

Detecting split surfaces, RM surfaces, and minimum walks on isogeny graphs

Eda Kırımli¹ and Gaurish Korpai²

¹ University of Birmingham, UK

² University of Auckland, New Zealand

`e.kirimli@bham.ac.uk`

`gaurish.korpai@auckland.ac.nz`

Abstract. We study the detectability of split surfaces in isogeny graphs of principally polarized superspecial abelian surfaces, a question relevant to the security analysis of dimension-2 isogeny-based cryptography. Our approach uses refined Humbert invariants to replace explicit isogeny computations with primitive representation problems for positive definite quadratic forms in five variables. We develop algorithms to detect (N, N) -splittings and to compute the minimum (N, N) -splitting level of a superspecial Jacobian without constructing the corresponding isogeny path. The same framework detects embeddings of real multiplication (RM) orders through primitive representations of discriminants of real quadratic orders. For RM, we use exhaustive small-prime data together with 100,000 random polarizations per prime for $227 \leq p \leq 1619$, testing primitive representations of square-free discriminants $D \leq 100$; the first nontrivial primitively represented discriminant is typically small. We apply these methods experimentally in two regimes. For $11 \leq p \leq 251$, where the irreducible principal polarizations are known exhaustively, the automorphism data recovered from the refined Humbert invariant reproduces the counts of Ibukiyama–Katsura–Oort for the irreducible polarizations. For large parameters, we reach primes of 1000 bits, where the splitting degrees produced satisfy $\log_2 N \approx \log_2 p$ with a distribution whose shape is stable across the whole range, so the detected (N, N) -isogeny has degree about p^2 ; the smallest observed largest prime-power divisor of N remains small up to 250 bits and increases sharply from 300 bits onward.

Keywords: isogenies · abelian surfaces · superspecial · refined Humbert invariants · splitting

1 Introduction

Isogeny-based cryptography is an active area of post-quantum cryptography, concerned with variants of the isogeny problem, which are believed to be computationally hard. Following the attacks on SIDH [5,75,88], increasing attention has been directed toward higher-dimensional settings, particularly principally polarized superspecial abelian surfaces. A better understanding of the structure and expansion properties of the isogeny graphs of principally polarized superspecial abelian surfaces is important for assessing the hardness of the general dimension-2 isogeny problem.

In this work, we focus on the splitting behavior of principally polarized superspecial abelian surfaces, which plays an important role in the security analysis of several constructions and is also a natural geometric problem in its own right. In particular, contrary to the increase in the number of cryptographic primitives based on principally polarized superspecial abelian surfaces, the structure of the associated isogeny graphs and the security assumptions derived from them remain only partially understood.

We call a *product surface*³ shortly the product of two elliptic curves, and call the product surface with product polarization a *split surface*⁴. A curve C of genus 2 is said to be *splitting* if its Jacobian is K -isogenous to a principally polarized abelian surface $E_1 \times E_2$ where E_i/K for $i = 1, 2$ are supersingular elliptic curves over a finite field K .

The main focus of this work is the detection of split surfaces in the isogeny graph of principally polarized superspecial abelian surfaces and the embeddings of RM orders in the endomorphism rings. The splitting behavior of isogeny graphs is important to understand the difficulty of isogeny problems in dimension 2. Recently, isogeny graphs of RM surfaces gained attention due to their Ramanujan properties shown by [10]. We give an algorithm to detect split surfaces encountered at random in the isogeny graph and use it to study shortest paths from Jacobians to split surfaces. Moreover, our methods allow us to show all possible embeddings of RM orders when only the principal polarization is provided as input.

We approach these problems using the arithmetically rich invariants of principally polarized abelian surfaces known as *refined Humbert invariants*, introduced by Kani [44] in 1994. The main advantage is that they enable the relevant computations without explicitly evaluating costly chains of dimension-2 isogenies.

Of particular relevance is the Costello–Smith algorithm [14] for the superspecial isogeny problem, whose first phase walks from a Jacobian to a split surface and therefore depends directly on how split surfaces are distributed; we describe it in Section 4.

While it is well known that split surfaces form only a small proportion of the full graph, comparatively little is understood about their distribution within the graph. Our results provide further insight into the security and performance of recent cryptographic constructions, while also contributing to a broader understanding of superspecial isogeny graphs in dimension 2.

Let $\mathcal{A}$ be an abelian surface over $\overline{\mathbb{F}}_p$ carrying a principal polarization θ . The intersection product on the Néron–Severi group $\text{NS}(\mathcal{A})$ induces a positive definite integral quadratic form $q_{(\mathcal{A}, \theta)}$ on the quotient $\text{NS}(\mathcal{A})/\mathbb{Z}\theta$, called the *refined Humbert invariant* of $(\mathcal{A}, \theta)$. Computing refined Humbert invariants is in general difficult, and has been studied extensively by Kani [48, 49, 50, 52]; when $\mathcal{A} \cong E_1 \times E_2$ for elliptic curves E_1, E_2 it becomes tractable, which is the case we exploit throughout. The construction is recalled in full in Appendix A; see also [44, 50].

Several previous works have used refined Humbert invariants, either directly or through the associated Humbert surfaces, in the study of isogeny-based cryptography. The computational problem of determining a refined Humbert invariant is itself studied in [61], where it is shown to be polynomially equivalent, under GRH, to the computational isogeny problem of elliptic curves. The works [12, 13] instead use the algebraic Humbert surfaces $\mathcal{H}_{N^2}$ to study splitting and endomorphism problems. Their methods, however, rely on explicitly defining equations for $\mathcal{H}_{N^2}$ when $\mathcal{H}_{N^2}$ is birational, and are restricted to $N \leq 11$. By working directly with refined Humbert invariants, we avoid the need for explicit equations parameterizing Humbert surfaces.

Our use of refined Humbert invariants rests on three properties, set out in Section 4: they decide whether a principal polarization is irreducible, they detect (N, N) -splittings, and they detect embeddings of real quadratic orders. In this way, we contribute to the understanding of superspecial isogeny graphs by considering problems such as their splitting behavior and the distribution of RM superspecial surfaces.

In this work, we study principally polarized superspecial abelian surfaces through their quintic refined Humbert invariants. For splitting problems, we fix a superspecial product surface $\mathcal{A} = E \times E$, choose a random principal polarization θ , and compute $q_{(\mathcal{A}, \theta)}$. After testing irreducibility by Proposition 3, we apply Theorem 3 to detect (N, N) -splittings through primitive representations

³ We follow Kani’s terminology here.

⁴ This is mostly referred to as a principally polarized superspecial split surface in the cryptography papers.

of N^2 . This framework is then used to study the distribution of split surfaces and shortest paths from Jacobians to split surfaces, with particular emphasis on small primes $N = \ell$, and composite N . As another use, refined Humbert invariants also detect real multiplication (RM): a primitive representation of a fundamental discriminant D by $q_{(\mathcal{A}, \theta)}$ yields an embedding of the corresponding RM order $\mathcal{O}_D$ into the endomorphism ring $\text{End}(\mathcal{A})$.

We study two complementary primitive-representation problems associated with quintic refined Humbert invariants. First, for a prescribed prime ℓ , we determine the least exponent k for which $q_{(\mathcal{A}, \theta)}$ primitively represents ℓ^{2k} . By Kani’s splitting theorem (Theorem 3), this detects the minimum (ℓ^k, ℓ^k) -splitting, and gives arithmetic information about the distance to split surfaces. Second, without prescribing the splitting degree, we reduce the search for a primitive square representation $q_{(\mathcal{A}, \theta)}(x) = N^2$ to finding an isotropic vector of an associated indefinite quadratic form of rank six. This yields an effective method for producing a composite degree N , hence an existence of a split (N, N) -isogeny.

We investigate these methods experimentally in two regimes. For small characteristic, where the principal polarizations are known exhaustively, we study the distribution of minimum splitting levels for $\ell = 2, 3$, together with RM and automorphism data. For larger parameters, we compute splitting levels for a 50-bit prime and apply the unrestricted square-witness method to primes up to 1000 bits, examining both the size and the arithmetic structure of the resulting splitting degrees.

Our contributions.

- We show that splitting detection and real-multiplication detection for principally polarized superspecial abelian surfaces reduce to *primitive-representation problems* for a positive definite quadratic form in five variables, the quintic refined Humbert invariant. The reduction takes the polarization data itself as input, so no Igusa invariants, no defining equations for a genus 2 curve and no explicit chain of isogenies are required at any stage.
- We realize this reduction in three algorithms: Section 3 gives a sampler for principal polarizations that works far beyond the range of exhaustive enumeration (Algorithm 1), a lattice-enumeration procedure for the least splitting level k_0 at a prescribed ℓ (Algorithm 2), and a reduction of the unrestricted problem “find some splitting degree N ” to finding an isotropic vector of an indefinite rank-six form, solved with Simon’s algorithm (Algorithm 3).
- We relate k_0 precisely to distance in the Richelot graph (Lemma 2): it is the length of the shortest walk to the split locus made of good extensions, and an upper bound for the graph distance.
- We apply these methods experimentally in two regimes: exhaustively for small p , where all principal polarizations are known, and up to 1000-bit p for the unrestricted problem. We use the resulting data to compare automorphism counts against Ibukiyama–Katsura–Oort and to estimate how often real multiplication by a prescribed order occurs.

Organization Section 2 recalls isogeny graphs of abelian surfaces and refined Humbert invariants; the full construction of the latter is deferred to Appendix A. Section 3 develops the three algorithms. Section 4 applies them to splitting and to real multiplication, and Section 5 presents the experimental data. Section 6 lists future directions.

We implemented all the algorithms from Section 3 using a Julia package called `OSCAR` [99,18], especially using its dependency package `Nemo/Hecke` [25]. The experiments were run under Julia 1.12.7 with `OSCAR` 1.8.2. The enumeration and sampling of polarizations, the refined Humbert invariants at large p , and Algorithm 2 were run on an HPC cluster; the remaining computations were run on a workstation with a 24-core Intel i7-12800HX and 16 GB of memory. Wall-clock timings for the individual runs are recorded in the output files of the repository; we make no

performance claims from them. The code and data are provided as part of the supplemental material and are available at:

<https://github.com/gkorpall/humbert-split>

2 Preliminaries

In this section, we introduce the terminology and recall several results from the literature concerning isogenies of superspecial principally polarized abelian surfaces. In particular, we review the theory of refined Humbert invariants, real multiplications, isogeny graphs of abelian surfaces, and some basic facts about primitive representations by integral quadratic forms.

2.1 Superspecial abelian varieties

An elliptic curve is an abelian variety of dimension 1. An isogeny between elliptic curves is a surjective homomorphism with finite kernel. An isogeny from an elliptic curve to itself is called an endomorphism, and the set of endomorphisms of E forms the ring $\text{End}(E)$. If two elliptic curves E_1, E_2 are isogenous, written $E_1 \sim E_2$, then $\text{End}^0(E_1) \simeq \text{End}^0(E_2)$. An elliptic curve E defined over $\overline{\mathbb{F}}_p$ is said to be *supersingular* if the endomorphism algebra, $\text{End}_{\overline{\mathbb{F}}_p}^0(E)$, is isomorphic to a definite quaternion algebra B_p over $\mathbb{Q}$ ramified at p and ∞ . Here, $B_p = \mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{ij}$ for $\mathbf{i}^2 = a$, $\mathbf{j}^2 = b$, and $\mathbf{ij} = -\mathbf{ji}$. In particular, for $p \equiv 11 \pmod{12}$ we can consider $(a, b) = (-1, -p)$ [23, Proposition 1].

An abelian variety over $\overline{\mathbb{F}}_p$ is said to be *supersingular* if it is isogenous to a product of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ [84], and it is said to be *superspecial* if it is isomorphic to a product of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ (as an unpolarized abelian variety). A curve $\mathcal{C}$ is called *supersingular* (respectively, *superspecial*) if its Jacobian $\mathcal{A} = \mathcal{J}(\mathcal{C})$ is supersingular (respectively, *superspecial*).

Theorem 1. (*Deligne, Ogus, Shioda*) *If $\mathcal{A}/\overline{\mathbb{F}}_p$ is a superspecial abelian variety with $\dim \mathcal{A} = g > 1$, then $\mathcal{A} \simeq E^g$ for any supersingular elliptic curve E .*

For a proof, see [82, Theorem 6.2], [95, Theorem 3.5], and [74, Section 1.6].

