KLPT^2: Algebraic pathfinding in dimension two and applications

Wouter Castryck[1], Thomas Decru[1], Péter Kutas[2,4],
Abel Laval[3], Christophe Petit[3,4], Yan Bo Ti[5,6]

[1] COSIC, KU Leuven, Belgium
[2] Faculty of Informatics, Eötvös Loránd University, Hungary
[3] Computer Science Department, Université Libre de Bruxelles, Belgium
[4] School of Computer Science, University of Birmingham, United Kingdom
[5] DSO National Laboratories, Singapore
[6] Temasek Laboratories, National University of Singapore, Singapore

Abstract. Following Ibukiyama, Katsura and Oort, all principally polarized superspecial abelian surfaces over $\overline{\mathbb{F}}_p$ can be represented by a certain type of 2×2 matrix g, having entries in the quaternion algebra $B_{p,\infty}$. We present a heuristic polynomial-time algorithm which, upon input of two such matrices g_1, g_2, finds a "connecting matrix" representing a polarized isogeny of smooth degree between the corresponding surfaces. Our algorithm should be thought of as a two-dimensional analog of the KLPT algorithm from 2014 due to Kohel, Lauter, Petit and Tignol for finding a connecting ideal of smooth norm between two given maximal orders in $B_{p,\infty}$.

The KLPT algorithm has proven to be a versatile tool in isogeny-based cryptography, and our analog has similar applications; we discuss two of them in detail. First, we show that it yields a polynomial-time solution to a two-dimensional analog of the so-called constructive Deuring correspondence: given a matrix g representing a superspecial principally polarized abelian surface, realize the latter as the Jacobian of a genus-2 curve (or, exceptionally, as the product of two elliptic curves if it concerns a product polarization). Second, we show that, modulo a plausible assumption, Charles–Goren–Lauter style hash functions from superspecial principally polarized abelian surfaces require a trusted set-up. Concretely, if the matrix g associated with the starting surface is known then collisions can be produced in polynomial time. We deem it plausible that all currently known methods for generating a starting surface indeed reveal the corresponding matrix. As an auxiliary tool, we present an efficient method for converting isogenies of powersmooth degree into the corresponding connecting matrix, a step for which a previous approach by Chu required super-polynomial (but sub-exponential) time.

1 Introduction

In isogeny-based cryptography, the core problem is that of finding an explicit isogeny between two isogenous elliptic curves over a finite field. Here, "explicit" often implicates that the degree of the isogeny is powersmooth, or a power of some small prescribed prime number ℓ. For reasons of both security and efficiency, almost all cryptographic constructions restrict their focus to supersingular elliptic curves. Famously, Deuring [16] proved that such curves are (essentially) in one-to-one correspondence with maximal orders in the quaternion algebra $B_{p,\infty}$ ramified at p and ∞; here p denotes the field characteristic. Under this correspondence, isogenies correspond to ideals, and the isogeny-finding problem translates into finding a connecting ideal between two given maximal orders $\mathcal{O}_0, \mathcal{O}_1 \subset B_{p,\infty}$, where one then aims for integral ideals I whose norm $\mathsf{n}(I)$ is powersmooth or a power of ℓ. Interestingly, this quaternion version of the isogeny-finding problem can be dealt with efficiently: in 2014, Kohel, Lauter, Petit, and Tignol [30] proposed a polynomial-time algorithm, now commonly known as the KLPT algorithm, for solving exactly this problem.

This result has had an amplitude of consequences, both constructive and destructive. For example, it breaks the second pre-image resistance of the Charles–Goren–Lauter (CGL) hash function [18, 19] when using an untrusted set-up. A more recent cryptanalytic example is the break of pSIDH [10].[†] More fundamentally, it has led to a key insight in isogeny-based cryptography. Namely, on one hand, given a maximal order in $B_{p,\infty}$, one can use the KLPT algorithm to compute a corresponding supersingular elliptic curve $E/\overline{\mathbb{F}}_p$ in polynomial time: this is called the constructive Deuring correspondence and it is practical for cryptographically sized values of p [20]. On the other hand, the converse problem, namely computing the endomorphism ring of a given supersingular elliptic curve, is believed to be very hard. By now, we understand, in a heuristic-free way,[‡] that this is in fact the central hard problem in (supersingular) isogeny-based cryptography [42]. That is, the Deuring correspondence is a one-way function, and it allows for trapdoors, e.g., in the form of secret isogenies to an easy base curve. This has sparked many important constructions, where we highlight the Galbraith–Petit–Silva (GPS) signature scheme [22] and SQIsign [15].

Recently, the field of isogeny-based cryptography was shaken up by the use of higher-dimensional principally polarized abelian varieties. Earlier works such as [7, 11, 21, 40] studied these objects in their own right, but the real catalysts were the attacks on SIDH [5, 32, 36] which revealed a very powerful interplay between higher dimension and dimension one, i.e., the world of elliptic curves. Constructive applications followed soon, especially because the machinery allows for efficient representations of isogenies of arbitrary degree [37]. This has culminated in various new schemes, including SQIsign variants [1, 14, 17, 34] improving over their ancestor in terms of speed, compactness, and security foundations.

In view of these current trends, a higher-dimensional analog of the KLPT algorithm is an important lacking tool. The direct provocation for this research is the PhD thesis by Chu [11], who mentions this as a missing ingredient in a GPS-style signature scheme from superspecial principally polarized abelian surfaces. Here, the Deuring correspondence is to be replaced with a correspondence

[†] The attack from [10] does not invoke the KLPT algorithm directly; rather, it uses and adapts several of its subroutines.

[‡] Modulo a reliance on the generalized Riemann hypothesis.

due to Ibukiyama, Katsura and Oort [26] describing principal polarizations and polarized isogenies in terms of 2×2 matrices with entries in $B_{p,\infty}$. Such a missing analog of KLPT is exactly the central result of our paper.

Main contributions:

- *KLPT^2.* We provide a two-dimensional analog of the KLPT algorithm: upon input of two matrices g_1, g_2 representing two principally polarized superspecial abelian surfaces, the KLPT^2 algorithm heuristically finds, in polynomial time, a "connecting matrix" representing a polarized isogeny of reduced degree N. We provide versions both for $N = \ell^e$ (where ℓ is a small prescribed prime number) and for N powersmooth. In both cases, the value of N achieved is in $O(p^{25+\varepsilon})$. The main techniques are the following. First we observe that if the matrices g_1, g_2 are in a very special form, then finding a connecting matrix is easy (Lemma 3.3). This turns the problem into a transformation problem: instead of connecting two matrices, try to transform one matrix into a standard form. An important challenge is to bound the output degree in a way that only depends on p and not on the sizes of the matrices g_i. This is handled using certain size reductions and solving certain Diophantine equations. One noteworthy ingredient is an algorithm that given $a, c \in \mathcal{O}$ (where $\mathcal{O}$ is a maximal order in $B_{p,\infty}$) that have coprime norm, finds $b, d \in \mathcal{O}$ such that the reduced norm of the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is a power of ℓ (or powersmooth) in $O(p^{3+\varepsilon})$. Quite surprisingly, this problem is essentially equivalent to 1-dimensional KLPT (Section 3.2). We deem it very likely that the exponent $25 + \varepsilon$ can be improved, but leave such sharpenings for future work (and we note that future improvements on one-dimensional KLPT also improve our results).
- *Constructive Ibukiyama–Katsura–Oort (IKO) correspondence.* In Section 4.1, we describe an efficient algorithm for matrix-to-isogeny conversion for powersmooth degrees (thereby ticking off an unsurprising but missing ingredient in Chu's aforementioned signature scheme). Combined with our KLPT^2 algorithm, this yields a heuristic polynomial-time method for an analog of the constructive Deuring correspondence, described in Section 5.1: given a matrix g representing a principally polarized superspecial abelian surface, we explicitly realize this surface as either the Jacobian of a genus-2 curve, or as a product of elliptic curves equipped with the product polarization.
- *Polynomial-time isogeny-to-matrix conversion for isogenies of smooth degree.* In order to transfer more advanced applications of KLPT to dimension two, one also needs an efficient solution to the converse problem: given a principally polarized superspecial abelian surface A_1 with known matrix g_1, along with a polarized isogeny $\varphi : A_1 \to A_2$, find a matrix g_2 corresponding to A_2 along with a connecting matrix corresponding to φ. In the special case of (ℓ, ℓ)-isogenies, where ℓ denotes any small prime, we provide a simple and efficient method for computing such a connecting matrix, and then g_2 follows right away. This then naturally extends to a polynomial-time algorithm for isogeny-to-matrix conversion for polarized isogenies of powersmooth degree.

In this way, we by-pass the need for invoking Chu's super-polynomial (but sub-exponential) time algorithm for the principal ideal problem (PIP) in quaternionic matrix rings [11, Chapter 2]. Finally, by mimicking a method due to Eisenträger, Hallgren, Lauter, Morrison and Petit [18, Algorithm 9], in Section 14 we lift this to a polynomial-time algorithm for isogeny-to-matrix conversion for polarized isogenies of arbitrary smooth degree, through a repeated application of KLPT^2.

– *Attacks on CGL style hash functions.* Section 5.4 describes our main application: an attack on CGL-type hash functions in dimension two, which were explicitly proposed in [7, 21, 31, 40], in the case of an untrusted set-up. This is similar to the KLPT-based attacks [18, 19] on the original CGL hash function. Concretely, if the starting surface comes with a known matrix g (which seems a fair assumption to make in all untrusted instantiations) then we can use the KLPT^2 algorithm to find collisions. Unfortunately, it does not allow us to find second pre-images, due to the fact that KLPT^2 does not produce "good" chains of (ℓ, ℓ)-isogenies in the sense of [7] (see Corollary 5.4).

We conclude this introduction by noting that our KLPT^2 algorithm can be seen as a constructive proof (modulo heuristic assumptions) of the dimension-two case of Jordan and Zaytman's recent result that the graph of $(\ell, \ldots, \ell)$-isogenies between superspecial principally polarized abelian varieties is connected [27].

Outline

We provide some background on the KLPT algorithm, principal polarizations, the Ibukiyama–Katsura–Oort correspondence, and quaternionic matrices in Section 2. We describe our generalization of KLPT to dimension two in Section 3 and discuss routines for matrix-to-isogeny and isogeny-to-matrix conversion in Section 4. We describe our applications of KLPT^2 in Section 5. This is the shortened proceedings version of a longer paper that can be found online [6], to which we refer for all the missing proofs, several accompanying remarks, and some natural directions for future research. The numbering of our theorems, lemmas, remarks etc. is consistent with that of the full version.

Acknowledgments and support

We thank Jonathan Komada Eriksen, Riccardo Invernizzi, Gábor Ivanyos, Harun Kir, Gioella Lorenzon, Aurel Page, Krijn Reijnders, Damien Robert and Frederik Vercauteren for sharing helpful insights. Castryck and Decru are supported in part by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement ISOCRYPT – No. 101020788), by the Research Council KU Leuven grant C14/ 24/099, as well as by CyberSecurity Research Flanders with reference number VR20192203. Together with Kutas, they are also supported by the CELSA alliance through the MaCro project. Decru is partly supported by Fonds de la Recherche Scientifique (FRS-FNRS) and by Fonds voor Wetenschappelijk Onderzoek (FWO) with reference number 1245025N. Kutas and Petit are partly supported by EPSRC through grant number EP/V011324/1. Kutas is supported by the Hungarian Ministry of Innovation and Technology NRDI Office within the framework of the Quantum Information National Laboratory Program and by the grant "EXCELLENCE-151343". Kutas is also supported by János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

2 Preliminaries

2.1 Deuring correspondence and the KLPT algorithm

For general background on quaternion algebras, we refer to [41]. For now, recall that a (rational) quaternion algebra B is a central simple algebra of dimension 4 over $\mathbb{Q}$. An order in B is a subring $\mathcal{O} \subset B$ containing 1 which has rank 4 as a $\mathbb{Z}$-module. An order is called maximal if it is maximal with respect to inclusion. The isomorphism class of a quaternion algebra is determined by its local behaviour: for which completions $\mathbb{Q}_v$ do we have that $B \otimes_{\mathbb{Q}} \mathbb{Q}_v$ is a division algebra? Such places v are called ramified.[†] In this paper we will be concerned with $B_{p,\infty}$, the unique quaternion algebra up to isomorphism which is ramified at ∞ and at a fixed prime number p (typically of cryptographic size). The endomorphism ring of every supersingular elliptic curve over $\overline{\mathbb{F}}_p$ is isomorphic to a maximal order $\mathcal{O} \subset B_{p,\infty}$. Under this isomorphism, the degree of an endomorphism corresponds to the norm[‡] $\mathsf{n}(u)$ of the corresponding quaternion u.

Example 2.1. If $p \equiv 3 \bmod 4$ then one can realize the quaternion algebra $B_{p,\infty}$ as $\mathbb{Q}\langle 1, i, j, k\rangle$ with $i^2 = -1$, $j^2 = -p$ and $k = ij = -ji$. The elliptic curve $E_0 : y^2 = x^3 + x$ with $j(E_0) = 1728$ is supersingular. Here $\mathrm{End}(E_0) \cong \mathcal{O}_0$ with

$$\mathcal{O}_0 = \left\langle 1, i, \frac{i+j}{2}, \frac{1+k}{2} \right\rangle.$$

One isomorphism $\tau : \mathcal{O}_0 \xrightarrow{\cong} \mathrm{End}(E_0)$ arises by letting $\tau(i) : (x, y) \mapsto (-x, \sqrt{-1}y)$ and $\tau(j) : (x, y) \mapsto (x^p, y^p)$. As mentioned: $\mathsf{n}(u) = \deg(\tau(u))$ for all $u \in \mathcal{O}_0$.

