjamin Wesolowski. On the computation of endomorphism rings of abelian surfaces over finite fields, 2025. arXiv: https://arxiv.org/pdf/2503.08925v1. arXiv:2503.08925.

[CDK+25] Wouter Castryck, Thomas Decru, Péter Kutas, Abel Laval, Christophe Petit, and Yan Bo Ti. KLPT^2: Algebraic Pathfinding in Dimension Two and Applications. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025*, pages 167–200, Cham, 2025. Springer Nature Switzerland.

[CDS20] Wouter Castryck, Thomas Decru, and Benjamin Smith. Hash functions from superspecial genus-2 curves using Richelot isogenies. *Journal of Mathematical Cryptology*, 14(1):268–292, 2020. URL: https://doi.org/10.1515/jmc-2019-0021, doi:doi:10.1515/jmc-2019-0021.

[CII+23] Mingjie Chen, Muhammad Imran, Gábor Ivanyos, Péter Kutas, Antonin Leroux, and Christophe Petit. Hidden stabilizers, the isogeny to endomorphism ring problem and the cryptanalysis of psidh. In *International Conference on*

the Theory and Application of Cryptology and Information Security, pages 99–130. Springer, 2023.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An Efficient Post-Quantum Commutative Group Action. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 395–427, Cham, 2018. Springer International Publishing.

[CLP24] Mingjie Chen, Antonin Leroux, and Lorenz Panny. SCALLOP-HD: group action from 2-dimensional isogenies. In *IACR International Conference on Public-Key Cryptography*, pages 190–216. Springer, 2024.

[CS20] Craig Costello and Benjamin Smith. The Supersingular Isogeny Problem in Genus 2 and Beyond. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography*, pages 151–168, Cham, 2020. Springer International Publishing.

[DEF+25] Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren, and Benjamin Wesolowski. PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025*, pages 67–99, Cham, 2025. Springer Nature Switzerland.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, pages 197–272, 1941.

[DFKL+20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93, Cham, 2020. Springer International Publishing.

[DG16] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Des. Codes Cryptography*, 78(2):425–440, February 2016.

[EPSV23] Jonathan Komada Eriksen, Lorenz Panny, Jana Sotáková, and Mattia Veroni. Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic. *LuCaNT 2023*, 2023.

[FFK+23] Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. SCALLOP: scaling the CSI-FiSh. In *IACR international conference on public-key cryptography*, pages 345–375. Springer, 2023.

[FIK+25] Jenny Fuselier, Annamaria Iezzi, Mark Kozek, Travis Morrison, and Changningphaabi Namoijam. Computing supersingular endomorphism rings using inseparable endomorphisms. *Journal of Algebra*, 668:145–189, 2025. URL: https://www.sciencedirect.com/science/article/pii/S0021869325000353, doi:10.1016/j.jalgebra.2025.01.012.

[FT19] E. V. Flynn and Yan Bo Ti. Genus Two Isogeny Cryptography. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography*, pages 286–306, Cham, 2019. Springer International Publishing.

[IKO86] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort. Supersingular curves of genus two and class numbers. *Compositio Mathematica*, 57(2):127–152, 1986.

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.

[KS26] Sabrina Kunzweiler and Min-Yi Shen. Endomorphisms via splittings. In Magali Bardet and Ruben Niederhagen, editors, *Post-Quantum Cryptography*, pages 3–38, Cham, 2026. Springer Nature Switzerland.

[Mil08] James S. Milne. Abelian Varieties (v2.00), 2008. Available at https://www.jmilne.org/math/CourseNotes/AV.pdf.

[Mon26] Mickaël Montessinos. Equivalent computational problems for superspecial abelian surfaces. Cryptology ePrint Archive, Paper 2026/120, 2026. URL: https://eprint.iacr.org/2026/120.

[Mum74] David Mumford. *Abelian Varieties*. Oxford University Press, 1974.

[PRS26] Aurel Page, Damien Robert, and Julien Soumier. On the conversion of module representations for higher dimensional supersingular isogenies. *Cryptology ePrint Archive*, 2026.

[PW24] Aurel Page and Benjamin Wesolowski. The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024*, pages 388–417, Cham, 2024. Springer Nature Switzerland.

[Rü90] Hans-Georg Rück. Abelian surfaces and jacobian varieties over finite fields. *Compositio Mathematica*, 76(3):351–366, 1990.

[Sil09] Joseph H Silverman. *The Arithmetic of Elliptic Curves*. Graduate texts in mathematics. Springer New York, 2009. doi:10.1007/978-0-387-09494-6.

[Tak17] Katsuyuki Takashima. Efficient algorithms for isogeny sequences and their cryptographic applications. In *Mathematical Modelling for Next-Generation Cryptography: CREST Crypto-Math Project*, pages 97–114. Springer, 2017.

[Wes22] Benjamin Wesolowski. Orientations and the supersingular endomorphism ring problem. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 345–371. Springer, 2022.