For $g = 1$, there are many superspecial abelian varieties, namely supersingular elliptic curves, each with a principal polarization. In contrast, for $g > 1$, a single superspecial abelian variety may admit many principal polarizations. The map in (9) (or using Corollary 2.9 of [36]) induces a bijection between principal polarizations $\theta \in \mathcal{P}(E_1 \times E_2)$ and positive definite quaternion unimodular hermitian matrices

$$\mathcal{P}(E_1 \times E_2) = \left\{ \begin{pmatrix} u & \alpha \\ \overline{\alpha} & v \end{pmatrix} : u, v \in \mathbb{Z}_{>0}, \alpha \in \mathcal{O}, uv - \alpha\overline{\alpha} = 1 \right\} \quad (1)$$

where $\mathcal{O}$ is a maximal order of B_p . Throughout, we write $\mathbf{h} = \mathbf{h}(p)$ for the number of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ up to isomorphism and $\mathbf{H} = \mathbf{H}(p)$ for the number of principally polarized superspecial abelian surfaces $(\mathcal{A}, \theta)$ up to isomorphism; exactly $\frac{\mathbf{h}(\mathbf{h}+1)}{2}$ of the latter carry a reducible polarization, so that $\mathbf{H} - \frac{\mathbf{h}(\mathbf{h}+1)}{2}$ are Jacobians with irreducible polarization⁵. For an integral quadratic form q , we write $\text{Gen } q$ for its genus, that is, the set of classes locally equivalent to q at every place. We refer to [60] for these quantities and for their computation. Assume that $\text{char}(K) = p \geq 3$. By Igusa [37], every genus 2 curve $\mathcal{C}$ admits a unique double

⁵ Closed forms for $\mathbf{h}$ and $\mathbf{H}$ are recalled in (13) and (14) of Appendix C.

cover $\mathcal{C} \rightarrow \mathbf{P}^1$, whose Galois group is generated by the hyperelliptic involution ι . The quotient $\text{RA}(\mathcal{C}) := \text{Aut}(\mathcal{C})/\langle \iota \rangle$ is called the *reduced automorphism group* of $\mathcal{C}$.

Following [36], for each reduced automorphism group, we now state how many supersingular genus 2 curves are Jacobians of the product of two supersingular elliptic curves (up to isomorphism).

Theorem 2. [36, Theorem 3.3] *For a prime p , let $a_G(p)$ denote the number of isomorphism classes of genus 2 curves $\mathcal{C}$ such that $\mathcal{J}(\mathcal{C})$ is isomorphic to a product of two supersingular elliptic curves and $\text{RA}(\mathcal{C}) \cong G$. If $p \geq 7$, then $G \in \{1, C_2, C_2 \times C_2, S_3, D_6, S_4, C_5\}$, and the explicit values of $a_G(p)$ are reproduced in Appendix C. For $p = 5$, there is a unique such curve, with reduced automorphism group $\text{PGL}(2, 5)$, while $a_G(p) = 0$ for all G when $p = 2, 3$.*

2.2 Isogeny graphs of abelian varieties

From an algorithmic viewpoint, an isogeny class of abelian varieties over a field K is naturally encoded by an *isogeny graph*. Its vertices are the K -isomorphism classes $[\mathcal{A}]$, and its edges are K -isomorphism classes of isogenies $\mathcal{A} \rightarrow \mathcal{A}'$ satisfying certain conditions, mostly on their degree. For a prime $\ell \nmid \text{char}(K)$, one considers separable isogenies of degree ℓ ; the resulting ℓ -isogeny graph reflects the endomorphism rings. For elliptic curves over finite fields, it is identified with imaginary quadratic orders in the ordinary case and with maximal orders in the quaternion algebra $B_p = \left(\frac{-1, -p}{\mathbb{Q}}\right)$, ramified at p and ∞ in the supersingular case. Accordingly, ordinary ℓ -isogeny graphs have a *volcano* structure, whereas supersingular ℓ -isogeny graphs are *connected regular graphs* described by ideals in maximal quaternion orders.

From a cryptographic perspective, isogeny graphs have become a fundamental setting for post-quantum constructions, beginning with dimension-one protocols based on random walks, group actions, and path-finding in isogeny graphs of elliptic curves [9, 15, 89, 8, 16, 40]. These developments naturally motivate extending isogeny-graph techniques to higher-dimensional principally polarized abelian varieties. Early work in dimension two was initiated by Charles, Goren, and Lauter [10], Takashima [98], and Flynn and Ti [29]. Generalizations of the Charles–Goren–Lauter construction to genus 2 were proposed by Castryck, Decru, and Smith [7] and studied further by Takashima [98]. The associated isogeny graphs were subsequently analyzed in detail. Building on the classification of automorphism groups of supersingular genus 2 Jacobians by Ibukiyama, Katsura, and Oort [36], the local structure of principally polarized superspecial isogeny graphs was determined in [27, 57]. The random-walk behavior and mixing rates were studied experimentally in [28]. Recently, the paper [1] introduced finite regular directed graphs of ℓ -marked principally polarized superspecial abelian varieties of dimension g and proved that their adjacency matrices have real spectra with spectral gaps independent of p .

In summary, isogeny graphs of elliptic curves and higher-dimensional abelian varieties over finite fields play an important role in post-quantum cryptography. Their cryptographic relevance relies on the presumed hardness of finding paths between arbitrary vertices.

The efficiency and security of dimension-2 isogeny-based constructions remain largely conjectural, reflecting the limited understanding of supersingular isogeny graphs in higher dimensions. Fundamental properties such as connectedness, diameter, and expansion are not yet fully understood. In particular, rapid mixing of random walks, which underlies the security of several hash constructions and is well established for elliptic curves, remains unclear even for $g = 2$.

For supersingular elliptic curves in characteristic p , the ℓ -isogeny graph is connected [66, Corollary 78]; equivalently, any two vertices are joined by a path of ℓ -isogenies. One proof uses the representation of sufficiently large integers by primitive integral quaternary quadratic forms, while another relies on the one-dimensionality of the weight-2 Eisenstein space for $\Gamma_0(p)$ [76, p. 223].

In higher dimensions, the connectivity of the $(\ell, \dots, \ell)$ -isogeny graph for supersingular abelian varieties was established via strong approximation for quaternion unitary groups [42, 104, 43]. For RM superspecial abelian varieties, connectivity is proved in [10, Theorem 4]; these graphs are moreover Ramanujan and have few loops and multiple edges [10, Section 3.2], properties relevant to cryptographic applications. See also [30].

Richelot and (ℓ, ℓ) -isogeny graphs Let $\mathcal{A}$ be a principally polarized abelian surface over K , and let $\ell \neq \text{char}(K)$ be a prime. An (ℓ, ℓ) -isogeny is an isogeny $\mathcal{A} \rightarrow \mathcal{A}'$ whose kernel is a maximal isotropic subgroup of $\mathcal{A}[\ell]$ with respect to the ℓ -Weil pairing. For primes ℓ and p , the (ℓ, ℓ) -isogeny graph $\Gamma_2(\ell; p)$ is the weighted multi-graph whose vertices are isomorphism classes of principally polarized abelian surfaces in a fixed isogeny class over $\overline{\mathbb{F}}_p$, and whose edges correspond to isomorphism classes of (ℓ, ℓ) -isogenies. Since an (ℓ, ℓ) -isogeny admits a dual, the graph is undirected once edges are weighted by the number of isomorphism classes of kernels realizing them, and it is regular of weighted degree $(\ell + 1)(\ell^2 + 1)$.

The (ℓ, ℓ) -isogeny graph of superspecial principally polarized abelian surfaces over $\overline{\mathbb{F}}_p$ is denoted by $\Gamma_2^{SS}(\ell; p)$. When the parameters ℓ and p are clear from the context, we call $\Gamma_2^{SS}(\ell; p)$ the *superspecial graph*. When $\ell = 2$, we say that $\Gamma_2^{SS}(2; p)$ is a *Richelot superspecial isogeny graph*.

Another important aspect of the structure of isogeny graphs is the behavior of *random walks*. We therefore recall several results concerning random walks on isogeny graphs. The supersingular ℓ -isogeny graph is a constant-degree Ramanujan expander graph [87]; consequently, a random walk on such a graph mixes rapidly. For any starting vertex, after $O(\log(p))$ steps, the distribution of the endpoint is ε -close to the uniform distribution on vertices, where the hidden constant depends only on the spectral gap (equivalently, on ℓ) and on ε . To discuss random walks on superspecial isogeny graphs in dimension 2, we recall the relevant spectral bounds. Let G be an undirected graph that is regular of weighted degree d , in the sense just described, and denote by $\lambda_*(G)$ its normalized second-largest adjacency eigenvalue. Florit-Smith conjecture that, for every prime ℓ , there exists a constant $\lambda = \lambda(2, \ell) < 1$, independent of p , such that $\lambda_*(\Gamma_2^{SS}(\ell; p)) \leq \lambda$ for every prime $p \geq 5$. In the Richelot case $\ell = 2$, they conjecture that $\frac{11}{15} \leq \lambda_*(\Gamma_2^{SS}(2; p)) \leq \frac{12}{15}$ for every $p \geq 41$ [28, Conjecture 4.10]. This uniform spectral gap conjecture implies rapid mixing of random walks on the corresponding superspecial Richelot isogeny graphs.

More precisely, assuming the conjecture, Florit-Smith show that a random walk of length $n \geq 4.5m \log p + 9$ approximates the stationary distribution with error at most p^{-m} ; taking $m = 4$, a walk of length $n \geq 18 \log p + 9$ therefore gives error at most p^{-4} [28, Theorem 6.1]. We use this only as a qualitative indication that logarithmic-length random walks are expected to mix rapidly.

Another useful piece of information at hand is the *diameter* of the (ℓ, ℓ) isogeny graph of principally polarized superspecial surfaces for a specific ℓ and p . Florit-Smith also gave a result on the diameter of such isogeny graphs in the generic case [28] and calculated them explicitly for small primes; see Table 1. For a given fixed p and ℓ , they concluded that the diameter of each isogeny graph $\Gamma_g^{SS}(\ell; p)$ is $O(\log(p))$, see [28, p.12]. While searching for a number represented by a refined Humbert invariant in our algorithm, we can use the upper bound on the diameter to put an upper bound on the number represented by the quadratic form.

A useful refinement is obtained by combining spectral bounds with general diameter estimates. Let $M = \#\Gamma_g^{SS}(\ell; p)$, and suppose that the absolute values of the non-trivial normalized adjacency eigenvalues are bounded above by a constant strictly smaller than 1. The usual logarithmic estimate then gives an upper bound for the diameter in terms of M and the spectral bound, while the Chebyshev-polynomial argument of Chung–Faber–Manteuffel [11] gives the sharper estimate $\text{diam}(\Gamma_g^{SS}(\ell; p)) \leq \left\lceil \frac{\text{arcosh}(M-1)}{\text{arcosh}(\frac{1}{\lambda_{\max}})} \right\rceil + 1$, where $\lambda_{\max}$ denotes the corresponding upper bound for

p	23	47	59	71	83	107	131	167	179	191	227	239	251	263
$d(G)$	3	4	5	5	6	6	7	7	7	7	7	8	8	7
p	311	347	359	383	419	431	443	467	479	491	503	563	587	599
$d(G)$	8	8	8	8	9	8	8	8	8	8	9	9	9	9

Table 1. Experimental diameters $d(G)$ of the superspecial Richelot isogeny graph $G = \Gamma_2^{SS}(2; p)$ for primes $p \equiv 11 \pmod{12}$ (data extracted from [28, Appendix A]).

the non-trivial normalized eigenvalues. For $g = 2$ we have $M = \mathbf{H}(p)$, given in closed form by (14); for instance $\mathbf{H}(1103) = 480508$. In general M is of size $p^{\frac{g(g+1)}{2}}$, so this recovers a logarithmic diameter bound in p . In dimension 2, the estimate of Oh [83] gives $\lambda_{\max} \leq \left(\frac{2\sqrt{\ell}}{\ell+1}\right)^2$. For the Richelot isogeny graph $\Gamma_2^{SS}(2; p)$, this gives $\lambda_{\max} \leq \frac{8}{9}$, and the estimate of Chung–Faber–Manteuffel gives $\text{diam}(\Gamma_2^{SS}(2; p)) \leq 4.20 \log_2(p) + O(1)$. This bound is unconditional. Assuming instead the upper bound $\lambda_*(\Gamma_2^{SS}(2; p)) \leq \frac{12}{15} = \frac{4}{5}$ of [28, Conjecture 4.10] quoted above, the same estimate gives the sharper but *conditional* bound $\text{diam}(\Gamma_2^{SS}(2; p)) \leq 3 \log_2(p) + O(1)$.

2.3 Refined Humbert invariants

Here, we shortly give the definition of a refined Humbert invariant of principally polarized abelian surface. For the details, we refer the reader to Appendix A.