The Deuring correspondence [16] asserts that this turns into a categorical equivalence between supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$ (up to Galois conjugation) and maximal orders in $B_{p,\infty}$ (up to isomorphism or, equivalently, up to conjugation). On the elliptic curve side, the non-zero morphisms are isogenies $\varphi : E_0 \to E_1$. On the quaternion side, such an isogeny φ corresponds to a rank-4 sub-$\mathbb{Z}$-module $I \subset B_{p,\infty}$ which is a left, resp. right, ideal of a maximal order $\mathcal{O}_0 \cong \mathrm{End}(E_0)$, resp. $\mathcal{O}_1 \cong \mathrm{End}(E_1)$. This ideal is then referred to as a connecting ideal of $\mathcal{O}_0$ and $\mathcal{O}_1$. Note that endomorphism rings can be embedded into $B_{p,\infty}$ in many ways: any embedding can be post-composed with conjugation.

[†] In the non-ramified cases we have $B \otimes_{\mathbb{Q}} \mathbb{Q}_v \cong \mathrm{M}_2(\mathbb{Q}_v)$.

[‡] Or rather to its *reduced* norm in the sense of [41, Section 3.3]; throughout this paper, for simplicity, we will drop the adjective "reduced".

This warrants the notion of equivalent ideals: a left ideal $J \subset \mathcal{O}_0$ will be a right ideal of an order $\mathcal{O}_1' \cong \mathcal{O}_1$ if and only if there exists $\beta \in B_{p,\infty} \setminus \{0\}$ such that $J = I\beta$. On the geometric side, this corresponds to different isogenies connecting the same curves. The left ideals $I, J \subset \mathcal{O}_0$ are then said to be equivalent.

There is an explicit geometric view on Deuring's construction of the ideal I: it can be seen as the subset of $\mathrm{End}(E_0)$ that is obtained by post-composing φ with all elements of $\mathrm{Hom}(E_1, E_0)$. Thus I encodes the set of all isogenies $E_1 \to E_0$, and the norm of every element of I is divisible by the degree of φ. More precisely, it can be shown that $\deg(\varphi)$ equals $\mathsf{n}(I) = \gcd\{\mathsf{n}(u) \mid u \in I\}$, the norm of I.

The Deuring correspondence implies that there is a natural quaternion analog of the ℓ-isogeny pathfinding problem. Indeed, upon input of two maximal orders $\mathcal{O}_0, \mathcal{O}_1 \subset B_{p,\infty}$ connected by an ideal I, it amounts to finding an equivalent left ideal $J \subset \mathcal{O}_0$ of norm ℓ^e for some $e \geq 1$. An alternative viewpoint taking the geometric interpretation into account is as follows: when given one connecting ideal I, it is enough to find $\sigma \in I$ such that $\mathsf{n}(\sigma) = \mathsf{n}(I)\ell^e$. This is exactly the problem that is addressed by the KLPT algorithm [30].[†] It is then easy to check that $J = I\beta$ with $\beta = \bar{\sigma}/\,\mathsf{n}(I)$ is an equivalent ideal with norm ℓ^e. Geometrically, under the above identification of I with $\mathrm{Hom}(E_1, E_0)\varphi$, we can write $\sigma = \tau\varphi$ for a degree-ℓ^e isogeny $\tau : E_1 \to E_0$, and then J corresponds to $\mathrm{Hom}(E_1, E_0)\varphi\hat{\sigma}/\deg(\varphi) = \mathrm{Hom}(E_1, E_0)\varphi\hat{\varphi}\hat{\tau}/\deg(\varphi) = \mathrm{Hom}(E_1, E_0)\hat{\tau}$.

Remark 2.2. This is an important view on KLPT as we will need it in exactly the version where it finds an element of prescribed norm in a certain ideal.

The way KLPT proceeds is as follows. Using a simple trick one can assume knowledge of a left ideal $I \subset \mathcal{O}_0$ of prime norm N, so we would like to find an element $\sigma \in I$ of norm $N\ell^e$. First one finds $\gamma \in \mathcal{O}_0$ whose norm is $N\ell^{e_0}$. Now the ideal $J = \mathcal{O}_0 N + \mathcal{O}_0\gamma$ has norm N. Locally, i.e., modulo N, I and J reduce to proper left ideals of the matrix ring $\mathrm{M}_2(\mathbb{Z}/N\mathbb{Z})$ and such ideals only differ by right-multiplication by an invertible element δ. Such a δ can be computed locally and lifted to $\mathcal{O}_0$ (using an explicit isomorphism between $\mathcal{O}_0/N\mathcal{O}_0$ and $\mathrm{M}_2(\mathbb{Z}/N\mathbb{Z})$) which implies that $\gamma\delta \in I$. Now the key is that δ is determined modulo N only, so what is left to do is choose an appropriate lifting such that $\mathsf{n}(\delta) = \ell^{e_1}$. This step is called *strong approximation* and in [30] it is carried out for special extremal orders $\mathcal{O}_0$, i.e., maximal orders containing an imaginary quadratic order with small discriminant (it can be modified to work for arbitrary orders, see [15, Section 5] and [10, Section 5]). Now it is clear that $\gamma\delta$ will fit our criteria with $e = e_0 + e_1$. The KLPT algorithm can guarantee that $\ell^e \in O(p^{3+\varepsilon})$.[‡]

2.2 Principally polarized abelian varieties

For detailed background, we refer to [4, 11, 26, 33]. An abelian variety over an algebraically closed field is a projective algebraic variety which is also an alge-

[†] In other applications of KLPT one searches for connecting ideals having powersmooth norm, but the approach is entirely the same.

[‡] The original bound from KLPT is in the order of $p^{3.5}$, but an improvement due to Petit and Smith [35], reported in [9, Algorithm 13], reduces this to $p^{3+\varepsilon}$ as stated.

braic group. The notion generalizes that of an elliptic curve, which is an abelian variety of dimension one. However, for most uses (including in cryptography), the more relevant generalization is that of an abelian variety equipped with a *principal polarization*. Unfortunately, this notion does not admit a down-to-earth definition. Luckily, the exact construction is not really important for this paper, which is mostly algebraic in nature. Therefore, the reader who is unfamiliar with the notation and terminology below can just think of a polarization as a certain kind of isogeny (i.e., a finite surjective homomorphism) between A and a companion abelian variety $\hat{A}$ called its dual.[†] We include a formal definition, e.g., to allow the reader to verify the proof of Theorem 2.8 further down:

Definition 2.3. *A* polarization *on a g-dimensional abelian variety A is an isogeny of the form*

$$\begin{aligned} \lambda : A \to \ & \hat{A} = \mathrm{Pic}^0(A) \\ P \mapsto \ & [t_{-P}(D) - D] \end{aligned}$$

with D an ample divisor on A, where t_{-P} denotes point-wise translation by $-P$. It can be shown that $\deg(\lambda) = (D^g/g!)^2$ with D^g the self-intersection number of D. If this degree is equal to 1 then the polarization is called principal. *Write* $\mathrm{PPol}(A)$ *for the set of principal polarizations on A.*

The reason why the notion of a principally polarized abelian variety still generalizes that of an elliptic curve is that, in the latter case, there is a unique principal polarization, called the canonical polarization. It is given by the negated Abel–Jacobi map: $P \mapsto [(\infty) - (P)]$. The uniqueness typically no longer holds in higher dimension. This is notoriously true for *superspecial* abelian varieties, which are our main objects of interest. A g-dimensional superspecial abelian variety is a variety which — as an unpolarized variety — is isomorphic to a product of g supersingular elliptic curves. It can be shown that, for a fixed characteristic p, all such products are pairwise isomorphic as soon as $g \geq 2$ [38, Theorem 3.5]. However, this unique isomorphism class carries $\Theta(p^{g(g+1)/2})$ inequivalent principal polarizations (in the sense of Definition 2.7 below).

Definition 2.4. *A (polarized) isogeny between two principally polarized abelian varieties (A, λ_A) and (B, λ_B) is an isogeny $\varphi : A \to B$ that respects the polarizations, i.e., there exists a positive integer N for which the following diagram commutes*

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "{[N]\lambda_A}"'] & B \arrow[d, "\lambda_B"] \\ \hat{A} & \hat{B} \arrow[l, "\hat{\varphi}"] \end{tikzcd}$$

Here, $\hat{\varphi}$ is the dual isogeny, defined by taking inverse image divisors under φ. One has $\deg(\varphi) = N^g$, and we call $N = \mathrm{degrd}(\varphi)$ the reduced degree *of φ. If $N = 1$ then φ is called a (polarized) isomorphism; we write $(A, \lambda_A) \cong (B, \lambda_B)$.*

[†] Not all isogenies $A \to \hat{A}$ are polarizations: a certain positivity condition should be satisfied. E.g., if λ is a polarization, then $-\lambda$ is not. See [12, pp. 6–7] for a discussion.

Remark 2.5. Given a principally polarized abelian variety (A, λ_A), an abelian variety B and an isogeny $\varphi : A \to B$, in general there does not exist a principal polarization $\lambda_B : B \to \hat{B}$ such that φ is polarized. If it does exist, then λ_B is unique and called the induced principal polarization. Assuming that $\deg(\varphi) = N^g$ for some integer N coprime with the field characteristic, a necessary and sufficient condition for existence [28, Proposition 1.1] is that $\ker(\varphi)$ is a maximal isotropic subgroup of $A[N]$, where isotropic means that $e_{N,\lambda_A}(P, Q) = 1$ for all $P, Q \in A[N]$, with $e_{N,\lambda_A} : A[N] \times A[N] \to \mu_N$ the N-Weil pairing with respect to the principal polarization λ_A. In this case $\mathrm{degrd}(\varphi) = N$.

Remark 2.6. An isogeny φ is said to be an $(N_1, \ldots, N_r)$-isogeny, for certain integers N_i, if it is separable, polarized and $\ker(\varphi) \cong \bigoplus_{i=1}^r \mathbb{Z}/N_i\mathbb{Z}$. If $\mathrm{degrd}(\varphi)$ is a prime number ℓ, then it concerns an $(\ell, \ldots, \ell)$-isogeny, where $r = g$.

For any isogeny $\varphi : A \to B$ and any choice of principal polarizations λ_A, λ_B, it is natural to consider the *adjoint* isogeny

$$\tilde{\varphi} = \lambda_A^{-1} \hat{\varphi} \lambda_B : B \to A$$

with respect to λ_A, λ_B. If φ is polarized, then so is $\tilde{\varphi}$ and we have $\tilde{\varphi}\varphi = [\mathrm{degrd}(\varphi)]$ and $\varphi\tilde{\varphi} = [\mathrm{degrd}(\varphi)]$. In the context of elliptic curves, the adjoint isogeny can be identified with the dual isogeny $\hat{\varphi} : \hat{B} \to \hat{A}$ via the canonical polarization, with which any isogeny is compatible. This is not the case in higher dimensions. This forces us to make a clear distinction between the dual isogeny, which is independent from any polarization, and the adjoint isogeny, which depends on a choice of principal polarizations and which exhibits the common properties we are familiar with from the elliptic curve case.

If λ is a principal polarization on an abelian variety A, then the adjoint operator $\mathrm{Ros}_\lambda : \alpha \mapsto \tilde{\alpha} = \lambda^{-1}\hat{\alpha}\lambda$, defines an involution of $\mathrm{End}(A)$ called the Rosati involution (with respect to λ).

Definition 2.7. *Two principal polarizations λ_1 and λ_2 on an abelian variety A are said to be* equivalent *if $(A, \lambda_1) \cong (A, \lambda_2)$, i.e., there exists an automorphism α of A such that $\hat{\alpha}\lambda_1\alpha = \lambda_2$. We write* $\mathrm{PPol}^0(A)$ *for the set of principal polarizations on A up to equivalence.*

Turning our focus to dimension $g = 2$, we recall that principally polarized abelian surfaces can be classified as follows: they are isomorphic to either

- a product $E_1 \times E_2$ of two elliptic curves, equipped with the *product polarization*, coming from $D = (E_1 \times \{\infty\}) + (\{\infty\} \times E_2)$, or
- the Jacobian $\mathrm{Jac}(C)$ of a genus-2 curve, equipped with the canonical polarization, coming from $D = (u(C))$ with $u : C \hookrightarrow \mathrm{Pic}^0(C) \cong \mathrm{Jac}(C) : P \mapsto [(P) - (\infty)]$ the Abel–Jacobi map (where $\infty \in C$ denotes any base point).

With respect to product polarizations, the adjoint admits a very explicit description which follows from the proof of [3, Proposition 4.10]. Consider four elliptic curves E_1, E_2, E_3, E_4 and assume we have an isogeny $\varphi : E_1 \times E_2 \to E_3 \times E_4$, not necessarily polarized. We can write this isogeny in matrix form:

$$\varphi : \begin{pmatrix} P \\ Q \end{pmatrix} \mapsto \begin{pmatrix} \alpha_{13} & \alpha_{23} \\ \alpha_{14} & \alpha_{24} \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix}$$

where each $\alpha_{ij} : E_i \to E_j$ is a homomorphism (an isogeny or the zero map) of elliptic curves. With respect to the product polarizations on $E_1 \times E_2$ and $E_3 \times E_4$, we have

$$\tilde{\varphi} : \begin{pmatrix} P \\ Q \end{pmatrix} \mapsto \begin{pmatrix} \hat{\alpha}_{13} & \hat{\alpha}_{14} \\ \hat{\alpha}_{23} & \hat{\alpha}_{24} \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix},$$

so in this case the map $\varphi \mapsto \tilde{\varphi}$ can be thought of as a conjugate-transpose. The isogeny φ is polarized if and only if

$$\begin{pmatrix} \hat{\alpha}_{13} & \hat{\alpha}_{14} \\ \hat{\alpha}_{23} & \hat{\alpha}_{24} \end{pmatrix} \begin{pmatrix} \alpha_{13} & \alpha_{23} \\ \alpha_{14} & \alpha_{24} \end{pmatrix} = \begin{pmatrix} [N] & 0 \\ 0 & [N] \end{pmatrix}$$

for some positive integer N. This integer necessarily equals $\operatorname{degrd}(\varphi)$, so that $\deg(\varphi) = N^2$. In general, by [29, Corollary 64] and [23, Proposition 3.9], we have

$$\deg(\varphi) = (\deg \alpha_{13} + \deg \alpha_{14})(\deg \alpha_{23} + \deg \alpha_{24}) - \deg(\hat{\alpha}_{23}\alpha_{13} + \hat{\alpha}_{24}\alpha_{14}). \quad (1)$$

2.3 Ibukiyama–Katsura–Oort correspondence

In the remainder of the paper, we fix a prime $p \notin \{2, 3\}$ and a supersingular elliptic curve $E_0/\overline{\mathbb{F}}_p$. Let $B_{p,\infty}$ be the unique quaternion algebra (up to isomorphism) ramified exactly at p and infinity. Then, as mentioned, $\operatorname{End}(E_0)$ is isomorphic through the Deuring correspondence to a maximal order $\mathcal{O}_0$ of $B_{p,\infty}$. Define $A_0 = E_0 \times E_0$ and consider the product polarization λ_0. By our previous discussion, the endomorphism ring of A_0 is isomorphic to $\mathrm{M}_2(\mathcal{O}_0)$ and under this isomorphism the Rosati involution (i.e., the adjoint operator) with respect to λ_0 corresponds to the conjugate-transpose.

Recall that, considered without their polarizations, all superspecial abelian surfaces in characteristic p are isomorphic. Consequently, every principally polarized superspecial abelian surface (A, λ_A) is isomorphic to (A_0, λ) for some principal polarization λ on A_0. Explicitly, if $\varphi : A_0 \to A$ is an (unpolarized) isomorphism, then we can take $\lambda = \hat{\varphi}\lambda_A\varphi$. The following method due to Ibukiyama, Katsura and Oort can be used to represent a principal polarization λ on A_0 as a matrix with coefficients in $\mathcal{O}_0$. One considers the map

$$\begin{aligned} \mu : \mathrm{PPol}(A_0) &\to \operatorname{End}(A_0) \\ \lambda \quad &\mapsto \quad \lambda_0^{-1}\lambda, \end{aligned}$$

noting that the image $\lambda_0^{-1}\lambda$ can be identified with an element of $\mathrm{M}_2(\mathcal{O}_0)$.

Theorem 2.8. *The map μ is injective and its image, once transferred to the quaternion world through the Deuring correspondence, corresponds to*

$$\mathrm{Mat}(A_0) := \left\{ \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix}, \quad s, t \in \mathbb{Z}_{>0}, r \in \mathcal{O}_0, st - r\bar{r} = 1 \right\} \quad \subset \ \mathrm{GL}_2(\mathcal{O}_0),$$

i.e., μ determines a bijection between $\mathrm{PPol}(A_0)$ *and* $\mathrm{Mat}(A_0)$.

Proof. This is [26, Corollary 2.9] specialized to principal polarizations (i.e., to ample divisors with self-intersection 2). □

Remark 2.9. An alternative way of specifying a principal polarization λ on A_0 is through the Rosati involution it induces on $\mathrm{M}_2(\mathcal{O}_0)$. This datum is very explicitly encoded in the matrix $g = \mu(\lambda)$:

$$\mathrm{Ros}_\lambda(\alpha) = \lambda^{-1}\hat{\alpha}\lambda = (\lambda_0^{-1}\lambda)^{-1}(\lambda_0^{-1}\hat{\alpha}\lambda_0)(\lambda_0^{-1}\lambda) = g^{-1}\,\mathrm{Ros}_{\lambda_0}(\alpha)g = g^{-1}\alpha^* g,$$

where we recall that the Rosati involution with respect to the product polarization λ_0 indeed amounts to the conjugate-transpose $-^*$.[†] Conversely, given black-box access to Ros_λ, one can reconstruct the matrix g via linear system solving, by considering $g\,\mathrm{Ros}_\lambda(b_i) = b_i^* g$ for a $\mathbb{Z}$-basis $b_1, \ldots, b_{16}$ of $\mathrm{M}_2(\mathcal{O}_0)$.

In a natural way, the matrix representation extends to polarized isogenies. Let $\lambda_1, \lambda_2 \in \mathrm{PPol}(A_0)$ be represented by matrices $g_1, g_2 \in \mathrm{Mat}(A_0)$ and let $\varphi : (A_0, \lambda_1) \to (A_0, \lambda_2)$ be a polarized isogeny of reduced degree N. Being an endomorphism of A_0, we can identify φ with a matrix $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$, and the property $\hat{\varphi}\lambda_2\varphi = N\lambda_1$ readily translates into

$$(\lambda_0^{-1}\hat{\varphi}\lambda_0)\lambda_0^{-1}\lambda_2\varphi = N\lambda_0^{-1}\lambda_1.$$

Using $\lambda_0^{-1}\lambda_i = g_i$ and identifying φ with γ, this can be rewritten as

$$\gamma^* g_2 \gamma = N g_1, \tag{2}$$

which is the chief equation of this entire paper. Conversely, whenever a matrix $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ satisfies (2), it determines a polarized isogeny $\varphi : (A_0, \lambda_1) \to (A_0, \lambda_2)$ of reduced degree N. In Section 4 we will discuss methods for converting polarized isogenies into matrices and vice versa.

We conclude with two remarks:

1. The equivalence relation for principal polarizations from Definition 2.7 naturally translates to the language of matrices as well: given $g_1, g_2 \in \mathrm{Mat}(A_0)$ encoding principal polarizations λ_1, λ_2 on A_0, we have

$$\lambda_1 \sim \lambda_2 \quad \Longleftrightarrow \quad \exists u \in \mathrm{GL}_2(\mathcal{O}_0), \quad u^* g_1 u = g_2.$$

   In this case, we say that the matrices are *congruent*; this terminology is taken from [24]. We then define $\mathrm{Mat}^0(A_0)$ as the set $\mathrm{Mat}(A_0)$ considered modulo congruence. Figure 1 summarizes the bijections that allow us to manipulate (isomorphism classes of) principally polarized superspecial abelian surfaces using only matrices with entries in $\mathcal{O}_0$.

[†] More generally, the adjoint of α with respect to $g_1 = \mu(\lambda_1)$, $g_2 = \mu(\lambda_2)$ is $g_1^{-1}\alpha^* g_2$.

$$\left\{\begin{array}{c}\text{Superspecial}\\ \text{principally polarized}\\ \text{abelian surfaces}\\ (A,\lambda_A)\\ \text{up to polarized}\\ \text{isomorphism}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{Principal}\\ \text{polarizations}\\ \lambda\in\mathrm{PPol}(A_0)\\ \text{up to equivalence}\end{array}\right\} \overset{\mu}{\longleftrightarrow} \left\{\begin{array}{c}\text{Matrices}\\ g\in\mathrm{Mat}(A_0)\\ \text{up to congruence}\end{array}\right\}$$

Fig. 1. Classification of principally polarized superspecial abelian surfaces

2. Every supersingular elliptic curve in characteristic p admits a model over $\mathbb{F}_{p^2}$, therefore the same is true for A_0 and the product polarization λ_0. When working with a model such that $\#A_0(\mathbb{F}_{p^2}) = (p \pm 1)^4$, as will be the case in practice, we know that all endomorphisms of A_0 are defined over $\mathbb{F}_{p^2}$ as well. Consequently, *every* principal polarization $\lambda = \lambda_0(\lambda_0^{-1}\lambda)$ is defined over $\mathbb{F}_{p^2}$. If (A, λ_A) is a superspecial principally polarized abelian surface defined over $\mathbb{F}_{p^2}$ such that $\#A(\mathbb{F}_{p^2}) = (p \pm 1)^4$, then it is $\mathbb{F}_{p^2}$-isomorphic to (A_0, λ) for some principal polarization λ on A_0. See [4] for an extended discussion.

2.4 Quaternionic matrices and determinants

When trying to define the determinant of a matrix

$$u = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(B_{p,\infty}),$$

care is needed in view of the non-commutativity. Note that there is no ambiguity in the Hermitian case (i.e., for matrices that are invariant under taking the conjugate-transpose), which are always defined over a quadratic, hence commutative, subfield of $B_{p,\infty}$. In particular, it makes sense to consider $\det(uu^*)$ instead. Alternatively, one can consider the (reduced) norm $\mathcal{N}(u)$, defined as $\det(\iota(u \otimes 1))$, where

$$\iota : \mathrm{M}_2(B_{p,\infty}) \otimes_{\mathbb{Q}} \mathbb{C} \to \mathrm{M}_4(\mathbb{C})$$

is any isomorphism of $\mathbb{C}$-algebras. As the following lemma shows, this leads to the same result.

Lemma 2.10. $\det(uu^*) = \det(u^*u) = \mathsf{n}(a)\,\mathsf{n}(d) + \mathsf{n}(b)\,\mathsf{n}(c) - \mathsf{tr}(\bar{a}b\bar{d}c) = \mathcal{N}(u)$.

One notable consequence of the above lemma is that the map $u \mapsto \det(uu^*)$ is multiplicative; indeed this property is immediate for $\mathcal{N}(-)$. Another interesting corollary, for which we could not find an explicit reference, is the following:

Corollary 2.11. *Let $E/\overline{\mathbb{F}}_p$ be a supersingular elliptic curve and let* $\mathrm{End}(E) \cong \mathcal{O} \subset B_{p,\infty}$. *Let $u \in \mathrm{End}(E^2)$, which via this isomorphism can be identified with an element of* $\mathrm{M}_2(\mathcal{O})$. *Then* $\deg u = \mathcal{N}(u)$.

Proof. This follows from (1) and an explicit calculation, see [6] for details. □

The multiplicativity also applies to the usual determinant when applied to Hermitian matrices. Up to sign, this is easy to see using that $\mathcal{N}(g) = \det(g)^2$ for any Hermitian matrix g. But the signs match as well:

Lemma 2.12. *Let $u, g, h \in \mathrm{M}_2(B_{p,\infty})$ where g, h are assumed Hermitian. Then*

- $\det(gh) = \det(g)\det(h)$,
- $\det(u^* g u) = \mathcal{N}(u)\det(g)$.

We end this section by showing that the "adjugate"[†] with respect to $\mathcal{N}(-)$ of an invertible matrix with entries in a subring $\mathcal{O} \subset B_{p,\infty}$ again has entries in $\mathcal{O}$.

Lemma 2.13. *If $u \in \mathrm{M}_2(\mathcal{O})$ is invertible in $\mathrm{M}_2(B_{p,\infty})$ then $u^{-1}\mathcal{N}(u) \in \mathrm{M}_2(\mathcal{O})$.*

3 Pathfinding in dimension 2

The goal of this section (and the main goal of the paper) is the description of an algorithm which solves the *algebraic pathfinding problem* in dimension 2. That is, upon input of $g_1, g_2 \in \mathrm{Mat}(A_0)$, the goal is to find a matrix $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ and a smooth integer N such that (2) holds. More precisely, we fix any small prime number ℓ and present the following solution, where N is a power of ℓ. Just as in the original KLPT algorithm, we assume that $\mathcal{O}_0$ is special extremal, i.e., it contains a quadratic order whose discriminant has a very small absolute value [30, §2.3]. In fact, for simplicity, we restrict to $p \equiv 3 \bmod 4$ and use the base curve $E_0 : y^2 = x^3 + x$ and maximal order $\mathcal{O}_0$ from Example 2.1. Note that the Gaussian integers $\mathbb{Z}[i]$ are contained in $\mathcal{O}_0$, so this order is of the desired kind.

Theorem 3.1 (KLPT^2). *There exists a polynomial-time algorithm which upon input $g_1, g_2 \in \mathrm{Mat}(A_0)$ and a prime number $\ell \neq p$, under plausible heuristic assumptions, returns $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ such that*

$$\gamma^* g_2 \gamma = \ell^e g_1$$

where $\ell^e \in O(p^{25+\varepsilon})$.

A proof-of-concept implementation of the algorithm can be found in:

`https://github.com/KLPT2/KLPT2`

[†] We intentionally avoid the word "adjoint", because the matrix $u^{-1}\mathcal{N}(u)$ should not be confused with the adjoint $\tilde{u}$ of u in the sense of Section 2.2. Firstly, the latter notion only makes sense when u describes a polarized isogeny with respect to certain principal polarizations. Secondly, in case it does make sense, we have $\tilde{u}u = u\tilde{u} = \mathrm{degrd}(u)\mathbb{I}_2$, whereas $u^{-1}\mathcal{N}(u)u = uu^{-1}\mathcal{N}(u) = \deg(u)\mathbb{I}_2 = \mathrm{degrd}(u)^2\mathbb{I}_2$ in view of Corollary 2.11. Recall that $\tilde{u} = g_1^{-1}u^* g_2$ when working with respect to principal polarizations associated with $g_1, g_2 \in \mathrm{Mat}(A_0)$.

Further down, in Theorem 3.15, we will present a variant for powersmooth N, which is often better-suited for (theoretically flavoured) applications.

Our implementation also supports the "plausible heuristic assumptions", which are hard to state out of context and will be highlighted during the description of the algorithm.

Remark 3.2. Our algorithm is randomized and expected to return a different matrix γ on each iteration. Unfortunately, the output never corresponds to a "good" chain of (ℓ, ℓ)-isogenies in the sense of [7], i.e., we never have $\ker(\gamma) \cong (\mathbb{Z}/\ell^e\mathbb{Z})^2$, see Corollary 5.4. In fact, as far as we are aware, even the mere connectedness of the superspecial (ℓ, ℓ)-isogeny graph by good isogeny chains is an open problem [7, Conjecture 3].