Let $\mathcal{A}$ be an abelian surface over a field K . Let $\text{Div}(\mathcal{A})$ be the set of divisors of $\mathcal{A}$. If $D_1, D_2 \in \text{Div}(\mathcal{A})$ we say that D_1 is *numerically equivalent* to D_2 , denoted by $D_1 \equiv D_2$, satisfying $(D_1 \cdot D) = (D_2 \cdot D)$ for all $D \in \text{Div}(\mathcal{A})$, where $(\cdot)$ denotes the intersection number (as defined in [32, p.357]). We define the *Néron-Severi group* $\text{NS}(\mathcal{A})$ of $\mathcal{A}$ to be $\text{NS}(\mathcal{A}) = \text{Div}(\mathcal{A}) / \equiv$, as defined in [91, Corollary of Theorem V.1]. We define the *set of principal polarizations* of $\mathcal{A}$ as

$$\mathcal{P}(\mathcal{A}) = \{D \in \text{NS}(\mathcal{A}) : D \in \text{Div}(\mathcal{A}) \text{ is ample and } D \cdot D = 2\}.$$

Let $\mathcal{A}/K$ be an abelian surface and let $\theta \in \mathcal{P}(\mathcal{A})$ be a principal polarization. We define the *polarized Néron-Severi group* of $(\mathcal{A}, \theta)$ to be $\text{NS}(\mathcal{A}, \theta) := \text{NS}(\mathcal{A}) / \mathbb{Z}\theta$.

Kani discusses in [44, §3] that there is a well-defined map on $\text{NS}(\mathcal{A})$, and this leads to a quadratic form $\tilde{q}_{(\mathcal{A}, \theta)}$ on $\text{NS}(\mathcal{A})$, given explicitly by the formula

$$\tilde{q}_{(\mathcal{A}, \theta)}(D) = (D \cdot \theta)^2 - 2(D \cdot D) \text{ for } D \in \text{NS}(\mathcal{A}).$$

It is evident that $\tilde{q}_{(\mathcal{A}, \theta)}(D + n\theta) = \tilde{q}_{(\mathcal{A}, \theta)}(D)$ for all $n \in \mathbb{Z}$. Consequently, $\tilde{q}_{(\mathcal{A}, \theta)}$ induces a positive-definite quadratic form $q_{(\mathcal{A}, \theta)}$ on the quotient module $\text{NS}(\mathcal{A}, \theta)$.⁶

Definition 1. Let $(\mathcal{A}, \theta)$ be a principally polarized abelian surface. A refined Humbert invariant⁷ $q_{(\mathcal{A}, \theta)}$ of $(\mathcal{A}, \theta)$ is the positive-definite integral quadratic form in $\rho - 1$ variables on $\text{NS}(\mathcal{A}, \theta)$ given by

$$q_{(\mathcal{A}, \theta)}(D + \mathbb{Z}\theta) = (D \cdot \theta)^2 - 2(D \cdot D), \quad D \in \text{NS}(\mathcal{A}).$$

The main use of a refined Humbert invariant in this paper is Kani’s splitting theorem, which converts the splitting of an abelian surface into a primitive representation.

⁶ This can be seen as an integral quadratic form on $\mathbb{Z}^{\rho-1}$ since $\text{NS}(\mathcal{A}, \theta) \simeq \mathbb{Z}^{\rho-1}$, where ρ is the Picard number of $\mathcal{A}$.

⁷ Note that a refined Humbert invariant is considered up to $\text{GL}_n(\mathbb{Z})$ equivalences.

Theorem 3. [50, Theorem 20] *A curve C/K has an elliptic⁸ subcover of degree N if and only if q_C primitively represents N^2 . Equivalently, $\mathcal{J}(C)$ is (N, N) split if and only if q_C primitively represents N^2 .*

2.4 Primitive representations by positive definite quadratic forms

A *quadratic lattice* is a pair $(\mathbb{Z}^n, q)$, where q is a quadratic form. A *representation* of $(\mathbb{Z}^m, q)$ by $(\mathbb{Z}^n, q_0)$ is an isometry $\eta : (\mathbb{Z}^m, q) \rightarrow (\mathbb{Z}^n, q_0)$. It is *primitive* if $\eta(\mathbb{Z}^m)$ is a primitive sublattice of $\mathbb{Z}^n$, equivalently, $\eta(\mathbb{Z}^m) = (\eta(\mathbb{Z}^m) \otimes_{\mathbb{Z}} \mathbb{Q}) \cap \mathbb{Z}^n$. We say that $(\mathbb{Z}^m, q)$ is *locally primitively representable* by $(\mathbb{Z}^n, q_0)$ if such a primitive representation exists over $\mathbb{Z}_\nu$ for every prime ν and over $\mathbb{R}$.

The integral local–global problem asks when local primitive representability implies primitive representability over $\mathbb{Z}$. For indefinite target forms and $n \geq m + 3$, this follows from Eichler’s strong approximation for spin groups [21]. The positive definite case is subtler. Hsia, Kitaoka, and Kneser [34] proved a local–global theorem for $n \geq 3m + 3$ when the minimum of the represented lattice is sufficiently large, and Jöchner and Kitaoka [41] reduced the dimension requirement to $n \geq 2m + 3$ under additional hypotheses. Ellenberg and Venkatesh [24] subsequently obtained an ineffective result for $n \geq m + 5$, and also for $n \geq m + 3$ when the minimum is sufficiently large. A recent effective result gives the following form of the principle in codimension at least 3.

Theorem 4 ([22, Theorem 1.3]). *Let $m, n \in \mathbb{Z}_{>0}$ with $n \geq m + 3$. There exist constants $C, A > 0$, depending only on n , such that the following holds. Let $(\mathbb{Z}^m, q)$ and $(\mathbb{Z}^n, q_0)$ be positive definite quadratic lattices. If $(\mathbb{Z}^m, q)$ is locally primitively representable by $(\mathbb{Z}^n, q_0)$ and $\min_{\{0 \neq x\}} q(x) \geq C \operatorname{disc}(q_0)^A$, then $(\mathbb{Z}^m, q)$ is primitively representable by $(\mathbb{Z}^n, q_0)$.*

For $m = 1$, this gives a local–global principle for primitive representations of sufficiently large integers by positive definite forms; classical results in this direction go back to Kloosterman and Tartakowsky (see [38, §11]). Related work of Kitaoka [62, 64, 65] studies more generally the relation between primitive and non-primitive representation problems.

2.5 Related work on splittings

It is important to distinguish three computational formulations of the (N, N) -splitting problem for a principally polarized superspecial abelian surface $(\mathcal{A}, \theta)$: (i) determining a splitting degree N for which $(\mathcal{A}, \theta)$ admits an (N, N) -splitting; (ii) for a prescribed N , deciding or certifying whether such an (N, N) -splitting exists; and (iii) constructing the corresponding explicit geometric isogeny $\mathcal{A} \rightarrow E_1 \times E_2$. Existing approaches address different parts of this problem.

Corte-Real Santos–Costello–Frengley [12, 13] work geometrically and, for a prescribed integer $N \leq 11$, efficiently test whether a superspecial genus 2 Jacobian is optimally (N, N) -split using the Humbert surface $\mathcal{H}_{N^2}$. Their test certifies the existence of such a splitting but does not construct the corresponding (N, N) -isogeny. They incorporate these fixed- N tests into *SplitSearcher*, which performs a walk in the Richelot $(2, 2)$ -isogeny graph and uses splitting detection to accelerate the search for a suitable endpoint. Thus, this approach addresses the fixed- N detection problem rather than (i), in which the candidate values of N are chosen in advance rather than determined intrinsically from $(\mathcal{A}, \theta)$.

Kunzweiler–Shen [70] instead study the computational consequences of having a splitting. They reduce the problem of finding a non-scalar endomorphism of a supersingular elliptic curve

⁸ Theorem 3 incorporated into our algorithms works on genus 2 curves lying on the product surface, that is to mean $\mathcal{J}(C) \cong E_1 \times E_2$ for any two elliptic curves E_1 and E_2 (not necessarily supersingular elliptic curves).

to a restricted *good splitting problem*, in which the returned splitting is required to satisfy an additional compatibility condition with a preceding isogeny, and give a proof-of-concept implementation based on a search in the isogeny graph via theta functions and Kani’s lemma. Kutas–Shen [71] subsequently eliminates the need for this restriction at the level of the security reduction: they give an oracle reduction from the non-scalar endomorphism problem to the unrestricted splitting problem, in which the oracle may return an arbitrary splitting. They further derive a heuristic equivalence between a suitably restricted degree splitting problem and the problem of computing the full endomorphism ring of a principally polarized superspecial abelian surface. These results clarify the computational relation between splitting and endomorphism computation, but treat the splitting problem itself as an oracle: they do not provide an algorithm for determining a splitting degree or constructing the corresponding explicit splitting isogeny.

On the algebraic representation, KLPT² [6] is particularly relevant since its input consists of IKO matrices (representing principal polarizations) on superspecial abelian surfaces. Thus, the IKO representation retains precisely the polarization data, and needed for polarized dimension 2 isogeny computations. This is the same type of polarized algebraic input from which the refined Humbert invariant is obtained in [60]. Page–Robert–Soumier [85] are especially relevant in this aspect, as they use splittings as an ingredient to improve KLPT². Their interpretation Hermitian modules allows them to work explicitly with orthogonal decompositions into rank-1 projective submodules and to construct smooth splitting similitudes from rank-2 modules to split modules. The corresponding polarized isogenies $\mathcal{A}_i \rightarrow E_0 \times E_i$ are then combined with KLPT algorithm [67] of elliptic curves, reducing the output degree of KLPT² from $O(p^{25})$ to $O(p^{15.5})$. Their result, therefore, highlights the importance of splitting isogenies for improving the efficiency of algebraic dimension-2 isogeny path-finding problem.

The refined Humbert invariant provides a direct arithmetic formulation of this splitting detection problem. From the algebraic representation of $(\mathcal{A}, \theta)$, one obtains the quintic refined Humbert invariant $q_{(\mathcal{A}, \theta)}$, and the (N, N) -splitting is detected by a primitive representation $q_{(\mathcal{A}, \theta)}(x) = N^2$. Thus, the splitting degree N itself can be searched for through primitive square representations of a positive definite integral quadratic form in five variables obtained from a principal polarization encoded by a IKO matrix.

3 Algorithms

3.1 Constructing random polarizations

Let $p \equiv 11 \pmod{12}$ be prime, let $B_p = (-1, -p \mid \mathbb{Q})$ be the definite quaternion algebra over $\mathbb{Q}$, and fix the maximal order $\mathcal{O} = \mathbb{Z}\langle 1, \beta_1, \beta_2, \beta_3 \rangle = \mathbb{Z}\langle 1, i, \frac{i+j}{2}, \frac{1+ij}{2} \rangle \cong \text{End}(E)$, $j(E) = 1728$. A principal polarization on the superspecial surface $\mathcal{A} = E \times E$ is then a positive definite unimodular Hermitian matrix [60, Equation (11)]

$$\theta = \begin{pmatrix} u & \alpha \\ \bar{\alpha} & v \end{pmatrix}, \quad u, v \in \mathbb{Z}_{>0}, \quad \alpha \in \mathcal{O}, \quad \det \theta = uv - \text{nr}d(\alpha) = 1,$$

and the object of this subsection is to sample such a θ at random, for p far larger than exhaustive enumeration can reach.

The sampler does not work directly on an order basis. It works instead in the half-coordinates $\alpha = \frac{1}{2}(A_0 + A_1 i + A_2 j + A_3 i j)$, for which the reduced norm is $\text{nr}d(\alpha) = \frac{1}{4}(A_0^2 + A_1^2 + p(A_2^2 + A_3^2))$ and membership $\alpha \in \mathcal{O}$ amounts to the two congruences $A_0 \equiv A_3$ and $A_1 \equiv A_2 \pmod{2}$. Setting $z = A_3$, $y = A_2$, $w = \frac{A_0 - z}{2}$ and $x = \frac{A_1 - y}{2}$ converts a solution back to $\alpha = w + x\beta_1 + y\beta_2 + z\beta_3$, which is the $[u, v, w, x, y, z]$ record format of the generated data.

As a construction, this is not new, and it is worth being precise about what is borrowed. The overall shape — draw u and v , set $n = uv - 1$, and hand n to a norm-equation solver — is KLPT²'s `RandomPolarisation` [6]. The solver it calls is the Kohel–Lauter–Petit–Tignol `RepresentInteger` [67], in the form used by SQIsign [17]. That the resulting matrices are exactly the principal polarizations is due to Ibukiyama–Katsura–Oort [36, Corollary 2.9], restated as [6, Theorem 2.8]. What is new here is a restriction on the search, which the following observation makes available.

Lemma 1. *Let $p \equiv 3 \pmod{4}$, let $n \in \mathbb{Z}$, and set $\text{rhs} = 4n - p(A_2^2 + A_3^2)$. Then*

$$\text{rhs} \equiv \begin{cases} 0 \pmod{4} & A_2, A_3 \text{ both even,} \\ 1 \pmod{4} & A_2, A_3 \text{ of opposite parity,} \\ 2 \pmod{4} & A_2, A_3 \text{ both odd.} \end{cases}$$

In particular the condition $\text{rhs} \equiv 1 \pmod{4}$ required by `Cornacchia` [81] holds exactly for opposite-parity pairs (A_2, A_3) , and this is known before rhs is computed.