3.1 Finding connecting matrices

Our proof strategy for Theorem 3.1 is based on the following lemma.

Lemma 3.3. *Let $h_1, h_2 \in \mathrm{M}_2(\mathcal{O}_0)$ be Hermitian matrices with equal upper-left entries and equal determinants, i.e., we have*

$$h_1 = \begin{pmatrix} D & r_1 \\ \bar{r}_1 & t_1 \end{pmatrix}, \quad h_2 = \begin{pmatrix} D & r_2 \\ \bar{r}_2 & t_2 \end{pmatrix}$$

for $D, t_1, t_2 \in \mathbb{Z}, r_1, r_2 \in \mathcal{O}_0$ such that $Dt_1 - \mathsf{n}(r_1) = Dt_2 - \mathsf{n}(r_2)$. Then for

$$\tau = \begin{pmatrix} D & r_1 - r_2 \\ 0 & D \end{pmatrix}$$

we have $\tau^* h_2 \tau = D^2 h_1$.

Proof. Explicit calculation; see the full version of our paper [6] for details. □

Note that in the above lemma we do not impose $\det(h_1) = \det(h_2) = 1$, so this is not always a special case of (2). We only want the two determinants to be equal, for reasons that will become apparent soon.

When given g_1, g_2, our goal is to transform them in a fashion such that Lemma 3.3 becomes applicable. This is aided by the following lemma:

Lemma 3.4. *Assume that $\delta^* g_2 \delta = N u^* g_1 u$ with $N \in \mathbb{Z}$, $u, \delta \in \mathrm{M}_2(\mathcal{O}_0)$. Then there exists $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ such that $\gamma^* g_2 \gamma = N \mathcal{N}(u)^2 g_1$.*

Proof. One can choose $\gamma = \delta u^{-1} \mathcal{N}(u)$. The equality $\gamma^* g_2 \gamma = N \mathcal{N}(u)^2 g_1$ is clearly satisfied and Lemma 2.13 implies that $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$. □

This naturally leads to the following plan for solving the problem $\gamma^* g_2 \gamma = \ell^e g_1$. Namely, given $g \in \mathrm{Mat}(A_0)$ we want to find $u \in \mathrm{M}_2(\mathcal{O}_0)$ with the following properties:

- $\mathcal{N}(u) = \ell^{e_1}$ where e_1 does not depend on g (but u does).

– The top left entry of u^*gu is ℓ^{e_2}, where e_2 does not depend on g.

How does this solve our initial problem? First we transform g_1 and g_2 with an appropriate u_1 and u_2 in the above fashion. Then we invoke Lemma 3.3 as by design the two sides have the same top left entry and the same determinant, by Lemma 2.12. This yields a matrix $\tau \in \mathrm{M}_2(\mathcal{O}_0)$ such that

$$\tau^* u_2^* g_2 u_2 \tau = \ell^{2e_2} u_1^* g_1 u_1. \tag{3}$$

We can then apply Lemma 3.4 with $\delta = u_2\tau$ to return

$$\gamma = u_2 \tau u_1^{-1} \mathcal{N}(u_1), \tag{4}$$

which has reduced degree $\ell^{2(e_1+e_2)}$.

So now our focus is on a single

$$g = \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix} \in \mathrm{Mat}(A_0),$$

where along the way we will explicitly bound ℓ^{e_1}, ℓ^{e_2} by appropriate constants. First let us calculate what the top left entry of u^*gu is.

Lemma 3.6. *Let $u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then the top left corner of u^*gu is given by*

$$s' := s \cdot \mathsf{n}(a) + t \cdot \mathsf{n}(c) + \mathsf{tr}(\bar{c}\bar{r}a).$$

Proof. This follows from a simple calculation. □

Note in particular that the top left corner s' only depends on a and c (likewise, the bottom right corner t' only depends on b and d). This motivates the following rough strategy:

1. Find $a, c \in \mathcal{O}_0$ such that s' is a fixed power of ℓ.
2. Given a, c, find values for $b, d \in \mathcal{O}_0$ such that the reduced norm $\mathcal{N}(u)$ is another fixed power of ℓ.

We first concentrate on Step 2, then come back to Step 1 in Section 3.4.

3.2 Controlling the reduced norm

Let us be given non-zero $a, c \in \mathcal{O}_0$, where we assume that $\mathsf{n}(a)$ and $\mathsf{n}(c)$ are coprime; this will indeed be ensured. In this section we explain how to find $x, y \in \mathcal{O}_0$ such that

$$\mathcal{N}\begin{pmatrix} a & x \\ c & y \end{pmatrix} = \mathsf{n}(a)\,\mathsf{n}(y) + \mathsf{n}(c)\,\mathsf{n}(x) - \mathsf{tr}(\bar{a}x\bar{y}c) = \ell^{e_0}$$

for some fixed power ℓ^{e_0} (we will eventually have $e_1 = 2e_0$). We do not solve this Diophantine equation directly. Instead, one can see that the problem amounts to a pathfinding problem in dimension 1, so that we can invoke the standard KLPT algorithm. Indeed, an easy calculation shows

$$\mathsf{n}(c)\,\mathcal{N}\begin{pmatrix} a & x \\ c & y \end{pmatrix} = \mathsf{n}(a\bar{c}y) + \mathsf{n}(\mathsf{n}(c)x) - \mathsf{tr}(\mathsf{n}(c)x\overline{a\bar{c}y}) = \mathsf{n}(\mathsf{n}(c)x - a\bar{c}y) \tag{5}$$

so it suffices to find an ω of norm $\mathsf{n}(c)\ell^{e_0}$ in the right $\mathcal{O}_0$-ideal I generated by $\mathsf{n}(c)$ and $a\bar{c}$. Note that I has norm $\mathsf{n}(c)$ because $\gcd(\mathsf{n}(a), \mathsf{n}(c)) = 1$. We can therefore find such an ω with $\ell^{e_0} \in O(p^{3+\varepsilon})$ using the KLPT algorithm (heuristically). Writing $\omega = \mathsf{n}(c)o_1 + a\bar{c}o_2$, we can then simply put $x = o_1, y = -o_2$.

Equation (5) seemingly comes out of the blue, but there is a conceptual explanation for it, which is discussed in the full version of the paper [6] and which may be key to future improvements of the KLPT^2 algorithm.

3.3 Reduction of the matrix g

Thanks to the previous subsection, our task has been (essentially) reduced to finding $a, c \in \mathcal{O}_0$ in such a way that the top-left entry

$$s' = K((a,c)) := s \cdot \mathsf{n}(a) + t \cdot \mathsf{n}(c) + \mathsf{tr}(\bar{c}\bar{r}a) \tag{6}$$

of u^*gu is some fixed power of ℓ, only depending on p. Moreover, we want to make sure that $\mathsf{n}(a)$ and $\mathsf{n}(c)$ are non-zero and coprime. We see that K is a quadratic form on $\mathcal{O}_0^2$, which is a free $\mathbb{Z}$-module of rank 8.

Proposition 3.10. *The quadratic form K is positive definite and has determinant $(p/4)^4$.*

The goal of this subsection is to describe an intermediate step, where we wish to find a transformation matrix u making s' as small as possible. This can be achieved through lattice reduction: using Proposition 3.10, we see that (6) expresses s' as the squared-Euclidean length of a vector in a lattice $\Lambda \subset \mathbb{R}^8$ having volume $(p/4)^2$.[†] By the Minkowski bound we can find a non-zero vector with K-value $s' < \frac{3}{2}\sqrt{p}$. Once a, c realizing a small value of s' are found, we can complement them with b, d using the KLPT algorithm, as described in the previous subsection. However, remember that we want $\mathsf{n}(a)$ and $\mathsf{n}(c)$ to be coprime for this. Furthermore, to simplify the analysis in Theorem 3.13 below, we will want s' to be a prime different from 2 and ℓ. Therefore we need some extra margin; in the full version of our paper [6] we give a heuristic argumentation showing that $s' < \sqrt{p}(\ln p)^{1/4}$ should always be feasible.

Despite the smallness of s', the other entries of u^*gu may become quite large. Thus, we use an extra transformation to keep these values contained. For this we can use a matrix of the form $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)$. To lighten notation, let us explain this step directly on g, rather than on u^*gu:

$$\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)^* g \left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right) = \begin{pmatrix} s & \alpha s + r \\ \bar{\alpha}s + \bar{r} & \mathsf{n}(\alpha)s + \mathsf{tr}(\bar{\alpha}r) + t \end{pmatrix}$$

[†] E.g., this follows via the Cholesky decomposition of the matrix in the proof of Proposition 3.10.

The main observation here is twofold. First s does not change. Second r changes to $\alpha s + r$, thus we can attain anything in $\mathcal{O}_0$ that is congruent to r modulo s. In particular we can ensure that the coordinates $r_i, i = 1, \dots, 4$ of r with respect to the basis from Example 2.1 satisfy $|r_i| \leq s/2$. This implies that $\mathsf{n}(r) \leq s^2(p+5)/8$. Note that $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathcal{O}_0)$, hence we do not have to worry about the reduced norm in this step.

Applying this to

$$u^*gu = \begin{pmatrix} s' & r' \\ \bar{r}' & t' \end{pmatrix},$$

first note that

$$s't' - \mathsf{n}(r') = \mathcal{N}(u) = \ell^{e_0} \in O(p^{3+\varepsilon})$$

by the KLPT step, where we have used Lemma 2.12. Thus from $\mathsf{n}(r') \leq s'^2(p+5)/8$ and $s' \leq \sqrt{p}(\ln p)^{1/4}$, one finds that $t' \leq \ell^{e_0}/s' + s'(p+5)/8 \in O(p^{3+\varepsilon}/s')$.

Finally, we will also want that $\ell \nmid t'$, or equivalently $\ell \nmid \mathsf{n}(r')$. This is easy to achieve by slightly tweaking α if needed. Indeed, one easily checks that, by relaxing the bounds $|r_i| \leq s/2$ to $|r_i| \leq s$, it can be ensured that $\mathsf{tr}(r') \not\equiv -1 \bmod \ell$. Then, if it so happens that $\ell \mid \mathsf{n}(r')$, an extra transformation using $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ will fix this issue.

In summary, by applying a suitable transformation $g \leftarrow u^*gu$, we can reduce to the case where g has bounded entries satisfying some non-divisibility conditions, at the cost of increasing the determinant from 1 to a power of ℓ. For clarity we give a definition for this case, while adding in another heuristic assumption, which should be satisfied with overwhelming probablity:

Definition 3.12. *A matrix*

$$g = \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix}, \quad s, t \in \mathbb{Z}_{>0}, r \in \mathcal{O}_0, st - r\bar{r} > 0$$

is called ℓ-reduced *if*

- $\det(g) = st - \mathsf{n}(r) = \ell^{e_0}$ *for some* $e_0 \geq 0$*,*
- $s \leq \sqrt{p}(\ln p)^{1/4}$ *is a prime number not dividing* $2\ell t$*,*
- $\mathsf{n}(r) \leq s^2 p$ *is not a multiple of* ℓ*.*

The extra assumption is $s \nmid t$. Note that the conditions imply $s \nmid \mathsf{n}(r)$ and $\ell \nmid t$.

3.4 Controlling the top-left entry and finalizing the algorithm

Starting from a reduced matrix g as in Definition 3.12, with determinant $\ell^{e_0} \in O(p^{3+\varepsilon})$, we now show how to find a matrix u, of ℓ-power reduced norm, such that u^*gu has a top left corner equal to ℓ^{e_2} for some $e_2 \geq 0$. As discussed before, this amounts to solving the Diophantine equation

$$\ell^{e_2} = s\,\mathsf{n}(a) + t\,\mathsf{n}(c) + \mathsf{tr}(\bar{c}\bar{r}a) \tag{7}$$

in such a way that $\gcd(\mathsf{n}(a), \mathsf{n}(c)) = 1$, and complementing with appropriate b, d via the KLPT algorithm.