Proof. A square is 0 or 1 modulo 4 according as its root is even or odd, so $A_2^2 + A_3^2$ is congruent to 0, 1 or 2 in the three respective cases. Since $p \equiv 3 \pmod{4}$ we have $-p \equiv 1$ and $-2p \equiv 2 \pmod{4}$, while $4n \equiv 0$, so that $\text{rhs} \equiv -p(A_2^2 + A_3^2) \pmod{4}$ takes the stated values.

Restricting the search to opposite-parity pairs, therefore, throws away half of every draw that could never have reached the Cornacchia step (line 11), and none that could. With that in hand, the whole sampler fits in one pass, as Algorithm 1.

Algorithm 1: `RandomPolarizations`: sample T principal polarizations

Input: prime $p \equiv 11 \pmod{12}$; exponent `sbound`; sample size T
Output: a list Θ of T matrices $\theta = \begin{pmatrix} u & \alpha \\ \alpha & v \end{pmatrix}$ with $u, v \in \mathbb{Z}_{>0}$, $\alpha \in \mathcal{O}$, $\det \theta = 1$

```

1  $\Theta \leftarrow \emptyset$ 
2 While  $|\Theta| < T$  do
3    $u \leftarrow \text{uniform in } [1, p^{\text{sbound}}]$ 
4    $v \leftarrow \text{uniform in } [1, p^{3 \cdot \text{sbound}}]$ 
5    $n \leftarrow uv - 1$ 
6    $B \leftarrow \lfloor \sqrt{4n/p} \rfloor$ 
7   repeat
8     sample  $(A_2, A_3)$  uniformly in  $[-B, B]^2$  of opposite parity
9      $\text{rhs} \leftarrow 4n - p(A_2^2 + A_3^2)$ 
10  until  $\text{rhs} > 0$  and  $\text{rhs}$  is prime
    // a draw exhausting its retry budget is abandoned; redraw  $u, v$ 
11   $(A_0, A_1) \leftarrow \text{Cornacchia}(\text{rhs})$ 
12  order  $A_0, A_1$  so that  $A_0 \equiv A_3$  and  $A_1 \equiv A_2 \pmod{2}$ 
13   $\alpha \leftarrow \frac{1}{2}(A_0 + A_1i + A_2j + A_3ij)$ 
14  append  $\theta = \begin{pmatrix} u & \alpha \\ \alpha & v \end{pmatrix}$  to  $\Theta$ 
15 Return  $\Theta$ 
```

The asymmetry of the bounds in lines 3–5 is deliberate: letting v range over $p^{3 \cdot \text{sbound}}$ while u ranges only over p^{sbound} makes $n = uv - 1$ vary widely relative to p , which keeps the supply of rhs passing the test in line 10 plentiful. Line 6 then bounds (A_2, A_3) so that rhs cannot go negative. The loop of lines 8–10 is the search proper, and Lemma 1 is what makes it cheap: because line 8 samples only opposite-parity pairs, the congruence $\text{rhs} \equiv 1 \pmod{4}$ holds automatically, so

primality is the sole condition left to test, and line 11 then recovers $\text{rhs} = A_0^2 + A_1^2$ by Cornacchia's algorithm [81] without factoring anything. The pair is redrawn afresh on each pass rather than swept in a fixed order, so a given n need not always produce the same α , and a corpus generated this way does not concentrate on small (A_2, A_3) . Line 12 uses the one remaining freedom, the choice of which of A_0, A_1 plays which role, to meet the membership congruences. This always succeeds: rhs is an odd prime, so exactly one of A_0, A_1 is even, while A_2, A_3 have opposite parity by Lemma 1; hence exactly one of the two orderings satisfies $A_0 \equiv A_3$ and $A_1 \equiv A_2 \pmod{2}$, and the line has no failure branch. Lines 13–14 assemble θ , and since $\text{nrd}(\alpha) = n = uv - 1$ by construction, its determinant is 1 without any verification step.

A word on what is being sampled. Algorithm 1 draws Hermitian *matrices*, not isomorphism classes, and the fibres of the map from matrices to classes are not of equal size: distinct θ can give isomorphic $(\mathcal{A}, \theta)$, and the number that do is governed by the automorphisms of the surface. The distribution induced on isomorphism classes is therefore not uniform, and we do not determine it here.

What the algorithm does produce, with overwhelming probability, is an *irreducible* polarization, which is the case of interest for splitting. Of the $\mathbf{H}$ principal polarizations on $E \times E$, exactly $\frac{\mathbf{h}(\mathbf{h}+1)}{2}$ are reducible [60, Table 1], so by (15) the reducible proportion is $10/p + O(p^{-2})$ and tends to zero. A reducible draw is in any case detected and discarded by Proposition 3, so this proportion measures only how rarely a draw is wasted. What does bear on the experiments is whether the distribution induced on the isometry classes of *irreducible* polarizations distorts the statistics we read off them; that is tested in Section 5 against the lists of [60].

Three practical matters are suppressed above. The search in lines 8–10 carries a retry budget, and a draw that exhausts it is abandoned and restarted with fresh u, v ; the budget grows as $\Theta(\text{sbound} \cdot \log p)$, which matches the $O(\log p)$ samples one expects to need before a prime rhs appears. For small p the implementation will also accept a composite rhs that it can factor outright, which brings the same-parity cases of Lemma 1 back into play; that path is unreachable at cryptographic size, and the restriction in line 8 is imposed only once it is provably dead. Finally, `sbound` is not a constant here. KLPT² fixes `sbound` = 20, so that $n \approx p^{80}$, which is harmless for a small test prime but runs to some 80,000 bits for a 1000-bit one; choosing `sbound` $\approx \text{target\_bits}/(4 \log_2 p)$ instead holds the norm equation near a fixed size across the whole range.

It is worth setting Algorithm 1 beside [60, Algorithm 2], which answers a different question. That algorithm, `polz`($p, V_{\max}, U_{\max}, T_{\max}$), enumerates principal polarizations exhaustively and classifies them up to isomorphism, growing its bounds until the count reaches $\mathbf{H}(p)$. That stopping condition is met, and the list is then complete, for $p \leq 191$; at $p = 227, 239, 251$ the published runs halt short of it [60, Table 1], and in each case every polarization missed is reducible, so the irreducible ones — the case of interest here — are complete throughout $p \leq 251$. Algorithm 1 surrenders both the completeness and the classification, returning raw polarizations rather than representatives, and buys with that the ability to keep going at sizes where enumeration has long since stopped. The two are complementary rather than interchangeable.

3.2 Primitive representations of 4^k and ℓ^{2k}

We now specialize to the case needed for quintic refined Humbert invariants below, following [60, Section 3.1]. Fix an odd prime $p \equiv 11 \pmod{12}$ and let

$$q_5(x_0, x_1, x_2, x_3, x_4) = x_0^2 + 4x_1^2 + 4x_1x_3 + 4x_2^2 + 4x_2x_4 + (p+1)x_3^2 + (p+1)x_4^2, \quad L_5 := (\mathbb{Z}^5, q_5).$$

For a quadratic form q in n variables we write G_q for the symmetric matrix with $q(x) = x^t G_q x$, so that $\text{disc}(q) = \det(2G_q) = 2^n \det G_q$. In the order of variables $x_0; x_1, x_3; x_2, x_4$ the matrix

G_{q_5} is block diagonal,

$$G_{q_5} = (1) \oplus \begin{pmatrix} 4 & 2 \\ 2 & p+1 \end{pmatrix} \oplus \begin{pmatrix} 4 & 2 \\ 2 & p+1 \end{pmatrix}, \quad \det G_{q_5} = 1 \cdot 4p \cdot 4p = 16p^2, \quad \text{disc}(q_5) = 2^5 \cdot 16p^2 = 2^9 p^2,$$

and L_5 is positive definite. All lattices $L = (\mathbb{Z}^5, q)$ of interest below lie in the genus of L_5 , i.e. q and q_5 agree up to a change of variables in $\text{GL}_5(\mathbb{Z}_\nu)$ for every prime ν ; in particular $\Delta_L = \text{disc}(q) = 2^9 p^2$.

Represents locally. For $m = 1$ the lattice to be represented is $(\mathbb{Z}, tz^2)$ with $t \in \mathbb{Z}_{>0}$. A representation η of $(\mathbb{Z}, tz^2)$ by $(\mathbb{Z}^5, q)$ over $\mathbb{Z}_\nu$ is $\eta(z) = z\alpha$ with $\alpha = \eta(1) \in \mathbb{Z}_\nu^5$ and $q(\alpha) = t$, and it is primitive exactly when $\alpha \notin \nu\mathbb{Z}_\nu^5$; over $\mathbb{R}$ a representation exists for every $t > 0$. A change of variables in $\text{GL}_5(\mathbb{Z}_\nu)$ maps $\mathbb{Z}_\nu^5 \setminus \nu\mathbb{Z}_\nu^5$ onto itself, so the existence of such α depends only on the genus of $(\mathbb{Z}^5, q)$.

Theorem 5. *Let p be an odd prime, let $L = (\mathbb{Z}^5, q)$ be a quadratic lattice in the genus of L_5 , and $t \in \mathbb{Z}_{>0}$.*

- (i) *For every odd prime ν , $(\mathbb{Z}, tz^2)$ is primitively representable by L over $\mathbb{Z}_\nu$.*
- (ii) *If $p \equiv 3 \pmod{4}$, then $(\mathbb{Z}, tz^2)$ is primitively representable by L over $\mathbb{Z}_2$ if and only if $t \equiv 0$ or $1 \pmod{4}$.*

Consequently, if $p \equiv 3 \pmod{4}$, then $(\mathbb{Z}, tz^2)$ is locally primitively representable by L if and only if $t \equiv 0$ or $1 \pmod{4}$; in particular for every square t , hence for $t = \ell^{2k}$ with ℓ any prime and $k \geq 0$, and for $t = 4^k$.

The proof is in Appendix B.

Represents globally. The shell of norm m is $\{x \in \mathbb{Z}^5 : q(x) = m\}$;

$$r(L, m) = \#\{x \in \mathbb{Z}^5 : q(x) = m\}, \quad r^*(L, m) = \#\{x \in \mathbb{Z}^5 : q(x) = m, \gcd(x) = 1\}$$

are its size and its primitive part. The lattice minimum $\lambda_1(L) = \min\{q(x) : 0 \neq x \in \mathbb{Z}^5\}$ is a squared length in this normalization. If $\ell^{2k} < \lambda_1(L)$ the shell is empty, and $\lambda_1(L) \leq 8^{1/5}(\det G_q)^{1/5}$ by Hermite, so the search starts at

$$k_1 = \lceil \log_{\ell^2} \lambda_1 \rceil \lesssim \frac{1}{5} \log_\ell p. \quad (2)$$

For a class L , put $k_0(L) = \min\{k \geq 1 : r^*(L, \ell^{2k}) > 0\}$, the least level at which L primitively represents ℓ^{2k} ; equivalently, the least k for which $(\mathcal{A}, \theta)$ admits an (ℓ^k, ℓ^k) -splitting. For $k \geq 0$,

$$r(L, \ell^{2k}) = \sum_{i=0}^k r^*(L, \ell^{2i}), \quad \text{hence} \quad k_0(L) \leq k \iff r(L, \ell^{2k}) > 0. \quad (3)$$

Moreover the shell of norm ℓ^{2k_0} consists of primitive vectors whenever $\lambda_1(L) > 1$: if $q(x) = \ell^{2k_0}$ and $g = \gcd(x) > 1$, then $g \mid \ell^{k_0}$, so x/g has norm ℓ^{2i} with $i < k_0$, which contradicts the minimality of k_0 when $i \geq 1$ and contradicts $\lambda_1(L) > 1$ when $i = 0$. Note that the term $i = 0$ in (3) is nonzero precisely when q represents 1, that is, precisely when θ is reducible by Proposition 3. Representation is therefore monotone in k by (3) while primitive representation is not: a class may primitively represent ℓ^{2k_0} and yet represent $\ell^{2(k_0+1)}$ only imprimitively.

Corollary 1. *Let $p \equiv 3 \pmod{4}$ and let $L = (\mathbb{Z}^5, q)$ lie in the genus of L_5 . With C_5, A_5 the constants of Theorem 4 for $m = 1, n = 5$, every integer $t \equiv 0, 1 \pmod{4}$ with $t \geq C_5 \Delta_L^{A_5}$ is primitively represented by L . In particular ℓ^{2k} is primitively represented by L as soon as*

$$k \geq \frac{1}{2} \log_\ell C_5 + \frac{A_5}{2} \log_\ell \Delta_L = \frac{1}{2} \log_\ell C_5 + \frac{9A_5}{2} \log_\ell 2 + A_5 \log_\ell p,$$

so the threshold satisfies $k_0(L) = O(\log p)$. The constants C_5, A_5 are not made explicit in Theorem 4, so the implied constant here is unknown and this bound cannot serve as a computational stopping rule; the rule we actually use is the diameter bound of Section 2.2, a logically independent statement that happens to agree in order of magnitude.

Proof. By Theorem 5, $(\mathbb{Z}, tz^2)$ is locally primitively representable by L , and $\min_{0 \neq z \in \mathbb{Z}} tz^2 = t$; apply Theorem 4 with $m = 1, n = 5$, and put $t = \ell^{2k}$, $\Delta_L = 2^9 p^2$.

Therefore, the whole computation is done by the Kannan-Fincke-Pohst enumeration algorithm [55,26,90].

Algorithm 2: FirstLevel($G_q, \ell, K_{\max}$): the least k with a primitive vector of norm ℓ^{2k}

Input: The Gram matrix G_q of a lattice $L = (\mathbb{Z}^5, q)$ in the genus of L_5 ; the prime ℓ ; a cap $K_{\max}$.

Output: $k_0(L)$ and a primitive $x \in \mathbb{Z}^5$ with $q(x) = \ell^{2k_0}$, or “ $k_0 > K_{\max}$ ”.

```

1  ( $G', U$ )  $\leftarrow$  LLL( $G_q$ )
2   $\lambda_1 \leftarrow$  ShortestVector( $G'$ )                                     // Kannan-Fincke-Pohst
3   $k_1 \leftarrow$  least  $k \geq 1$  with  $\ell^{2k} \geq \lambda_1$ 
4  For  $k = k_1, \dots, K_{\max}$  do
5      For each  $z$  in Enumerate( $G', \ell^{2k}$ ) do
6          If  $\gcd(z) = 1$  then
7               $x \leftarrow Uz$ 
8              Verify ( $x^t G_q x = \ell^{2k}$  and  $\gcd(x) = 1$ ) in exact integer arithmetic; abort on failure
9              Return ( $k, x$ )
10 Return  $k_0 > K_{\max}$ 

```

Bounds for the search. The diameter bounds of Section 2.2 give a stopping criterion for our representation search. For any fixed p a rigorous bound is obtained by substituting the exact value $M = \# \Gamma_2^{SS}(2; p)$ into the Chung–Faber–Manteuffel inequality. Once a diameter bound Diam is established, it is enough in our search to consider $k \leq \text{Diam}$, and hence refined Humbert invariant values of the form $2^{2k} = 4^k$ with $k \leq \text{Diam}$.

That bound lies far above what the experiments need, and in practice $K_{\max}$ is set from p directly. The small-prime runs of Section 5 take $K_{\max} = \lceil \ln p \rceil$, which is 3 at $p = 11$ and 6 at $p = 251$, and decide every level by exhaustive enumeration, so a negative answer at a given k is a proof rather than a timeout. The 50-bit run of Algorithm 2 uses $K_{\max} = \lceil 2 \ln p / (3 \ln \ell) \rceil = 33$, twice the heuristic value of k_0 ; it is never reached, the largest k_0 observed over the 10,000 classes being 17.

3.3 Random primitive representation

For $L = (\mathbb{Z}^5, q)$ in the genus of L_5 put $F = 2G_q \oplus (-2)$, so that $\det F = -2^{10} p^2$ and $v^t F v = 2(q(x) - z^2)$ for $v = (x, z) \in \mathbb{Z}^5 \times \mathbb{Z}$. (The factor 2 makes F even, as the implementation requires; it does not change the isotropic vectors.)

Proposition 1. (a) $v = (x, z)$ is isotropic for F iff $q(x) = z^2$; then $z \neq 0$.
(b) If moreover $\gcd(v) = 1$ then $\gcd(x) = 1$: x is a witness for $N = |z|$.
(c) Every totally isotropic subspace of $(\mathbb{Q}^6, F)$ has dimension at most 1.
(d) F has an isotropic vector: every class of the genus has a witness.

Proof. (a) q is positive definite, so $z = 0$ forces $x = 0$.
(b) $g = \gcd(x)$ gives $g^2 \mid z^2$, so $g \mid \gcd(v) = 1$.
(c) Over $\mathbb{R}$, F has five positive and one negative square, so a totally isotropic subspace has dimension at most 1 [92, Ch. IV, §3.1].
(d) F is indefinite in six variables: Meyer’s theorem [92, Ch. IV, §3.2, Corollary 2].

Meyer’s theorem is not effective. Simon’s indefinite LLL [96] solves $v^t F v = 0$ for unimodular F ; his general algorithm [97] (see [101]) reduces an arbitrary F , given the factorisation of $\det F$, to that case, and returns a totally isotropic sublattice of maximal dimension, here a single vector, by (c), in time polynomial in the bit size of F , the factorisation being the only non-polynomial step [97, §8]. Since $\det F = -2^{10}p^2$ is known by construction, that step is free at every size of p . We use the algorithm as a black box and certify its output ourselves. We note that Proposition 1(d) asserts only that a witness exists: neither it nor anything else we prove controls the size of the witness that Simon’s algorithm returns, and the concentration of $\log_2 N$ near $\log_2 p$ reported in Section 5 is an empirical observation.

Algorithm 3: Witness(q, p): a primitively represented square of one class

Input: $L = (\mathbb{Z}^5, q)$ in the genus of L_5 , given by G_q ; the prime p .
Output: A primitive $x \in \mathbb{Z}^5$ and $N \geq 1$ with $q(x) = N^2$.
1 $F \leftarrow 2G_q \oplus (-2)$
2 $w \leftarrow \text{IsotropicVector}(F, \det F = -2^{10}p^2)$ // one vector, by Proposition 1(c)
3 $v \leftarrow w / \gcd(w)$; write $v = (x, z)$
4 **Verify**($\gcd(v) = 1$, $v^t F v = 0$, $z \neq 0$, $\gcd(x) = 1$, $x^t G_q x = z^2$) in exact integer arithmetic; abort on failure
5 **Return** $(x, |z|)$ // a witness, by Proposition 1(b)

3.4 Primitive representation of small square-free integers

As discussed in Appendix A.1, the refined Humbert invariant $q_{(\mathcal{A}, \theta)}$ encodes real multiplication by $\mathcal{O}_D$ on a principally polarized abelian surface $(\mathcal{A}, \theta)$: a positive fundamental discriminant D is primitively represented by $q_{(\mathcal{A}, \theta)}$ if and only if there exists an embedding $\mathcal{O}_D \hookrightarrow \text{End}_\theta(\mathcal{A})$, equivalently, if $(\mathcal{A}, \theta)$ lies on the Humbert surface $\mathcal{H}_D$. Computationally, we can directly apply Kannan-Fincke-Pohst enumeration algorithm [55, 26, 90], as in Algorithm 2, to check if a small square-free integer is primitively represented by a refined Humbert invariant $q_{(\mathcal{A}, \theta)}$ for a given reducible or irreducible polarization.

The value $n = 1$ is excluded deliberately: by Proposition 3, $q_{(\mathcal{A}, \theta)}$ represents 1 exactly when θ is reducible, so $n = 1$ is a separate test rather than a discarded case. The cost is one enumeration of a ball of radius $\sqrt{D}$ for each surviving n ; throughout this paper we run Algorithm 4 only with $D \leq 100$.

Algorithm 4: PrimitiveReps(G_q, D): primitive square-free representations up to D

Input: The Gram matrix G_q of a positive definite lattice $L = (\mathbb{Z}^5, q)$; a bound $D \geq 2$.

Output: The square-free n with $2 \leq n \leq D$ primitively represented by L , each with a witness $x \in \mathbb{Z}^5$.

```
1  $S \leftarrow \{2, \dots, D\}$ 
2 For  $d = 2, \dots, \lfloor \sqrt{D} \rfloor$  do
3    $\lfloor$  delete from  $S$  every multiple of  $d^2$ 
4  $(G', U) \leftarrow \text{LLL}(G_q)$ 
5  $R \leftarrow \emptyset$  //  $R$  maps represented targets to witnesses
6 For each  $n \in S$  do
7   For each  $z$  in Enumerate( $G', n$ ) do
8     If  $\gcd(z) = 1$  then
9        $x \leftarrow Uz$ 
10      Verify ( $x^t G_q x = n$  and  $\gcd(x) = 1$ ) in exact integer arithmetic; abort on failure
11      add  $(n, x)$  to  $R$ 
12      break
13 Return  $R$ 
```

4 Applications

In this section we put the refined Humbert invariant to work. It serves three purposes. First, the *irreducibility criterion* of Proposition 3 distinguishes Jacobians with irreducible principal polarization from product surfaces with reducible polarization. Second, Kani’s splitting theorem (Theorem 3) characterizes (N, N) -splittings in terms of primitive representations of N^2 by the refined Humbert invariant q_C . Third, primitive representations of discriminants D detect embeddings of the corresponding real multiplication orders $\mathcal{O}_D$ into the endomorphism ring. We take these in turn, and in each case work out what the representation problem says about the isogeny graph: for splittings, a precise relation between the least level k_0 and distance to the split locus, together with the branching that restricts the walks involved; for real multiplication, a test that needs no walk at all; and for automorphisms, a comparison against the counts of Ibukiyama–Katsura–Oort. The experiments that exercise all of this are reported in Section 5. Among two-dimensional superspecial isogeny graphs, Richelot graphs are particularly well suited to explicit computation and already possess a rich structure, which is why we take them as our main testing ground throughout.

4.1 Detecting splittings

Of relevance to isogeny-based cryptography, Costello and Smith’s algorithm for the superspecial isogeny problem [14] proceeds in two parts. The first part performs pseudo-random walks starting from the given Jacobians to the products of supersingular elliptic curves, obtaining isogenies $\varphi : \mathcal{J}(\mathcal{C}) \rightarrow E_1 \times E_2$ and $\varphi' : \mathcal{J}(\mathcal{C})' \rightarrow E_1' \times E_2'$. Assuming these walks rapidly approach a uniform distribution, it costs $\tilde{O}(p)$ since only an $O(1/p)$ fraction of superspecial abelian surfaces are isomorphic to a product of elliptic curves. The second part uses the Delfs–Galbraith algorithm [20] to find isogeny paths $E_1 \rightarrow E_1'$ and $E_2 \rightarrow E_2'$, and then glues them to obtain a path $\pi : E_1 \times E_2 \rightarrow E_1' \times E_2'$, costing $\tilde{O}(p^{1/2})$. The final solution is the composition $\Phi := \hat{\varphi}' \circ \pi \circ \varphi$, and the expected running time is $\tilde{O}(p)$, dominated by the first phase. Motivated by the isogeny-based cryptography discussions above, we aim to give a new method to detect close split surfaces to a randomly chosen

vertex in the isogeny graph. It does not depend on any isogeny calculation; it does not have to be on the Richelot isogeny graph, and it gives us a more conceptually general method in theory for any (N, N) split case. On the other hand, as a fallback, we do not know the geometric description of the principally polarized superspecial surface.

We now continue the analysis of this problem with refined Humbert invariants. Let $q_{\mathcal{C}}$ be a refined Humbert invariant of a principally polarized superspecial Jacobian abelian surface. We can always guarantee choosing a random polarization in a way that it leads to a Jacobian variety; this can be done efficiently by computing the refined Humbert invariant $q_{(\mathcal{A}, \theta)}$ by calculations in [60], and verifying that it is actually a Jacobian by the irreducibility criterion, Proposition 3. We emphasize that we do not know which abelian surface $\mathcal{J}(\mathcal{C})$ is exactly, so it is just a random vertex corresponding to a $(\mathcal{J}(\mathcal{C}), \theta_{\mathcal{C}})$. By Kani's splitting theorem, see Theorem 3, we have that a primitive representation of 4^k by the associated refined Humbert invariant $q_{\mathcal{C}}$ gives rise to a $(2^k, 2^k)$ -isogeny from $\mathcal{J}(\mathcal{C})$ to a split surface $E \times E'$. The least such exponent is exactly the quantity k_0 of Section 3, and it measures a restricted notion of distance to the split locus, which we now make precise. Write $\mathcal{S} \subset \Gamma_2^{SS}(2; p)$ for the set of vertices carrying a reducible polarization, and $d(\cdot, \cdot)$ for the graph distance in $\Gamma_2^{SS}(2; p)$.