Theorem 3.13. *Let $g \in \mathrm{M}_2(\mathcal{O}_0)$ be an ℓ-reduced matrix as in Definition 3.12. There exists a (heuristic) polynomial-time algorithm that finds a solution to* (7) *with $\mathsf{n}(a)$ and $\mathsf{n}(c)$ coprime, provided that $\ell^{e_2} \in \Theta(p^{6.5+\varepsilon})$.*

Proof. We make the following restrictions: we take a of the form $a_1 + a_2 i \in \mathbb{Z}[i]$ and we take c of the form $c_1\bar{r}j + c_2\bar{r}k \in \bar{r}j\mathbb{Z}[i]$. Since $\mathsf{tr}(\bar{c}\bar{r}a)$ is zero for every such choice of a, c, equation (7) simplifies to $\ell^{e_2} = s\,\mathsf{n}(a) + t\,\mathsf{n}(c)$. We then solve the quadratic equation

$$t\,\mathsf{n}(c) = tp\,\mathsf{n}(r)(c_1^2 + c_2^2) \equiv \ell^{e_2} \bmod s.$$

Since s is an odd prime and $s \nmid t, p, \mathsf{n}(r), \ell$, this provides us with an irreducible conic equation over $\mathbb{F}_s$ which always has a solution: this gives us c, with $c_1, c_2 \in \{0, \ldots, s-1\}$. Now we have that $\ell^{e_2} - t\,\mathsf{n}(c)$ is divisible by s, reducing to

$$\frac{\ell^{e_2} - t\,\mathsf{n}(c)}{s} = \mathsf{n}(a). \tag{8}$$

Since $a \in \mathbb{Z}[i]$ this can be solved using Cornacchia's algorithm, provided we know the factorization of $\ell^{e_2} - t\,\mathsf{n}(c)$. Thus we iterate until (8) has a solution and we can factor $\ell^{e_2} - t\,\mathsf{n}(c)$ efficiently. Here one expects a polylogarithmic number of iterations. The reason for the size constraints on ℓ^{e_2} is that one needs $\ell^{e_2} - t\,\mathsf{n}(c)$ to be positive, as otherwise it cannot be the sum of two squares. From

$$t\,\mathsf{n}(c) = t \cdot p \cdot \mathsf{n}(r) \cdot (c_1^2 + c_2^2) \in O\left(\frac{p^{3+\varepsilon}}{s} \cdot p \cdot s^2 p \cdot 2s^2\right) \subset O(p^{6.5+\varepsilon})$$

the bound follows. Note that (8) does not guarantee that $\gcd(\mathsf{n}(a), \mathsf{n}(c)) = 1$, so a number of retries, each time choosing different representants of $c_1, c_2 \bmod s$ (or choosing a genuinely different solution to the above quadratic equation over $\mathbb{F}_s$), may be needed. This does not affect the above asymptotic estimate. □

Remark 3.14. In particular, from (8) it is clear that c should be chosen such that $\ell \nmid \mathsf{n}(c)$, for otherwise $\ell \mid \gcd(\mathsf{n}(a), \mathsf{n}(c))$. This is the reason for the condition $\ell \nmid \mathsf{n}(r)$ in Definition 3.12. It is interesting to specialize this to our main case of interest $\ell = 2$: both $\mathsf{n}(r)$ and $c_1^2 + c_2^2$ should be odd. Then, assuming $e_0, e_2 \geq 2$, equation (8) implies that

$$-t\,\mathsf{n}(c) = -tp\,\mathsf{n}(r)(c_1^2 + c_2^2) \equiv s\,\mathsf{n}(a) \bmod 4 \quad \Rightarrow \quad -t^2 p(c_1^2 + c_2^2) \equiv \mathsf{n}(a) \bmod 4,$$

showing that $\mathsf{n}(a) \equiv -1 \cdot 3 \cdot 1 \equiv 1 \bmod 4$. This is a necessary condition for the Cornacchia-step to succeed.

We are now ready to prove our main result:

Proof of Theorem 3.1: The algorithm to find $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ when given

$$g_1 = \begin{pmatrix} s_1 & r_1 \\ \bar{r}_1 & t_1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} s_2 & r_2 \\ \bar{r}_2 & t_2 \end{pmatrix} \quad \in \mathrm{Mat}(A_0)$$

is summarized in Algorithm 1. From the preceding discussions, it should be clear that all steps are heuristically polynomial-time. As for the output length, note that the matrices u_1, u_2 produced in Step 7 have reduced norm ℓ^{e_1} with $e_1 = 2e_0$, and for $i = 1, 2$ the upper-left entry of $u_i^* g_i u_i$ equals ℓ^{e_2}. Thus, from (4) we find that γ has reduced degree

$$\ell^e = \ell^{2(e_1+e_2)} = (\ell^{e_0})^4 \cdot (\ell^{e_2})^2 \in O(p^{12+\varepsilon} \cdot p^{13+\varepsilon})$$

in view of the KLPT bound and Theorem 3.13. □

Algorithm 1: KLPT^2: An algorithm to solve the quaternion ℓ-isogeny path problem in dimension 2

```
Input   : $g_1, g_2 \in \mathrm{Mat}(A_0)$
Output: $\gamma \in \mathrm{M}_2(\mathcal{O})$ such that $\gamma^* g_2 \gamma = \ell^e g_1$ with $\ell^e \in O(p^{25+\varepsilon})$
1 For i=1,2 do
2     Find $a, c$ using lattice reduction such that $\gcd(\mathsf{n}(a), \mathsf{n}(c)) = 1$, and
        $s_i\,\mathsf{n}(a) + t_i\,\mathsf{n}(c) + \mathsf{tr}(\bar{c}\bar{r}_i a) < \sqrt{p}(\ln p)^{1/4}$ is prime (not $2, \ell$).
3     Find $b, d$ using KLPT as described in Section 3.2 such that the
        reduced norm of $u := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is $\ell^{e_0}$.
4     Find $\alpha$ such that $g' = \left(\begin{smallmatrix} s' & r' \\ \bar{r}' & t' \end{smallmatrix}\right) := \left(\begin{smallmatrix} 1 & 0 \\ \bar{\alpha} & 1 \end{smallmatrix}\right) u^* g_i u \left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)$ is reduced.
5     Find $a', c'$ using lattice reduction such that $\gcd(\mathsf{n}(a'), n(c')) = 1$ and
        $s'\,\mathsf{n}(a') + t'\,\mathsf{n}(c') + \mathsf{tr}(\bar{c}'\bar{r}'a') = \ell^{e_2}$ using Theorem 3.13.
6     Find $b', d'$ using KLPT as described in Section 3.2 such that the
        reduced norm of $u' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$ is $\ell^{e_0}$.
7     Let $u_i = u \left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right) u'$.
8 Compute $\tau$ connecting $u_1^* g_1 u_1$ and $u_2^* g_2 u_2$ as in Lemma 3.3.
9 Return $\gamma := u_2 \tau u_1^{-1} \mathcal{N}(u_1)$ as in (4).
```

The algebraic pathfinding problem was studied here for $N = \ell^e$ similarly to the original KLPT algorithm. However, it is clear that both KLPT and Theorem 3.13 can be adjusted to any number that is big enough; see also [22]. Now by invoking powersmooth versions of KLPT and Theorem 3.13 we get a powersmooth degree isogeny, since the product of powersmooth numbers is still powersmooth. This implies the following version of Theorem 3.1:

Theorem 3.15. *There exists a (heuristic) polynomial-time algorithm which upon input $g_1, g_2 \in \mathrm{Mat}(A_0)$ and a smoothness bound B returns $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ such that*

$$\gamma^* g_2 \gamma = N g_1$$

where $N \in O(p^{25+\varepsilon})$ is B-powersmooth.

4 Translating between matrices and isogenies

The main applications of the standard KLPT algorithm go hand in hand with efficient methods for converting left (non-zero) ideals of $\mathcal{O}_0$ into isogenies emanating from E_0 and vice versa. Likewise, in order to put KLPT^2 to practical use, we need methods for translating appropriately chosen 2×2 matrices with entries in $\mathcal{O}_0$ to polarized isogenies emerging from A_0 and conversely.

The analogy with the elliptic curve case becomes more apparent when noting that $\mathrm{M}_2(\mathcal{O}_0)$ is a principal ideal ring. Consequently, we have a natural identification of left ideals $I \subset \mathrm{M}_2(\mathcal{O}_0)$ with their generating matrices $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$, up to left-multiplication with elements of $\mathrm{GL}_2(\mathcal{O}_0)$. On a high level, the known approaches for translating between ideals and isogenies in dimension one carry over to dimension two. But in the case of isogeny-to-ideal conversion there is an important caveat: the ideal returned by the standard isogeny-to-ideal approaches is described in terms of multiple generators, and extracting a single generating matrix from this description is not a trivial task. Indeed, a large part of Chu's thesis [11, Chapter 2] is devoted to the design of a sub-exponential time algorithm for solving this instance of the principal ideal problem (PIP).

In this section, we describe some first routines for converting matrices to isogenies and vice versa; our main result is presented in Section 4.2, where we show how to by-pass the PIP for powersmooth-degree isogenies. Then, in Section 5, we will enhance these basic routines through the use of KLPT^2.

Remark 4.1. At several points in the remainder of this article, we rely on an algorithm which upon input of

- a principally polarized abelian surface A over a finite field $\mathbb{F}_q$, described either as the Jacobian of an explicit genus-2 curve $C/\mathbb{F}_q$ (with the canonical polarization) or as the product of two explicit elliptic curves E_1, E_2 over $\mathbb{F}_q$ (with the product polarization),
- a subgroup $K \subset A(\mathbb{F}_q)$ which is also a maximal isotropic subgroup of $A[\ell^e]$ with respect to the ℓ^e-Weil pairing, for some given prime power ℓ^e,
- a point $P \in A(\mathbb{F}_q)$,

computes, in time polynomial in $\log q$ and ℓ, the codomain of a polarized isogeny φ with kernel K, again described as either an explicit Jacobian or an explicit product of two elliptic curves,[†] along with the image point $\varphi(P)$. E.g., if $\ell = 2$ then this can be done through an e-fold application of the classical formulae due to Richelot [39]; the occasional gluing and splitting steps can be handled using [25]. In general, the existence of such an algorithm is considered "folklore". While large parts of this task are handled by [13], a ready-to-use reference that does this in complete generality appears to be lacking.

[†] In general, it is possible that this concerns a pair of conjugate elliptic curves over $\mathbb{F}_{q^2}$, i.e., the codomain concerns a Weil restriction. But in our case, where we work with superspecial abelian surfaces over an extension of $\mathbb{F}_{p^2}$, this does not occur: the two elliptic curves are necessarily supersingular, hence can be defined over $\mathbb{F}_{p^2}$.

4.1 Matrices to polarized isogenies from A_0

This is stated in [11, Section A.2] as a "required routine", but no details are given, even though the method is not too surprising. The input is a matrix $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ of reduced norm N^2, where $N = N_1 N_2 \cdots N_r$ is assumed powersmooth, i.e., the factors N_i are pairwise coprime and bounded by B for some constant $B = \mathrm{poly}(\log p)$. In view of Remark 2.5, we also assume that the kernel of γ, when identified with an endomorphism of A_0, is a maximal isotropic subgroup of $A_0[N]$ with respect to the N-Weil pairing for the product polarization λ_0. (If γ fails to meet this condition, then our method will detect this along the way.) The desired output is a chain of polarized isogenies

$$A_0 \xrightarrow{\varphi_1} A_1 \xrightarrow{\varphi_2} A_2 \xrightarrow{\varphi_3} \dots \xrightarrow{\varphi_r} A_r \tag{9}$$

of respective reduced degrees N_i, such that $\ker(\gamma) = \ker(\varphi_r \circ \cdots \circ \varphi_2 \circ \varphi_1)$, where each A_i is either a product $E_1 \times E_2$ of two elliptic curves equipped with the product polarization, or the Jacobian $\mathrm{Jac}(C)$ of a curve of genus 2 equipped with the canonical polarization. The method is summarized in Algorithm 2. We refer to the full version of our paper [6] for a more detailed discussion.

Algorithm 2: MatrixToIsogeny: powersmooth degree

```
Input  : $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ with $\mathrm{degrd}(\gamma) = N_1 \cdots N_r$ powersmooth
Output: polarized isogenies $\varphi_r \circ \cdots \circ \varphi_1 : A_0 \to A_r$ with $\mathrm{degrd}\,\varphi_i = N_i$

$\tilde{\gamma} \leftarrow N\gamma^{-1}$, $\varphi_0 = \mathrm{id}$.
For $i = 1, \dots, r$ do
    $P_i, Q_i \leftarrow$ basis of $E_0[N_i]$.
    $S_i \leftarrow \tilde{\gamma}\,(\{(P_i, 0), (0, P_i), (Q_i, 0), (0, Q_i)\})$.
        // Generators of $(\ker \gamma)[N_i]$.
For $i = 1, \dots, r$ do
    $S_i \leftarrow (\varphi_{i-1} \circ \cdots \circ \varphi_0)(S_i)$.
    $\varphi_i \leftarrow$ isogeny $A_{i-1} \to A_i$ with kernel $\langle S_i \rangle$.
Return $\varphi_r \circ \cdots \circ \varphi_1 : A_0 \to A_r$.
```

4.2 Polarized isogenies from A_0 to matrices

Conversely, given a chain of polarized isogenies emanating from A_0 as in (9), where the degrees $N_i = \deg \varphi_i$ are pairwise coprime and bounded by B, here the goal is to produce a matrix $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ such that $\ker(\gamma) = \ker(\varphi_r \cdots \varphi_2 \circ \varphi_1)$. Such a matrix is uniquely determined up to left-multiplication with an element of $\mathrm{GL}_2(\mathcal{O}_0)$ and will automatically satisfy

$$\gamma^* g_r \gamma = N \cdot \mathbb{I}_2$$

with $N = N_1 N_2 \cdots N_r$, for some representant $g_r \in \mathrm{Mat}(A_0)$ of the class in $\mathrm{Mat}^0(A_0)$ corresponding to the principally polarized abelian surface A_r. Note that g_r can then be computed as $N\gamma^{*-1}\gamma^{-1} = N(\gamma\gamma^*)^{-1}$.

This conversion can be done as in Algorithm 3, which at a high level coincides with Chu's method from [11, Algorithm A.2.2]. Concerning Step 3, recall that $N_i \leq B$ implies that the elements of G_i are defined over an extension field of degree $O(B^2)$. The main difference with Chu's method lies in how we handle Step 6, which we have labeled as the "key step". This is where Chu invokes a sub-exponential time algorithm for the PIP in $\mathrm{M}_2(\mathcal{O}_0)$, described in [11, Chapter 2]. We by-pass the need for invoking a PIP solver, by instead running the following polynomial-time method. It is clear that we can assume that $N_i = \ell^e$ equals a power of a prime number ℓ.

Algorithm 3: IsogenyToMatrix: powersmooth degree

```
Input  : chain $\varphi_r \circ \cdots \circ \varphi_1 : A_0 \to A_r$ of polarized isogenies
         with $N_i := \mathrm{degrd}(\varphi_i) \leq B$ pairwise coprime
Output: $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ such that $\ker(\gamma) = \ker(\varphi_r \circ \cdots \circ \varphi_1)$,
         $g_r \in \mathrm{Mat}(A_0)$ corresponding to $A_r$
1 $\gamma \leftarrow \mathbb{I}_2$.
2 For $i = 1, \ldots, r$ do
3     $G_i \leftarrow (\tilde{\varphi}_{i-1} \circ \cdots \circ \tilde{\varphi}_2 \circ \tilde{\varphi}_1)(\ker \varphi_i) \subset A_0[N_i]$.
4         // Pulling back the kernel of $\varphi_i$ to $A_0$.
5     $K_i \leftarrow \gamma(G_i)$. // Pushing the kernel forward under $\gamma$.
6     $\gamma_i \leftarrow$ matrix with kernel $K_i$. // *** key step ***
7     $\gamma \leftarrow \gamma_i \gamma$.
8 Return $\gamma$,  $N_1 \cdots N_r (\gamma\gamma^*)^{-1}$.
```

We first describe the method in case $e = 1$, i.e., $N_i = \ell$. Then $K_i \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. Consider $A_0 = E_0^2$ together with the natural projection maps

$$\begin{tikzcd} & E_0 \times E_0 \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\ E_0 & & E_0 \end{tikzcd}$$

For each $j = 1, 2$ the projected subgroup $\pi_j(K_i) \subset E_0[\ell]$ is either trivial, a cyclic subgroup of order ℓ, or all of $E_0[\ell]$. Moreover, if $\pi_1(K_i), \pi_2(K_i) \subsetneq E_0[\ell]$ then necessarily both groups are cyclic, i.e., $K_i = \langle (P, \infty), (\infty, Q) \rangle$ for order-ℓ points $P, Q \in E_0$. Based on this observation, we make a case distinction:

(i) Assume $\pi_1(K_i) = E_0[\ell]$. Let P_1, P_2 be a basis of $E_0[\ell]$. Then

$$(P_1, \lambda_{11} P_1 + \lambda_{12} P_2),\ (P_2, \lambda_{21} P_1 + \lambda_{22} P_2)\ \in K_i$$

for certain integers λ_{jk}, and these points necessarily generate K_i. We claim that we can find an endomorphism $a \in \mathcal{O}_0$ such that

$$a(P_j) = \lambda_{j1} P_1 + \lambda_{j2} P_2$$

for $j = 1, 2$, so that $K_i = \langle (P_1, a(P_1)), (P_2, a(P_2)) \rangle$ and then we can take

$$\gamma_i = \begin{pmatrix} \ell & 0 \\ -a & 1 \end{pmatrix}$$

whose kernel contains K_i (but then for norm reasons equality must hold). The existence of a follows because the ℓ^4 elements of $\mathcal{O}_0/\ell\mathcal{O}_0$ all act differently on $E_0[\ell]$ (indeed, if two endomorphisms a_1, a_2 are such that $E_0[\ell] \subset \ker(a_1 - a_2)$, then necessarily $\ell \mid a_1 - a_2$). In practice, finding a is just an easy linear algebra problem mod ℓ (express a as an unknown linear combination of the basis from Example 2.1, evaluate at P_1, P_2, and solve for the coefficients).

(ii) Assume $\pi_2(K_i) = E_0[\ell]$: this is of course entirely analogous, leading to a matrix of the form

$$\gamma_i = \begin{pmatrix} 1 & -a \\ 0 & \ell \end{pmatrix}.$$

(iii) If $K_i = \langle (P, \infty), (\infty, Q) \rangle$ for order-ℓ points $P, Q \in E_0$, then we can easily find an endomorphism $b \in \mathcal{O}_0$ such that $b(Q) \notin \langle P \rangle$.[†] The matrix

$$\gamma_0 = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_0)$$

transforms K_i into the group $\gamma_0(K_i) = \langle (P, \infty), (b(Q), Q) \rangle$. This group satisfies $\pi_1(\gamma_0(K_i)) = E_0[\ell]$, so using (i) we can find a matrix γ_0' such that $\gamma_0'(\gamma_0(K_i)) = 0$. Letting $\gamma_i = \gamma_0' \gamma_0$, for norm reasons we can conclude that $\ker(\gamma_i) = K_i$.

The case where $N_i = \ell^e$ for arbitrary $e \geq 1$ can be handled by iterating this procedure. For ease of exposition, let us first assume that

$$K_i \cong \frac{\mathbb{Z}}{\ell^e \mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^e \mathbb{Z}}.$$

Then the method is totally straightforward and can be found in Algorithm 4. Note that this algorithm does not assume that ℓ^e is polynomially bounded, i.e., we can drop the powersmoothness assumption, as long as the elements of K_i are defined over $\mathbb{F}_{p^2}$ or a small-degree extension thereof.[‡]

[†] We thank the ISOCRYPT brainstorm team for their help with this step.

[‡] Of course, this rationality assumption still comes with an implicit bound, i.e., of the kind $\ell^e \mid p^r - (-1)^r$ with r the extension degree. In Section 5.2 we will use the KLPT^2 algorithm to get rid of this bound.

Algorithm 4: IsogenyToMatrix: ℓ-power degree

```
Input  : subgroup $K \cong (\mathbb{Z}/\ell^e\mathbb{Z})^2$ of $A_0$ generated by points defined
         over a small extension of $\mathbb{F}_{p^2}$
Output: $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ such that $\ker(\gamma) = K$
1 $\gamma \leftarrow \mathbb{I}_2$,  $K_1 \leftarrow K$.
2 For $i = 1, \ldots, e$ do
3     $G_i \leftarrow \ell^{e-i} K_i$.
4     $\gamma_i \leftarrow$ matrix with kernel $G_i$.  // Method for $(\ell,\ell)$-subgroups.
5     $\gamma \leftarrow \gamma_i \gamma$,  $K_{i+1} \leftarrow \gamma_i(K_i)$.
6 Return $\gamma$.
```

This method can be easily adapted to work for arbitrary kernel types, i.e., of the form

$$K_i \cong \frac{\mathbb{Z}}{\ell^e\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{e-f}\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^f\mathbb{Z}}$$

for some $f \in \{0 \ldots, \lfloor e/2 \rfloor\}$ [21, Proposition 2], again as long as this kernel is generated by points defined over a small extension of $\mathbb{F}_{p^2}$. (We can always reduce to the case of 3 or fewer generators: if there are 4 generators then the corresponding matrix γ_i factors through $\ell\mathbb{I}_2$ and one can reduce to the case of reduced degree ℓ^{e-2}.) The main caveat lies in Step 3 of Algorithm 4, where one should be more careful: indeed, in this case $\ell^{e-1}K_i \ncong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. A clean workaround, which serves as a warm-up for Section 5.4, is to define the subgroup

$$K_i' = \langle \ell^{e-f}P, R \rangle \cong \frac{\mathbb{Z}}{\ell^f\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^f\mathbb{Z}}$$

with $P \in K_i$ any point of order ℓ^e and $R \in K_i$ any point of order ℓ^f that is not halvable in K_i. Since $e_{\ell^f,\lambda_0}(\ell^{e-f}P, R) = e_{\ell^e,\lambda_0}(P, R) = 1$, this concerns a maximal isotropic subgroup of $A_0[\ell^f]$. We can now run Algorithm 4 on input K_i', returning a matrix γ_i', and then rerun the algorithm on input

$$\gamma_i'(K_i') \cong K_i/K_i' \cong \frac{\mathbb{Z}}{\ell^{e-f}\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{e-f}\mathbb{Z}},$$

after initializing $\gamma \leftarrow \gamma_i'$ rather than $\gamma \leftarrow \mathbb{I}_2$ in Step 1.

5 Applications of KLPT^2

We are ready to discuss a number of applications of the KLPT^2 algorithm.

5.1 Constructive IKO correspondence

For elliptic curves, the *constructive Deuring correspondence* asks to solve the following problem: upon input of a maximal order $\mathcal{O} \subset B_{p,\infty}$, return a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ such that $\mathrm{End}(E) \cong \mathcal{O}$. The KLPT algorithm can be turned into a heuristic polynomial-time algorithm for solving this problem. At a high level, the method works as follows. One starts from an elliptic curve $E_0/\mathbb{F}_{p^2}$ having a known, special extremal endomorphism ring $\mathrm{End}(E_0) \cong \mathcal{O}_0$. Using the KLPT algorithm, one computes a left ideal $I \subset \mathcal{O}_0$ of powersmooth norm N connecting $\mathcal{O}_0$ and $\mathcal{O}$. This ideal can then be converted into an isogeny emerging from E_0 using the elliptic-curve counterpart of Algorithm 2. The codomain of this isogeny is a valid output for the constructive Deuring correspondence.

For *unpolarized* superspecial abelian surfaces, the direct analog of the constructive Deuring correspondence is void: all such surfaces are pairwise isomorphic and therefore share the same endomorphism ring, namely $\mathrm{M}_2(\mathcal{O}_0)$. However, in the principally polarized case, the endomorphism ring comes equipped with an extra datum: the Rosati involution, which as explained in Remark 2.9 is completely encoded in the matrix $g \in \mathrm{Mat}(A_0)$ corresponding to λ. Therefore, a more meaningful counterpart of the constructive Deuring correspondence reads:

Theorem 5.1 (constructive IKO correspondence). *There exists a (heuristic) polynomial-time algorithm which upon input $g \in \mathrm{Mat}(A_0)$, either finds two elliptic curves E_1, E_2 or finds a genus-2 curve C such that for*

$$\begin{aligned}(A,\lambda) &= (E_1 \times E_2, \textit{product polarization}), \quad \textit{resp.}\\ (A,\lambda) &= (\mathrm{Jac}(C), \textit{canonical polarization}),\end{aligned}$$

we have $(A,\lambda) \cong (A_0, \mu^{-1}(g))$, with μ the map from Theorem 2.8.

Proof. Using our pathfinding algorithm from Theorem 3.15 we can find $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ such that

$$\gamma^* g \gamma = N\mathbb{I}_2,$$

with N powersmooth. To produce the desired output, one then simply converts γ into a polarized isogeny emanating from A_0 using Algorithm 2. If the codomain of this polarized isogeny is a product $E_1 \times E_2$, we output E_1, E_2; when landing on a Jacobian $\mathrm{Jac}(C)$, output C. □

5.2 Relaxing powersmoothness assumptions when translating between matrices and isogenies

(i) Matrices to isogenies from A_0 in arbitrary degree. Let us be given a matrix $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ as in Section 4.1, but we drop the assumption that N is powersmooth. We claim that, using KLPT^2, we can nevertheless convert γ into a polarized isogeny φ emanating from A_0. This mimicks well-known techniques from the elliptic curve case [18, 42]. First, recall that a matrix $g \in \mathrm{Mat}(A_0)$ representing the codomain can be computed as $g = N(\gamma\gamma^*)^{-1}$. Then, using Theorem 3.15, we can find a matrix γ' and a powersmooth integer N' such that $\gamma'^* g \gamma' = N' \cdot \mathbb{I}_2$, and we know that γ, γ' correspond to polarized isogenies φ, φ' with the same codomain, i.e. $\varphi, \varphi' : A_0 \to A$, where $\mathrm{degrd}(\varphi) = N$ and $\mathrm{degrd}(\varphi') = N'$. We can compute φ' as a composition of small-degree isogenies using Algorithm 2, which also reveals A. We have $N'\varphi = \varphi'\tilde{\varphi}'\varphi$ where we note that

$$\tilde{\varphi}'\varphi = \lambda_0^{-1}\hat{\varphi}'\lambda\varphi = \lambda_0^{-1}\hat{\varphi}'\lambda_0\,\lambda_0^{-1}\lambda\,\varphi \ \in \mathrm{End}(A_0)$$

can be identified with $\gamma'^* g\gamma \in \mathrm{M}_2(\mathcal{O}_0)$. Thus we can evaluate

$$\varphi(P) = \frac{1}{N'}\varphi'(\gamma'^* g\gamma P)$$

on any input point P whose order is coprime with N'. This is enough for considering φ as being known, e.g., in view of [36, 37].

Remark 5.2 (matrices to isogenies from A_0 in smooth degree). If N is smooth (but not powersmooth, so that Algorithm 2 may not be applicable) then the above "evaluation representation" of φ may not be the preferred format. Rather, one may want an explicit decomposition $\varphi = \varphi_r \circ \cdots \circ \varphi_1$ into isogenies of small degree. A polynomial-time conversion between these formats is possible through a repeated use of a higher-dimensional analogue of [37, Corollary 6.8], but this seems impractical. Alternatively, this can be handled using multiple applications of KLPT^2 as outlined in Algorithm 5.

Algorithm 5: MatrixToIsogeny: smooth degree

```
Input  : $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ with $\mathrm{degrd}(\gamma) = N_1 N_2 \cdots N_e$ where $N_i \leq B$
Output: polarized isogenies $\varphi_e \circ \cdots \circ \varphi_1 : A_0 \to A_e$ with $\mathrm{degrd}\,\varphi_i = N_i$
For $i = 1, \ldots, e-1$ do
    $G_i \leftarrow (\ker\gamma)[N_i]$.
    $\gamma_i \leftarrow$ matrix with kernel $G_i$. // Step 6 in Algorithm 3.
    $\gamma \leftarrow \gamma\gamma_i^{-1}$.
$\gamma_e \leftarrow \gamma$, $\gamma \leftarrow \mathbb{I}_2$.
    // Input $\gamma$ decomposed as $\gamma_e \cdots \gamma_1$; then reinitialize $\gamma$.
For $i = 1, \ldots, e$ do
    $\gamma \leftarrow \gamma_i\gamma$.
    $g_i \leftarrow N_1 N_2 \cdots N_i (\gamma\gamma^*)^{-1}$. // Codomain matrix of $\varphi_i$.
    Find $\gamma' \in \mathrm{M}_2(\mathcal{O}_0)$ and powersmooth $N'$ coprime with $N_1 N_2 \cdots N_i$
      s.t. $\gamma'^* g_i \gamma' = N' \cdot \mathbb{I}_2$. // Mild strengthening of Thm 3.15.
    Using Algorithm 2, convert $\gamma'$ to polarized isogeny $\varphi' : A_0 \to A_i$.
    $G_i \leftarrow \ker(\tilde{\gamma}\gamma')[N_i]$. // Note $\tilde{\gamma} = N_1 N_2 \cdots N_i \gamma^{-1}$.
    $\varphi_i \leftarrow$ adjoint of isogeny $A_i \to A_{i-1}$ with kernel $\varphi'(G_i)$.
Return $\varphi_e \circ \cdots \circ \varphi_1 : A_0 \to A_e$.
```

(ii) Isogenies from A_0 to matrices in smooth degree. The KLPT^2 algorithm can also be used to convert polarized isogenies from A_0 into matrices when the degree is smooth, rather than powersmooth. For this we recycle a trick due to Eisenträger, Hallgren, Lauter, Morrison and Petit [18, Algorithm 9]; see also

Wesolowski [42, Algorithm 3]. The method is detailed in Algorithm 6, where we note that Steps 3–9 are trivial at iteration $i = 1$.