Branching for splittings The isogeny walks based on Kani's splitting theorem, Theorem 3, are not arbitrary random walks in the isogeny graph. Recall that by Theorem 3, a primitive representation $q_{\mathcal{C}}(x) = N^2$ corresponds to an (N, N) -splitting of $\mathcal{J}(\mathcal{C})$. When an (N, N) split isogeny is a composition of lower-degree isogenies, primitiveness implies that every intermediate vertex is a Jacobian surface. Thus, we consider isogeny paths of the form

$$\mathcal{J}(\mathcal{C}) \rightarrow \mathcal{J}(\mathcal{C}_1) \rightarrow \cdots \rightarrow \mathcal{J}(\mathcal{C}_k) \rightarrow E_1 \times E_2,$$

where no intermediate vertex $\mathcal{J}(\mathcal{C}_i)$ is a split surface. In particular, the split surface can only be reached at the final vertex. Hence, the isogeny walks here are a restricted class of isogeny walks.

Moreover, when $N = \ell^k$ and the corresponding splitting is factored into (ℓ, ℓ) -isogenies, primitiveness implies that the kernel of every intermediate isogeny is isomorphic to $(\mathbb{Z}/\ell^i\mathbb{Z})^2$. Consequently, each isogeny after the first is a good extension of the preceding one in the sense of [4]. Equivalently, if $\mathcal{A}_{i-1} \rightarrow \mathcal{A}_i$ is fixed, then the kernel of the next isogeny $\mathcal{A}_i \rightarrow \mathcal{A}_{i+1}$ intersects the kernel of the dual isogeny $\mathcal{A}_i \rightarrow \mathcal{A}_{i-1}$ trivially. This condition gives a uniform reduction in the number of possible continuations of the walk. The full (ℓ, ℓ) -isogeny graph has weighted out degree $d_{\ell} = (\ell + 1)(\ell^2 + 1)$, so there are d_{ℓ}^k unrestricted isogeny walks of length k . The first isogeny has d_{ℓ} possible kernels. Once an incoming isogeny has been fixed, exactly ℓ^3 of the d_{ℓ} outgoing (ℓ, ℓ) -isogenies are good extensions; see [7, Lemma 2.1], and which is also the branching used in the good-extension digraph of [19]. Hence the number of isogeny walks of length k in which every isogeny after the first isogeny is a good extension is $\ell^{3(k-1)}d_{\ell}$.

Therefore, among all unrestricted isogeny walks of length k , the proportion satisfying the good-extension condition is $\left(\frac{\ell^3}{d_{\ell}}\right)^{k-1} = \left(\frac{\ell^3}{(\ell+1)(\ell^2+1)}\right)^{k-1}$. For the case of $\ell = 2$, this proportion is $\left(\frac{8}{15}\right)^{k-1}$. The walks associated with splittings derived from refined Humbert invariants $q_{\mathcal{C}}$ satisfy an additional restriction: every intermediate vertex must remain a Jacobian, while a split surface may occur only at the final vertex. Thus ℓ^3 is the number of good extensions available after a fixed incoming isogeny, but not every such extension is admissible for a primitive splitting. At an intermediate step, only good extensions with Jacobian codomain are allowed, whereas at the final step the codomain must be a product surface. Hence the actual branching for the splitting walks considered here is bounded above by ℓ^3 at every step after the first, and may be strictly smaller because of the requirement that the walk remain in the Jacobian locus until its final edge.

Lemma 2. *Let $(\mathcal{A}, \theta)$ be a principally polarized superspecial abelian surface with irreducible polarization and refined Humbert invariant $q_{(\mathcal{A}, \theta)}$, and let $k_0 = k_0(\mathcal{A}, \theta)$ be the least $k \geq 1$ such that $q_{(\mathcal{A}, \theta)}$ primitively represents 4^k . Then*

- (i) k_0 is the least length of a walk from $(\mathcal{A}, \theta)$ to $\mathcal{S}$ in $\Gamma_2^{SS}(2; p)$ in which every edge after the first is a good extension of its predecessor and no intermediate vertex lies in $\mathcal{S}$;
- (ii) consequently $d((\mathcal{A}, \theta), \mathcal{S}) \leq k_0$, with equality if and only if some geodesic from $(\mathcal{A}, \theta)$ to $\mathcal{S}$ is a chain of good extensions; and
- (iii) equality holds in (ii) whenever $k_0 \leq 2$.

Proof. (i) By Theorem 3, a primitive representation of 4^k by $q_{(\mathcal{A}, \theta)}$ is equivalent to a $(2^k, 2^k)$ -isogeny $\varphi : \mathcal{A} \rightarrow E_1 \times E_2$, that is, one whose kernel is maximal isotropic in $\mathcal{A}[2^k]$ and hence isomorphic to $(\mathbb{Z}/2^k\mathbb{Z})^2$. Factoring φ into k successive $(2, 2)$ -isogenies, the condition on $\ker \varphi$ says precisely that each step after the first is a good extension of the preceding one, and primitivity says that no intermediate codomain lies in $\mathcal{S}$; both points are the content of the branching discussion above. Conversely, a walk with these two properties composes to an isogeny with kernel $(\mathbb{Z}/2^k\mathbb{Z})^2$, hence to a $(2^k, 2^k)$ -splitting, hence to a primitive representation of 4^k . Minimality of k_0 now gives the claim.

(ii) The walk furnished by (i) has length k_0 and ends in $\mathcal{S}$, so $d((\mathcal{A}, \theta), \mathcal{S}) \leq k_0$. If some geodesic is a chain of good extensions then its length is at least k_0 by the minimality in (i), and at most k_0 because it is a geodesic; so the two agree. Conversely, if $d((\mathcal{A}, \theta), \mathcal{S}) = k_0$ then the walk furnished by (i) has length exactly $d((\mathcal{A}, \theta), \mathcal{S})$, so it is itself a geodesic — and it is a chain of good extensions.

(iii) By Theorem 3, $q_{(\mathcal{A}, \theta)}$ primitively represents 4 precisely when $\mathcal{A}$ is $(2, 2)$ -split, that is, precisely when $\mathcal{A}$ has a neighbor in $\mathcal{S}$; so $k_0 = 1$ if and only if $d((\mathcal{A}, \theta), \mathcal{S}) = 1$. Since θ is irreducible, $(\mathcal{A}, \theta) \notin \mathcal{S}$ and hence $d((\mathcal{A}, \theta), \mathcal{S}) \geq 1$. So if $k_0 = 2$ then $d((\mathcal{A}, \theta), \mathcal{S}) \neq 1$, while $d((\mathcal{A}, \theta), \mathcal{S}) \leq 2$ by (ii); the two therefore agree. $\square$

Whether the inequality in (ii) can be strict we leave open: by (iii) any witness must have $k_0 \geq 3$, and deciding the question requires the graph distance d , which the method of this paper does not compute.

Thus k_0 is an upper bound for the graph distance to the split locus, and is exactly the distance measured along walks that correspond to a single $(2^k, 2^k)$ -isogeny. The latter is the quantity of cryptographic interest, since it is (N, N) -isogenies, and not arbitrary walks, that one computes. In fact, the set of all primitively represented 4^k for exponents k describes the set of split surfaces reachable from $\mathcal{J}(\mathcal{C})$ by isogenies of degree $(2^k, 2^k)$. Therefore, we restrict our attention to values of k up to a diameter bound k_{diameter} for the isogeny graph of principally polarized superspecial abelian surfaces. By the discussion in Section 2.2, the Chung–Faber–Manteuffel estimate gives $k_{\text{diameter}} = 4.20 \log_2(p) + O(1)$ unconditionally, and $k_{\text{diameter}} = 3 \log_2(p) + O(1)$ under [28, Conjecture 4.10]; for any fixed p a rigorous bound is obtained by substituting the exact value $M = \#\Gamma_2^{SS}(2; p)$ into that inequality. For the small primes of [28, Appendix A] the diameter has been computed exactly, see Table 1, and we use the tabulated value in place of the bound whenever it is available.

Our data is obtained differently from that of [28]: they construct the full Richelot isogeny graph, computing the surfaces via Igusa–Clebsch invariants and the edges via compact Richelot isogeny formulas, whereas we read the same information off the refined Humbert invariant.

Remark 1. The difference between our method and the results in [12] is one of input: we use neither the equations of the genus 2 curve, which would be obtained by computing Igusa invariants, nor an explicit chain of isogenies. We emphasize that we simply chose a random Jacobian in the

isogeny graph, and that we do not know the equations of the curve $\mathcal{C}$ of genus 2. We make no claim of a runtime advantage: we have not benchmarked the two approaches against one another, and any such comparison would depend on the regime of N , since [12] targets prescribed $N \leq 11$ whereas N is determined intrinsically here.

Remark 2. It is an interesting question whether one can compute the refined Humbert invariant $q_{\mathcal{C}}$ for a given model of curve $\mathcal{C}$ of genus 2. The question of finding an algorithm to determine $q_{\mathcal{C}}$ for a given curve $\mathcal{C}$ is mostly open. Note that there is no such algorithm to compute the quintic refined Humbert invariant $q_{\mathcal{C}}$ for a given model of $\mathcal{C}$. The existence of such an algorithm would be a powerful method for isogeny graphs and isogeny problems, yet it is challenging to solve in the general case. Evidence that this difficulty is intrinsic is given by Kırımlı–Martindale [61], who show that in the settings of SQIsign and CSIDH, and under GRH, the computational isogeny problem is polynomially equivalent to the computational refined Humbert invariant problem; that work also surveys what is known about computing refined Humbert invariants.

4.2 Detecting endomorphisms

For supersingular elliptic curves, computing endomorphisms is essentially as hard as finding isogenies [103]; Wesolowski showed a GRH-based polynomial-time reduction between the isogeny problem over $\mathbb{F}_{p^2}$ and the endomorphism ring problem. Further, Page–Wesolowski showed that finding a single nontrivial $\varphi \in \text{End}(E)$ is equivalent to solving the supersingular isogeny problem [86]. This naturally raises the question of whether a similar equivalence holds in dimension 2, yet there is neither a widely accepted algorithm nor a mature complexity analysis for computing endomorphism rings of superspecial principally polarized abelian surfaces. We now show that the refined Humbert invariant gives a direct arithmetic test for real multiplication, and use it to estimate how common RM is among superspecial surfaces. Recall from Appendix A.1 that every $\mathcal{H}(q)$ is contained in any Humbert surface $\mathcal{H}_N$ that q primitively represents, in arbitrary characteristic by [51, Definition 8, Proposition 12].

We investigate RM orders experimentally using the complete sets of principal polarizations for small primes up to 191, and, separately, by sampling 100,000 random principal polarizations for each prime $227 \leq p \leq 1619$ and determining the primitively represented square-free discriminants $D \leq 100$.

Frequency of real multiplication with refined Humbert invariants $q_{(\mathcal{A}, \theta)}$ We describe an experiment to estimate the frequency of principally polarized superspecial abelian surfaces admitting real multiplication by a prescribed quadratic order $\mathcal{O}_D$. For each sampled principally polarized superspecial abelian surface $v_i = (\mathcal{A}, \theta_i)$ over $\overline{\mathbb{F}}_p$, we compute its quintic refined Humbert invariant $q_i = q_{(\mathcal{A}, \theta_i)}$.

Fix a positive discriminant D corresponding to a real quadratic order $\mathcal{O}_D$. We test whether q_i primitively represents D , namely, whether there exists a primitive vector x such that $q_i(x) = D$. By the primitive-representation criterion, see Theorem 10, this detects an embedding of the corresponding real quadratic order $\mathcal{O}_D$ into the additive subgroup $\text{End}_{\theta_i}(\mathcal{A})$ consisting of endomorphisms fixed by the Rosati involution with respect to θ_i .

Thus, RM detection is carried out directly from q_i , without requiring genus 2 curve equations, Igusa invariants, explicit equations for describing the Humbert surfaces, or the computation of Richelot isogenies or (ℓ, ℓ) -isogenies.

A further advantage is that a single sampled refined Humbert invariant q_i can be tested simultaneously for many discriminants D . Once q_i is computed, we determine the set of positive discriminants $D \leq D_{\max}$ that it primitively represents. The same collection of sampled principally

polarized abelian surfaces therefore yields estimates for all discriminants in the prescribed range and allows the resulting data to be grouped according to arithmetic invariants of $\mathcal{O}_D$, such as its class number or narrow class number. We further emphasize that our method does not require the class number or narrow class number of $\mathcal{O}_D$ to be equal to 1.