Algorithm 6: IsogenyToMatrix: smooth degree

```
   Input  : chain $\varphi_r \circ \cdots \circ \varphi_1 : A_0 \to A_r$ of polarized isogenies
            with $N_i := \mathrm{degrd}(\varphi_i) \leq B$
   Output: $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ such that $\ker(\gamma) = \ker(\varphi_r \circ \cdots \circ \varphi_1)$,
            $g_r \in \mathrm{Mat}(A_0)$ corresponding to $A_r$
1  $\gamma \leftarrow \mathbb{I}_2$.
2  For $i = 1, \ldots, r$ do
3      $g_i \leftarrow N_1 \cdots N_{i-1}(\gamma\gamma^*)^{-1}$. // Codomain matrix of $\varphi_{i-1}$.
4      Find $\gamma' \in \mathrm{M}_2(\mathcal{O}_0)$ and powersmooth $N'$ with $\gcd(N', N_i) = 1$ and
        $\gamma'^* g_i \gamma' = N' \cdot \mathbb{I}_2$. // Mild strengthening of Theorem 3.15.
5      Using Algorithm 2, convert $\gamma'$ to polarized isogeny $\varphi' : A_0 \to A_{i-1}$.
6          // Domain of $\varphi_i$.
7      $G_i \leftarrow \tilde{\varphi}'(\ker \varphi_i) \subset A_0[N_i]$.
8          // Pulling back the kernel of $\varphi_i$ to $A_0$.
9      $K_i \leftarrow \gamma'(G_i)$. // Pushing the kernel forward under $\gamma'$.
10     $\gamma_i \leftarrow$ matrix with kernel $K_i$. // Step 6 in Algorithm 3.
11     $\gamma \leftarrow \gamma_i \gamma$
12 Return $\gamma$, $N_1 \cdots N_r(\gamma\gamma^*)^{-1}$.
```

5.3 Translating between matrices and isogenies from other starting surfaces

(i) Matrices to polarized isogenies. Next, let us be given a matrix $g_1 \in \mathrm{Mat}(A_0)$ and a matrix $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ of reduced norm N^2 (for arbitrary N), with the promise that γ defines a polarized isogeny emanating from (A_0, λ_1), where $\lambda_1 = \mu^{-1}(g_1)$ is the principal polarization corresponding to g_1. Our goal is to tackle the following enhanced version of the constructive IKO correspondence: return the top row in a commutative diagram of the form

$$\begin{tikzcd}
\begin{matrix}\mathrm{Jac}(C_1) \text{ or} \\ E_{11} \times E_{12}\end{matrix} \arrow[r, "\varphi"] \arrow[d, "\cong"'] & \begin{matrix}\mathrm{Jac}(C_2) \text{ or} \\ E_{21} \times E_{22}\end{matrix} \arrow[d, "\cong"] \\
(A_0, \lambda_1) \arrow[r, "\gamma"] & (A_0, \lambda_2).
\end{tikzcd}$$

That is, for $i = 1, 2$ one should return the underlying genus-2 curve C_i or elliptic curves E_{i1}, E_{i2}, along with an efficient representation of φ. This can be done as follows. If N is powersmooth, then using a mild strengthening of Theorem 3.15 we can compute a matrix $\kappa \in \mathrm{M}_2(\mathcal{O}_0)$ and a powersmooth integer K such that

$\gcd(K, N) = 1$ and $\kappa^* g_1 \kappa = K \cdot \mathbb{I}_2$. This implies that

$$(\gamma\kappa)^* g_2 (\gamma\kappa) = NK \cdot \mathbb{I}_2$$

with $g_2 = \mu(\lambda_2) = N\gamma^{*-1} g_1 \gamma^{-1}$. We can then run Algorithm 2 on input $\gamma\kappa$, first processing the factors of K, to end up with an isogeny that naturally factors as

$$(A_0, \lambda_0) \longrightarrow \begin{array}{c}\mathrm{Jac}(C_1)\text{ or}\\ E_{11} \times E_{12}\end{array} \xrightarrow{\varphi} \begin{array}{c}\mathrm{Jac}(C_2)\text{ or}\\ E_{21} \times E_{22}\end{array} :$$

hence the desired output. If N is not powersmooth then we first apply Theorem 3.15 to replace γ with a matrix γ' of powersmooth reduced norm N'^2 (i.e., satisfying $\gamma'^* g_2 \gamma' = N' \cdot g_1$) and proceed as in Section 5.2.

(ii) Polarized isogenies to matrices. We can easily extend the foregoing methods for isogeny-to-matrix conversion from (A_0, λ_0) to any principally polarized starting surface (A, λ), say given as a Jacobian $\mathrm{Jac}(C)$ or a product of elliptic curves $E_1 \times E_2$, as soon as a corresponding matrix $g \in \mathrm{Mat}(A_0)$ is known. As for the output matrix,

- let us recall from Section 4.2 that it is determined up to left-multiplication with an element of $\mathrm{GL}_2(\mathcal{O}_0)$ only,
- in addition, if in the method below one replaces g with a different representant of its class in $\mathrm{Mat}^0(A_0)$, then this amounts to *right*-multiplication with an element of $\mathrm{GL}_2(\mathcal{O}_0)$.

The problem of isogeny-to-matrix conversion easily reduces to the case $(A, \lambda) = (A_0, \lambda_0)$. Indeed, by means of Theorem 3.1 we can find a matrix γ' with reduced degree 2^e connecting $\mathbb{I}_2$ and g. Using Algorithm 5 this matrix can be converted into a polarized isogeny $\varphi' : (A_0, \lambda_0) \to (A, \lambda)$, represented as a chain of $(2, 2)$-isogenies. Now if φ is a polarized isogeny emanating from (A, λ), then $\varphi \circ \varphi'$ is a polarized isogeny emanating from (A, λ_0), and if γ is a matrix corresponding to $\varphi \circ \varphi'$, then $\gamma\gamma'^{-1}$ is a matrix corresponding to φ.

5.4 Attacks on CGL hash functions

We now arrive at our main cryptographic application: finding collisions for two-dimensional variants of the Charles–Goren–Lauter (CGL) hash function [8], in the case of an untrusted set-up.

CGL hash functions in dimension two. In 2018, Takashima [40] proposed the first such variant, using random non-backtracking walks in the $(2, 2)$-isogeny graph of superspecial principally polarized abelian surfaces. It was observed by Flynn and Ti [21] that such hash functions admit trivial collisions, coming from the fact that every $(4, 2, 2)$-isogeny admits three different decompositions into two $(2, 2)$-isogenies. Therefore, starting with [7], all subsequent proposals restrict to "good" chains of $(2,2)$-isogenies, i.e., composing to a $(2^e, 2^e)$-isogeny for some $e \geq 1$. This means that the kernel of every outgoing $(2,2)$-isogeny trivially intersects the kernel of the dual of the previous, incoming $(2,2)$-isogeny.[†]

Let us briefly detail how CGL hash functions in dimension two are currently constructed, generalizing from $(2,2)$-isogenies to (ℓ,ℓ)-isogenies for any small prime ℓ. During set-up, an initial node in the graph is chosen, corresponding to some superspecial principally polarized abelian surface A_1, as well as ℓ^3 "allowed" outgoing edges, corresponding to a subset of the set of $(\ell^2+1)(\ell+1)$ outgoing polarized (ℓ,ℓ)-isogenies from this initial node. At each node, the outgoing edges are sorted in some deterministic way; e.g. by comparing the invariants of all the neighbor nodes. The input message mess is mapped deterministically to $(m_1, m_2, \ldots, m_k) \in \{0, 1, \ldots, \ell^3 - 1\}^*$, with some padding if necessary. To hash, one of the ℓ^3 allowed edges is chosen according to the value of m_1, and we compute the corresponding neighbor node, yielding a new principally polarized abelian surface A_2. Using the value m_2, we choose one of the ℓ^3 outgoing edges corresponding to an (ℓ,ℓ)-isogeny whose kernel trivially intersects the kernel of the dual of the previous (ℓ,ℓ)-isogeny. This results in a node corresponding to a surface A_3 and we repeat this process until we have landed on a node corresponding to a surface A_{k+1}. We deterministically map suitable invariants of A_{k+1} to $\{0,1\}^n$, where $n \approx 3\log p$, and use this as the output of our hash function.

KLPT^2 produces "bad" chains. In dimension one, the KLPT algorithm can be used to compute second pre-images for the CGL hash function as soon as the endomorphism ring of the starting curve is known [18]. In dimension two, a very similar reasoning applies as soon as a matrix $g_1 \in \mathrm{Mat}(A_0)$ corresponding to the initial node is known: given a message mess_1,

- using the method from Section 5.3(ii), one can compute a matrix g_{k+1} corresponding to its hash value A_{k+1},
- using KLPT^2 on input g_1, g_{k+1}, one then computes a connecting matrix γ corresponding to a polarized isogeny of reduced degree ℓ^e; with overwhelming probability this will be different from the isogeny hashing mess_1,
- as outlined in Section 5.3(i), one can then effectively convert γ into a chain of (ℓ,ℓ)-isogenies from A_1 to A_{k+1}.

But, alas, this chain will fail to hash a second pre-image mess_2, because with overwhelming probability it will not be a "good" chain. Indeed, in general, KLPT^2 fails to return (ℓ^e, ℓ^e)-isogenies in view of Corollary 5.4 below:

Lemma 5.3. *Let $a, c \in \mathcal{O}_0$ be non-zero elements such that* $\gcd(\mathsf{n}(a), \mathsf{n}(c)) = 1$ *and assume that $\ell \nmid \mathsf{n}(a), \mathsf{n}(c)$. Let $b, d \in \mathcal{O}_0$ be such that*

$$\mathcal{N}(u) = \ell^{e_0}, \qquad u = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

[†] Rather than merely not coinciding with it: this is how "non-backtracking" was understood in Takashima's proposal [40].

computed by finding an element of norm $\mathsf{n}(c)\ell^{e_0}$ *in* $\mathsf{n}(c)\mathcal{O}_0 + a\bar{c}\mathcal{O}_0$ *via the KLPT algorithm, as explained in Section 3.2. Assume that the degree-*ℓ^{e_0} *component of this element is cyclic (this is generically expected). Then* $\ker(u) \cong \mathbb{Z}/\ell^{e_0}\mathbb{Z}$*.*

Corollary 5.4. *Under the assumption from Lemma 5.3 that the KLPT algorithm produces cyclic isogenies, to describe the kernel of the matrix* $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ *returned by Algorithm 1, one needs at least* 3 *generators.*

Under plausible heuristic assumptions, one can be more precise about the structure of $\ker(\gamma)$. In the full version of our paper [6], we argue that

$$\ker(\gamma) \cong \frac{\mathbb{Z}}{\ell^{2e_1+2e_2}\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{e_1+2e_2}\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{e_1}\mathbb{Z}} \tag{10}$$

holds with a probability that is bounded (from below) by a constant only depending on ℓ and converging to 1 as $\ell \to \infty$. Consequently, this is expected to be true after a constant number of reruns of KLPT^2 if needed. Here the exponents e_1, e_2 are as in Section 3.1; recall from (4) that the final exponent e arises as $2e_1 + 2e_2$ with $e_1 = 2e_0$. We stress that, while it is convenient to restrict to the shape (10) for expository purposes, our collision finding method outlined below can be adapted to any other isomorphism type.

Collision finding. While second pre-images seem out of reach, the KLPT^2 algorithm still lends itself to finding collisions, as we now discuss. The first step is to run KLPT^2 on input g_1, g_1, resulting in a matrix $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ defining a polarized endomorphism

$$(A_0, \lambda_1) \longrightarrow (A_0, \lambda_1), \quad A_1 \cong (A_0, \lambda_1),\ g_1 = \mu(\lambda_1)$$

of reduced degree ℓ^e. In view of the previous discussion, we can assume that $\ker(\gamma)$ is of isomorphism type (10).

Then the idea for converting γ into a collision is inspired by the reasoning at the end of Section 4.2, where it was argued that there exists a subgroup of $\ker(\gamma)$ determining a polarized (ℓ^{e_1}, ℓ^{e_1})-isogeny $\gamma_1 : (A_0, \lambda_1) \to (A_0, \lambda)$, through which γ factors, in such a way that the remaining factor $\gamma_2 : (A_0, \lambda) \to (A_0, \lambda_1)$ is a polarized $(\ell^{e_1+2e_2}, \ell^{e_1+2e_2})$-isogeny. Thus we have two "good" paths γ_1, $\tilde{\gamma}_2$ emanating from (A_0, λ_1) with the same codomain: this is the algebraic version of the desired collision. If we effectively succeed in finding γ_1, γ_2 then these matrices can be converted into two colliding isogenies emanating from A_1, by following the procedure described in Section 5.3.

In Section 4.2 we also had an explicit description of the subgroup $\ker(\gamma_1)$, namely

$$\langle \ell^{e_1+2e_2} P, R \rangle \tag{11}$$

where $P \in \ker(\gamma)$ is any point of order $\ell^e = \ell^{2e_0+2e_2}$ and R is any point of order ℓ^{e_1} that cannot be divided by ℓ inside $\ker(\gamma)$. This explicit description is of lesser use to us, because the generators in (11) are in general defined over a huge-degree extension of $\mathbb{F}_{p^2}$ only. Before explaining our workaround, let us note that many other subgroups of $\ker(\gamma)$ are equally valid choices: the only crucial features are that

- the subgroup is isomorphic to $(\mathbb{Z}/\ell^{e_1}\mathbb{Z})^2$, i.e. γ_1 is a "good" chain of isogenies,
- it contains a point R that is not divisible by ℓ in $\ker(\gamma)$, so that
$$\frac{\ker(\gamma)}{\ker(\gamma_1)} \cong (\mathbb{Z}/\ell^{e_1+2e_2}\mathbb{Z})^2,$$
i.e., also the cofactor γ_2 is a "good" chain of isogenies, and
- it concerns a maximal isotropic subgroup with respect to the ℓ^{e_1}-Weil pairing for λ_1, so that γ_1 is a polarized isogeny.

The following lemma shows that γ_1 can be built following a "greedy" approach.

Lemma 5.6. *Consider any subgroup $G \cong (\mathbb{Z}/\ell^{e_1}\mathbb{Z})^3$ of $A_0[\ell^{e_1}]$ and let $K_1 \subset G[\ell]$ be maximal isotropic with respect to the ℓ-Weil pairing e_{ℓ,λ_1}. Consider the following iterative procedure for $i \geq 2$: let K_i be any subgroup of G for which*

$$K_i \supset K_{i-1}, \qquad K_i \cong \frac{\mathbb{Z}}{\ell^i\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^i\mathbb{Z}}, \qquad e_{\ell^i,\lambda_1}|_{K_i \times K_i} = 1. \tag{12}$$

Then, regardless of the choices made, this procedure can be repeated up to $i = e_1$, and for every i we have that K_i is maximal isotropic with respect e_{ℓ^i,λ_1}.

We start with any subgroup $K_1 \subset (\ker\gamma)[\ell]$ that

- is maximal isotropic with respect to e_{ℓ,λ_1},
- contains $\ell^{e_1-1}R \in K_1$, with R a point that is not divisible by ℓ in $\ker(\gamma)$.

Then the subgroup K_{e_1} produced by Lemma 5.6 will indeed be a suitable instance of $\ker(\gamma_1)$. A point of the form $\ell^{e_1-1}R$ can be found by taking any order-ℓ point independent of $\ker(\tau)$ and $\ker(u_1)$, and taking its image under u_1. Once K_1 is fixed, we look for a matrix $\kappa_1 \in \mathrm{M}_2(\mathcal{O}_0)$ with kernel $H_1 = K_1$. We then know that γ factors through κ_1, and continue with the remaining factor $\gamma\kappa_1^{-1}$: we look for any maximal isotropic subgroup $H_2 \cong (\mathbb{Z}/\ell\mathbb{Z})^2$, with corresponding matrix κ_2, which forms a "good" extension of κ_1. We then continue with $\gamma\kappa_1^{-1}\kappa_2^{-1}$, and so on. In this way we implicitly build a tower of subgroups $K_i = (\ker\kappa_i \circ \cdots \circ \kappa_1)$ as in Lemma 5.6. Eventually, this leads to (see the full version [6] for more details):

Proposition 5.8. *Assuming knowledge of a matrix $g_1 \in \mathrm{Mat}(A_0)$ corresponding to the initial node, under plausible heuristic assumptions, collisions for the two-dimensional variant of the CGL hash function can be produced in polynomial time.*

We deem it likely that all currently known ways for constructing a superspecial principally polarized abelian surface A_1 implicitly reveal an isogeny to E_0^2. This would be analogous to the current situation for supersingular elliptic curves [2]. See the full version of this paper [6] for an extended discussion.

Bibliography

[1] Andrea Basso, Luca De Feo, Pierrick Dartois, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. SQIsign2D-west: The fast, the small, and the safer. In *ASIACRYPT 2024 Part III*, volume 15486 of *LNCS*, pages 339–370. Springer, 2024. https://doi.org/10.1007/978-981-96-0891-1_11.

[2] Jeremy Booher, Ross Bowden, Javad Doliskani, Tako Boris Fouotsa, Steven D Galbraith, Sabrina Kunzweiler, Simon-Philipp Merz, Christophe Petit, Benjamin Smith, Katherine E Stange, Yan Bo Ti, Christelle Vincent, José Felipe Voloch, Charlotte Weitkämper, and Lukas Zobernig. Failing to hash into supersingular isogeny graphs. *The Computer Journal*, 67(8):2702–2719, 2024. https://doi.org/10.1093/comjnl/bxae038.

[3] Irene Bouw, Jenny Cooley, Kristin Lauter, Elisa Lorenzo García, Michelle Manes, Rachel Newton, and Ekin Ozman. Bad reduction of genus three curves with complex multiplication. In *Women in Numbers Europe*, volume 2, pages 109–151. Springer International Publishing, 2015. https://doi.org/10.1007/978-3-319-17987-2_5.

[4] Bradley Brock. *Superspecial curves of genera two and three.* PhD thesis, Princeton University, 1994.

[5] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In *EUROCRYPT 2023 Part V*, volume 14008 of *LNCS*, pages 423–447. Springer, 2023. https://doi.org/10.1007/978-3-031-30589-4_15.

[6] Wouter Castryck, Thomas Decru, Péter Kutas, Abel Laval, Christophe Petit, and Yan Bo Ti. KLPT^2: Algebraic pathfinding in dimension two and applications. Cryptology ePrint Archive, Paper 2025/372, 2025. Full version of this paper, available at https://eprint.iacr.org/2025/372.

[7] 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. https://doi.org/10.1515/jmc-2019-0021.

[8] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, 2009. https://doi.org/10.1007/s00145-007-9002-x.

[9] Jorge Chavez-Saab, Maria Corte-Real Santos, Luca De Feo, Jonathan Komada Eriksen, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Michael Meyer, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Francisco Rodríguez Henríquez, Sina Schaeffler, and Benjamin Wesolowski. SQIsign: Algorithm specifications and supporting documentation, v1.0. available at https://sqisign.org/.

[10] 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 *ASIACRYPT 2023 Part III*, volume 14440 of *LNCS*, pages 99–130. Springer, 2023. https://doi.org/10.1007/978-981-99-8727-6_4.

[11] Hao-Wei Chu. *Algorithms for abelian surfaces over finite fields and their applications to cryptography.* PhD thesis, Pennsylvania State University, 2021. Available at `https://etda.libraries.psu.edu/files/final_submissions/24383`.

[12] Brian Conrad. Polarizations, 2004. Notes of the VIGRE Number Theory Working Group, available at `https://math.stanford.edu/~conrad/vigregroup/vigre04/polarization.pdf`.

[13] Romain Cosset and Damien Robert. Computing (ℓ, ℓ)-isogenies in polynomial time on jacobians of genus 2 curves. *Mathematics of Computation*, 84(294):1953–1975, 2015. `http://www.jstor.org/stable/24489183`.

[14] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. SQIsignHD: New dimensions in cryptography. In *EUROCRYPT 2024 Part I*, volume 14651 of *LNCS*, pages 3–32. Springer, 2024. `https://doi.org/10.1007/978-3-031-58716-0_1`.

[15] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In *ASIACRYPT 2020 Part I*, volume 12491 of *LNCS*, pages 64–93. Springer, 2020. `https://doi.org/10.1007/978-3-030-64837-4_3`.

[16] Max Deuring. Die Typen der Multiplikatorenringe Elliptischer Funktionenkörper. In *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, volume 14, pages 197–272. Springer Berlin/Heidelberg, 1941.

[17] Max Duparc and Tako Boris Fouotsa. SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies. In *ASIACRYPT 2024 Part III*, volume 15486 of *LNCS*, pages 396–429. Springer, 2024. `https://doi.org/10.1007/978-981-96-0891-1_13`.

[18] Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In *EUROCRYPT 2018 Part III*, volume 10822 of *LNCS*, pages 329–368. Springer, 2018. `https://doi.org/10.1007/978-3-319-78372-7_11`.

[19] Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park. Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs. *The Open Book Series*, 4:215–232, 2020. `https://doi.org/10.2140/obs.2020.4.215`.

[20] Jonathan Komada Eriksen, Lorenz Panny, Jana Sotáková, and Mattia Veroni. Deuring for the people: Supersingular elliptic curves with prescribed endomorphism ring in general characteristic. In *LuCaNT: LMFDB, Computation, and Number Theory*, Cont. Math., pages 339–365, 2023. `https://doi.org/10.1090/conm/796/16008`.

[21] E. Victor Flynn and Yan Bo Ti. Genus two isogeny cryptography. In *Post-Quantum Cryptography*, volume 11505 of *LNCS*, pages 286–306. Springer International Publishing, 2019. `https://doi.org/10.1007/978-3-030-25510-7_16`.

[22] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In *ASIACRYPT 2017 Part I*, volume 10624 of *LNCS*, pages 3–33. Springer, 2017. `https://doi.org/10.1007/978-3-319-70694-8_1`.

[23] Pierrick Gaudry, Julien Soumier, and Pierre-Jean Spaenlehauer. Isogeny-based cryptography using isomorphisms of superspecial abelian surfaces. Cryptology ePrint Archive, Paper 2025/136, 2025. `https://eprint.iacr.org/2025/136`.

[24] Alexandre Gélin, Everett Howe, and Christophe Ritzenthaler. Principally polarized squares of elliptic curves with field of moduli equal to $\mathbb{Q}$. *The Open Book Series*, 2(1):257–274, 2019. `http://dx.doi.org/10.2140/obs.2019.2.257`.

[25] Everett W. Howe, Franck Leprévost, and Bjorn Poonen. Large torsion subgroups of split jacobians of curves of genus two or three. *Forum Mathematicum*, 12(3):315–364, 2000. `https://doi.org/10.1515/form.2000.008`.

[26] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort. Supersingular curves of genus two and class numbers. *Compositio Mathematica*, 57(2):127–152, 1986. `http://eudml.org/doc/89752`.

[27] Bruce W. Jordan and Yevgeny Zaytman. Isogeny graphs of superspecial abelian varieties and Brandt matrices. *Mathematische Zeitschrift*, 2024. To appear, preprint available at `https://arxiv.org/pdf/2005.09031.pdf`.

[28] Ernst Kani. The number of curves of genus two with elliptic differentials. *Journal für die reine und angewandte Mathematik*, 485:93–121, 1997. `https://doi.org/10.1515/crll.1997.485.93`.

[29] Ernst Kani. The moduli spaces of jacobians isomorphic to a product of two elliptic curves. *Collectanea Mathematica*, 67:21–54, 2015. `https://doi.org/10.1007/s13348-015-0148-9`.

[30] 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. `https://doi.org/10.1112/S1461157014000151`.

[31] Sabrina Kunzweiler, Luciano Maino, Tomoki Moriya, Christophe Petit, Giacomo Pope, Damien Robert, Miha Stopar, and Yan Bo Ti. Radical 2-isogenies and cryptographic hash functions in dimensions 1, 2 and 3. In *PKC 2025 Part III*, volume 15676 of *LNCS*, pages 265–299. Springer, 2025. `https://doi.org/10.1007/978-3-031-91826-1_9`.

[32] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on SIDH. In *EUROCRYPT 2023 Part V*, volume 14008 of *LNCS*, pages 448–471. Springer, 2023. `https://doi.org/10.1007/978-3-031-30589-4_16`.

[33] James Milne. Abelian varieties, version 2.0, 2008. Course notes available at `https://www.jmilne.org/math/CourseNotes/av.html`.

[34] Kohei Nakagawa, Hiroshi Onuki, Wouter Castryck, Mingjie Chen, Riccardo Invernizzi, Gioella Lorenzon, and Frederik Vercauteren. SQIsign2D-East: A new signature scheme using 2-dimensional isogenies. In *ASIACRYPT 2024*

Part III, volume 15486 of *LNCS*, pages 272–303. Springer, 2024. https://doi.org/10.1007/978-981-96-0891-1_9.

[35] Christophe Petit and Spike Smith. An improvement to the quaternion analogue of the ℓ-isogeny problem. *Presentation at MathCrypt*, 2018.

[36] Damien Robert. Breaking SIDH in polynomial time. In *EUROCRYPT 2023 Part V*, volume 14008 of *LNCS*, pages 472–503. Springer, 2023. https://doi.org/10.1007/978-3-031-30589-4_17.

[37] Damien Robert. On the efficient representation of isogenies: a survey for NuTMiC 2024. In *NuTMiC 2024*, volume 14966 of *LNCS*, pages 3–84, 2025. https://doi.org/10.1007/978-3-031-82380-0_1.

[38] Tetsuji Shioda. Supersingular K3 surfaces. In Knud Lønsted, editor, *Algebraic Geometry*, pages 564–591. Springer Berlin Heidelberg, 1979. https://doi.org/10.1007/BFb0066664.

[39] Benjamin Smith. *Explicit Endomorphisms and Correspondences.* PhD thesis, University of Sydney, 2005. https://www.academia.edu/77805612/Explicit_endomorphisms_and_Correspondences.

[40] Katsuyuki Takashima. Efficient algorithms for isogeny sequences and their cryptographic applications. In *Mathematical Modelling for Next-Generation Cryptography. Mathematics for Industry*, volume 29, pages 97–114, Singapore, 2018. Springer. https://doi.org/10.1007/978-981-10-5065-7_6.

[41] John Voight. *Quaternion algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer Nature, 2021. https://doi.org/10.1007/978-3-030-56694-4.

[42] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1100–1111. IEEE, 2022. https://doi.org/10.1109/FOCS52979.2021.00109.