Motivated by the square-discriminant case [28, Section 6.2], the following heuristic on the distribution of RM vertices is extended in [13, Section 8.2] to an arbitrary discriminant D by introducing a function $\tilde{\mathfrak{D}}_D$. The expected number of steps required for a random walk in $\Gamma_2^{SS}(2; p)$ to reach an abelian surface admitting RM by $\mathcal{O}_D$ is then predicted to be

$$\frac{p}{\tilde{\mathfrak{D}}_D} + O(1), \quad (4)$$

where $\tilde{\mathfrak{D}}_D = O(D^{3/2})$ and, for square discriminants $D = N^2$, it satisfies $\tilde{\mathfrak{D}}_{N^2} = 5\mathfrak{D}_N$ with $\mathfrak{D}_N$ denoting the number of maximal isotropic (N, N) -subgroups of the N -torsion of a principally polarized abelian surface. A heuristic for $\tilde{\mathfrak{D}}_D$ is given in [13] as follows. Let D be a fundamental discriminant such that $\mathcal{O}_D$ has narrow class number one, and let $K = \text{Frac}(\mathcal{O}_D)$. As explained in [13, §8.2.1], combining [80, Theorem 2.5.35] with the Eichler mass formula [100, Theorem 26.1.5] gives the estimate $\frac{\zeta_K(2)D^{3/2}}{8\pi^4}p^2 + O(p)$ for the number of superspecial principally polarized abelian surfaces equipped with an embedding $\mathcal{O}_D \hookrightarrow \text{End}(\mathcal{A})$, with the discrepancy from the unweighted count governed by the Eichler class number formula. For $D \ll p$, it is further expected that almost every surface admitting RM by $\mathcal{O}_D$ gives rise to exactly two such embeddings. This leads to the following heuristic $\tilde{\mathfrak{D}}_D = \frac{1}{2} \frac{360\zeta_K(2)}{\pi^4} D^{3/2}$.

Remark 3. In contrast to the random-walk experiment of [13], we estimate the occurrence of real multiplication directly from refined Humbert invariants. Rather than starting from a fixed vertex of the superspecial $(2, 2)$ -isogeny graph and measuring the first hitting time of the locus admitting RM by $\mathcal{O}_D$, we sample principally polarized superspecial abelian surfaces $(\mathcal{A}, \theta)$, compute their refined Humbert invariants $q_{(\mathcal{A}, \theta)}$, and test whether D is primitively represented. This directly estimates the density $\delta_D(p) = \Pr(q_{(\mathcal{A}, \theta)} \text{ primitively represents } D)$ of vertices admitting RM by $\mathcal{O}_D$. In [13], μ_D denotes the mean number of steps in $\Gamma_2^{SS}(2; p)$ required to encounter a principally polarized abelian surface with RM by $\mathcal{O}_D$. Under the heuristic that a sufficiently mixed Richelot walk samples from the same distribution, one expects $\mu_D \simeq \delta_D(p)^{-1}$ and hence $p/\mu_D \simeq p\delta_D(p)$. Our approach neither uses explicit curve equations nor a random walk in the Richelot isogeny graph; instead, the main issue is to ensure that the sampled polarizations induce the desired distribution on principally polarized isomorphism classes.

4.3 Automorphism groups

Computing refined Humbert invariants detects genus 2 Jacobians with extra automorphisms and thereby identifies special vertices and their local neighborhoods in the isogeny graph. This viewpoint was investigated experimentally for Richelot graphs in [28] using reduced automorphism groups. By Proposition 6, the refined Humbert invariants determine the automorphism group of the corresponding principally polarized abelian surface.

Here, we illustrate some experiments verifying the relationship between the automorphism groups of curves $\mathcal{C}$ of genus 2 and their associated refined Humbert invariants $q_{\mathcal{C}}$. Note that the list of possibilities for $\text{Aut}(\mathcal{C})$ for any genus 2 curve is given in the first row of Table 4, see [94, Theorem 2], [2]. Recall from Proposition 6 that if $\iota(\text{Aut}(\mathcal{C}))$ denotes the number of involutions of the group $\text{Aut}(\mathcal{C})$, then we have that $\iota(\text{Aut}(\mathcal{C})) - 1 = r_4(q_{\mathcal{C}})$ by [53, Proposition 26]. Although the statement of Theorem 2 is given by reduced automorphism groups $\text{RA}(\mathcal{C})$, we converted them back to $\text{Aut}(\mathcal{C})$ in Table 2.

The polarizations used here are not sampled: we take them from the exhaustive enumeration of [60, Algorithm 2], which as recalled in Section 3 is complete for $p \leq 191$ and, at $p = 227, 239, 251$, misses only reducible polarizations, so that the irreducible ones — the case of interest here — are complete throughout the range. For the primes $p \in \{11, 23, 47, 59, 71, 83, 107, 131, 167, 179, 191, 227, 239, 251\}$ we compute the refined Humbert invariant of every polarization, discard those that represent 1, and classify the remainder up to isometry. These are the refined Humbert invariants q_C corresponding to principally polarized superspecial surfaces (with irreducible polarizations) $(\mathcal{A}, \theta) = (\mathcal{J}(\mathcal{C}), \theta_C)$.

Table 2. Automorphism data for the principal polarizations of $\mathcal{A} = E \times E$, enumerated with [60, Algorithm 2]. The count columns are: $\#\Theta = \mathbf{H}(p)$, the principal polarizations up to isomorphism; $\#\text{RHI}_{\text{irred}} = \mathbf{H} - \frac{\mathbf{h}(\mathbf{h}+1)}{2}$, those that are irreducible; $\#\text{RHI}_{\text{iso}}$, the number of distinct refined Humbert invariants they realize up to isometry; and $\#\text{Gen } q_{5 \text{ not } 1}$, the number of classes in the genus of q_5 that do not represent 1. The last two columns agree in every row, so the irreducible polarizations realize *every* class of the genus that does not represent 1. Within each pair, the first entry is the number of *polarizations* predicted by Theorem 2 (the column sums to $\#\text{RHI}_{\text{irred}}$), and the second the number of *isometry classes* observed (summing to $\#\text{RHI}_{\text{iso}}$); these count different objects, so they coincide only where little collapse occurs. The C_{10} entries are marked by $*$ because r_4 cannot separate C_2 from C_{10} ; see the discussion after the table.

p	$\#\Theta$	$\#\text{RHI}_{\text{irred}}$	$\#\text{RHI}_{\text{iso}}$	$\#\text{Gen } q_{5 \text{ not } 1}$	# Aut($\mathcal{C}$) type: (Theorem 2 bound, Table 4 count)						
					C_2	C_{10}	$C_2 \times C_2$	D_4	D_6	$C_3 \rtimes D_4$	$\text{GL}_2(\mathbb{F}_3)$
11	5	2	2	2	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(1, 1)	(1, 1)	(0, 0)
23	16	10	9	9	(0, 0)	(0, 0)	(5, 4)	(1, 1)	(2, 2)	(1, 1)	(1, 1)
47	72	57	43	43	(14, 9)	(0, 0)	(31, 23)	(4, 4)	(6, 5)	(1, 1)	(1, 1)
59	125	104	74	74	(35, 25)	(1, 1 $*$)	(52, 35)	(6, 5)	(9, 7)	(1, 1)	(0, 0)
71	198	170	116	116	(70, 42)	(0, 0)	(81, 58)	(7, 6)	(10, 8)	(1, 1)	(1, 1)
83	296	260	165	165	(123, 80)	(0, 0)	(114, 67)	(9, 7)	(13, 10)	(1, 1)	(0, 0)
107	581	526	311	311	(296, 178)	(0, 0)	(200, 111)	(12, 8)	(17, 13)	(1, 1)	(0, 0)
131	1008	930	554	554	(583, 340)	(0, 0)	(310, 186)	(15, 11)	(21, 16)	(1, 1)	(0, 0)
167	1978	1858	1058	1058	(1290, 709)	(0, 0)	(521, 313)	(19, 15)	(26, 19)	(1, 1)	(1, 1)
179	2404	2268	1266	1266	(1614, 894)	(1, 1 $*$)	(602, 336)	(21, 14)	(29, 20)	(1, 1)	(0, 0)
191	2886	2733	1540	1540	(1988, 1079)	(0, 0)	(691, 420)	(22, 17)	(30, 22)	(1, 1)	(1, 1)
227	4712	4502	2425	2425	(3447, 1848)	(0, 0)	(990, 533)	(27, 18)	(37, 25)	(1, 1)	(0, 0)
239	5460	5229	2869	2869	(4057, 2164)	(1, 1 $*$)	(1103, 654)	(28, 21)	(38, 27)	(1, 1)	(1, 1)
251	6281	6028	3271	3271	(4736, 2541)	(0, 0)	(1220, 680)	(30, 21)	(41, 28)	(1, 1)	(0, 0)

Two comparisons in Table 2 are meaningful, and one is not. First, each column sums to the total it should: the predicted counts sum to $\#\text{RHI}_{\text{irred}}$ and the observed ones to $\#\text{RHI}_{\text{iso}}$, in every row. Second, for the rare types D_4 , D_6 , $C_3 \rtimes D_4$ and $\text{GL}_2(\mathbb{F}_3)$ the two entries of a pair are equal or nearly so, because almost no collapse occurs there; in particular the unique $C_3 \rtimes D_4$ curve, and the unique $\text{GL}_2(\mathbb{F}_3)$ curve whenever Theorem 2 predicts one, are recovered at every prime tested. By contrast, no agreement should be expected in the C_2 and $C_2 \times C_2$ columns: at $p = 251$ the C_2 entry falls from 4736 predicted polarizations to 2541 observed isometry classes, which measures the collapse and not a discrepancy, since the two numbers count different objects. A further observation is that $\#\text{RHI}_{\text{iso}}$ equals $\#\text{Gen } q_{5 \text{ not } 1}$ in every row: the irreducible polarizations of $E \times E$ realize the full genus of q_5 away from the classes representing 1. The entries marked with a star require a caveat. By Table 4 we have $r_4(q_C) = 0$ for both $\text{Aut}(\mathcal{C}) \cong C_2$ and $\text{Aut}(\mathcal{C}) \cong C_{10}$, so the refined Humbert invariant cannot distinguish these two cases; the C_{10} entries are therefore

not an independent measurement, but the count of Theorem 2 subtracted from the total number of classes with $r_4 = 0$. More generally, the counts we obtain are smaller than the predicted ones because two different principally polarized surfaces $(\mathcal{J}(\mathcal{C}), \theta_{\mathcal{C}})$ and $(\mathcal{J}(\mathcal{C}'), \theta_{\mathcal{C}'})$ can share a refined Humbert invariant $q_{\mathcal{C}} \sim q_{\mathcal{C}'}$ up to equivalence.

An experiment of this kind was carried out in [28], where they construct Richelot isogeny graphs and compute chains of isogenies and Igusa-Clebsch invariants. In contrast, our approach does not require the explicit construction or navigation of the full isogeny graph of principally polarized superspecial abelian surfaces, but we do not know which automorphism group belongs to which principally polarized superspecial surface. Instead, we compute the associated refined Humbert invariants directly, thereby extracting the necessary information without enumerating the vertices and edges of the underlying graph. Moreover, the proposed method is generic in the sense that it is independent of any auxiliary choice of a particular (ℓ, ℓ) -isogeny graph. Given that the set of polarizations is complete, we can also count curves $\mathcal{C}$ of genus 2 with specified $\text{Aut}(\mathcal{C})$ just by checking the representation of 4 by the corresponding quintic refined Humbert invariant $q_{\mathcal{C}}$.

5 Data

5.1 The experiment with all the polarizations for small primes

Splittings We start with small characteristic primes p for which all principal polarizations are known, using the verified polarizations from [60]. This enables us to analyze the full splitting behavior of $(2^k, 2^k)$ -isogeny walks in the superspecial Richelot isogeny graph $\Gamma_2^{SS}(2; p)$ and of $(3^k, 3^k)$ -isogeny walks in the superspecial $(3, 3)$ -isogeny graph $\Gamma_2^{SS}(3; p)$, for primes $11 \leq p \leq 191$. The same experiment can be carried out efficiently for other small primes ℓ , particularly for $\ell < 31$.

In the first experiment in Figure 1(a), we record, for each refined Humbert invariant in the sample and for each $\ell \in \{2, 3\}$, the smallest exponent $k_{\min}$ for which ℓ^{2k} is primitively represented. The resulting distributions are shown as functions of p . For the smaller primes, primitive representation frequently occurs already at $k = 1$, whereas for larger p the mass gradually shifts toward $k_{\min} = 2$ and $k_{\min} = 3$. This shift is more pronounced for $\ell = 2$: throughout the larger-prime range, the $\ell = 3$ experiment places a substantially larger proportion of the forms at $k_{\min} = 1$ or 2. Thus, although the smallest represented exponent tends to increase with p , the computations indicate that primitive representations of powers of 3 are typically attained at smaller exponents than the corresponding powers of 2. This is what the branching count of Section 4 predicts: the (ℓ, ℓ) -isogeny graph has weighted degree $d_{\ell} = (\ell + 1)(\ell^2 + 1)$, so $d_2 = 15$ against $d_3 = 40$, and the number of good extensions available after a fixed incoming isogeny is ℓ^3 , so 8 against 27. Balls around a vertex therefore grow considerably faster at $\ell = 3$, and the split locus is met at a smaller exponent, which is precisely the shift seen between the two panels.

The second experiment in Figure 1(b) measures the extent to which each refined Humbert invariant represents the entire range of tested powers, rather than only the first one that occurs. For each form, we count the tested exponents k for which ℓ^{2k} fails to be primitively represented, with a separate class for forms representing every tested value $1 \leq k \leq K_{\max}$; here $K_{\max} = \lceil \ln p \rceil$ as in Section 3.2, which is 3 at $p = 11$ and 6 at $p = 251$. The proportion representing all tested exponents decreases as p grows, particularly for $\ell = 2$, while the corresponding proportion for $\ell = 3$ remains consistently larger. Nevertheless, the overwhelming majority of forms represent all but at most one or two of the tested exponents. This experiment, therefore, complements the $k_{\min}$ -distribution by showing that a small first represented exponent does not by itself determine the subsequent representation pattern, and by quantifying how close the observed forms are to representing the full tested range.

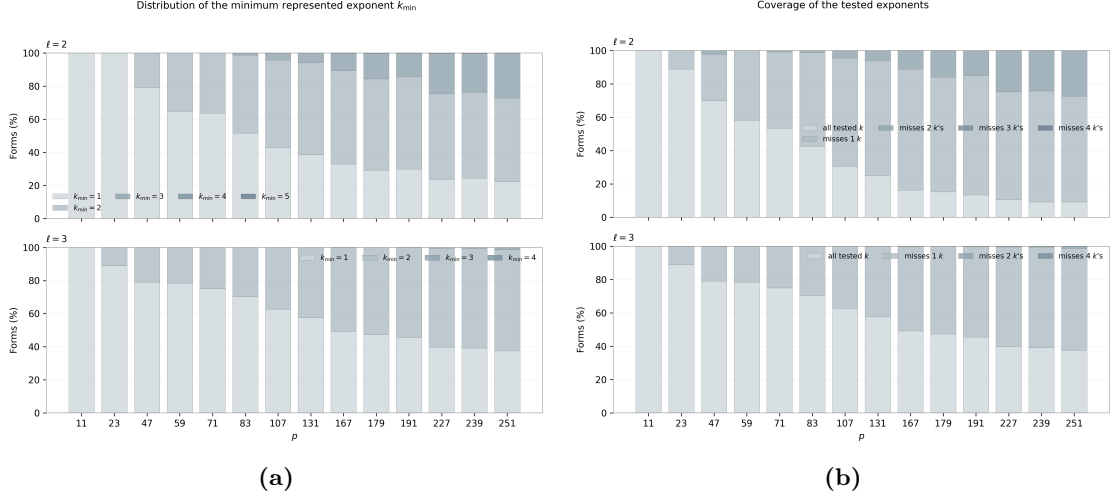


Fig. 1. (a) For each prime p , the stacked bars give the proportion of refined Humbert invariants for which $k_{\min} = k$, where $k_{\min}$ is the smallest tested exponent such that ℓ^{2k} is primitively represented. The upper and lower panels correspond to $\ell = 2$ and $\ell = 3$, respectively. As p increases, the distribution shifts from $k_{\min} = 1$ toward larger values, with the shift occurring more slowly for $\ell = 3$ than for $\ell = 2$. (b) For each prime p , the stacked bars record the proportion of refined Humbert invariants according to the number of tested exponents k for which ℓ^{2k} is not primitively represented. The segment labelled “all tested k ” consists of forms representing ℓ^{2k} primitively for every $1 \leq k \leq K_{\max}$; the remaining segments distinguish forms missing one or more tested values of k . The upper and lower panels correspond to $\ell = 2$ and $\ell = 3$, respectively, where $K_{\max} = \lceil \ln p \rceil$ is the maximal exponent tested for the corresponding prime p .

RM vertices We start with small characteristic primes p for which all principal polarizations are known, using the verified polarizations from [60]. We report how RM by $\mathcal{O}_D$ appears for the full isogeny graphs for these primes. By a *Type* we mean an isometry class of refined Humbert invariants occurring in the sample. Distinct principally polarized surfaces may share a Type, so each Type accounts for at least one, and possibly several, vertices of the isogeny graph. For each prime p and each Type, we consider the primitively represented square-free values, excluding $D = 1$, and define $D_{\min} := \min\{D > 1 : D \text{ is primitively represented}\}$.

Figure 2(a) shows the distribution of $D_{\min}$ across the Types for each p , with marker area proportional to the corresponding proportion. The minima are concentrated mainly at $D = 5, 13$, and 17 , while larger values occur with substantially lower frequency. The second figure considers the cumulative proportion $F_p(D_0) := \frac{\#\{T: D_{\min}(T) \leq D_0\}}{\#\{T\}}$ for $D_0 \in \{5, 13, 17, 21, 29\}$. Thus, $F_p(D_0)$ measures the proportion of Types for which a nontrivial primitive representation occurs by the threshold D_0 . Although the proportions for the smallest thresholds decrease as p grows, the thresholds $17, 21$, and 29 still account for a large proportion of the Types.

5.2 The experiment with random polarizations for small primes

For each prime $p \equiv 11 \pmod{12}$ with $227 \leq p \leq 1619$, we sample 100,000 random polarizations with Algorithm 1 and compute the corresponding refined Humbert invariants. For every resulting Type, we test primitive representations of the square-free integers $D \leq 100$. Since $D = 1$ corresponds to the trivial case, we exclude it and define $D_{\min}(T) := \min\{D > 1 : D \text{ is primitively represented by } q_T\}$.

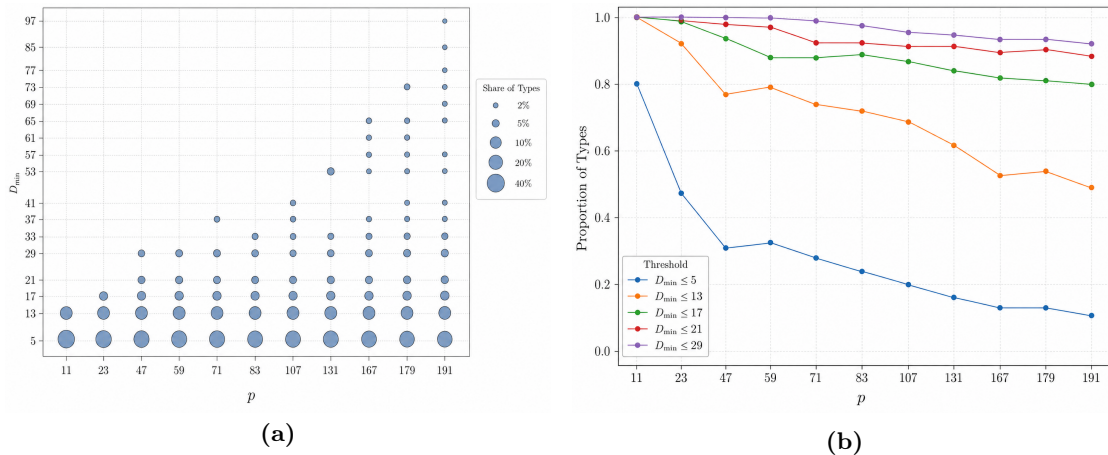


Fig. 2. (a) Distribution of the minimum primitively represented value $D_{\min}$ for each prime p . For each Type, the value $D = 1$ is excluded and $D_{\min}$ denotes the least remaining primitively represented value. For each pair $(p, D_{\min})$, the marker area is proportional to the fraction of Types attaining that minimum. (b) Cumulative proportions of Types satisfying prescribed bounds on $D_{\min}$. For each prime p , after excluding $D = 1$, the curves give the proportion of Types for which $D_{\min} \leq D_0$, with $D_0 \in \{5, 13, 17, 21, 29\}$.

Figure 3(a) describes the distribution of the first nontrivial represented value. For each prime p and value D , the marker area is proportional to the fraction of recorded Types satisfying $D_{\min} = D$. The experiment, therefore, measures how early, with respect to the discriminant bound, a nontrivial primitive representation is encountered. The distribution is strongly concentrated at small values, principally $D_{\min} = 5, 13$, and 17 , whereas Types whose first primitive representation occurs at a substantially larger discriminant form only a sparse upper tail.

Figure 3(b) gives a cumulative description of the same data. For each threshold $D_0 \in \{5, 13, 17, 21, 29\}$, we compute $F_p(D_0) := \frac{\#\{T: D_{\min}(T) \leq D_0\}}{\#\{T\}}$, where T ranges over the recorded Types obtained from the random-polarization experiment for the prime p . Thus, $F_p(D_0)$ is the empirical proportion for which a nontrivial primitive representation has already occurred by the time the search reaches D_0 . The curves show that the proportion attaining the very smallest values decreases as p increases. Nevertheless, a large fraction of the Types still satisfy $D_{\min} \leq 17$, and allowing the threshold to increase to 21 or 29 captures an even larger proportion. Hence, throughout the tested range of primes, the first nontrivial primitive representation is typically found at a comparatively small discriminant.

This experiment also serves as a partial check on the sampler. Figure 2 and Figure 3 record the same statistic, the distribution of $D_{\min}$ over Types, computed once from the complete set of principal polarizations ($11 \leq p \leq 191$) and once from 100,000 draws of Algorithm 1 ($227 \leq p \leq 503$). The two ranges do not overlap, so we cannot compare the two directly; what we can say is that the sampled curves continue the exhaustive ones without a visible discontinuity at the join, with $F_p(5)$ passing from 0.11 at $p = 191$ to 0.10 at $p = 227$, and that $D_{\min}$ concentrates on 5, 13 and 17 in both. A like-for-like comparison would require running the sampled experiment at a prime where the exhaustive list of [60] is also available; we have not done so, and the distribution Algorithm 1 induces on isometry classes therefore remains uncharacterized, as noted in Section 6.

Experimental distribution of RM vertices. We summarize the experimental data in [13] for the distribution of RM surfaces by $\mathcal{O}_D$ in the isogeny graph of principally polarized superspecial abelian surfaces. The observed values suggest that the leading term in (4) can be more accurately

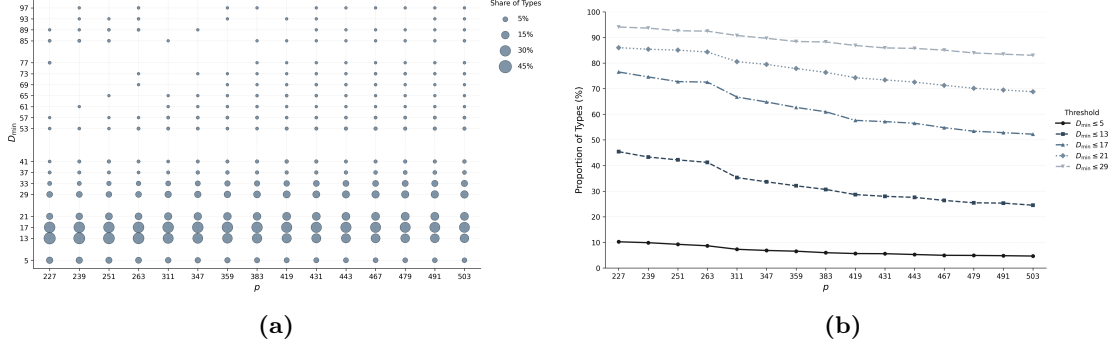


Fig. 3. (a) Empirical distribution of the minimum primitively represented value $D_{\min}$ obtained from the 100,000-polarization sampling experiment. For each recorded Type, we exclude $D = 1$ and define $D_{\min}$ to be the least remaining primitively represented square-free value. For each pair $(p, D_{\min})$, the marker area is proportional to the fraction of recorded Types attaining that minimum. Types for which no value $D > 1$ is represented up to 100 are omitted from this distribution.

(b) Cumulative proportions of the recorded Types satisfying prescribed bounds on $D_{\min}$. For each prime p and threshold $D_0 \in \{5, 13, 17, 21, 29\}$, the plotted value is the proportion of Types obtained from the 100,000-polarization sampling experiment for which $D_{\min} \leq D_0$. Thus, each curve measures how frequently a first nontrivial primitive representation occurs by the corresponding threshold D_0 .

approximated by $p/\tilde{\mathfrak{D}}_D^{\text{expt}}$. These experiments appear to suggest that the leading term in (4) should be closer to $p/\tilde{\mathfrak{D}}_D^{\text{expt}}$ where

$$\tilde{\mathfrak{D}}_D^{\text{expt}} = \begin{cases} \frac{5}{4} \mathfrak{D}_N & \text{if } D = N^2, \text{ and} \\ \frac{1}{3} \cdot \frac{360\zeta_K(2)}{\pi^4} D^{3/2} & \text{if } D \text{ is fundamental.} \end{cases} \quad (5)$$

The condition of narrow class number being 1 is not needed for us. Nevertheless, the heuristic still aligns with our experimental data, even when $\mathcal{O}_D$ does not have narrow class number 1.

5.3 Large primes

The two experiments reported here are independent. The first fixes a single 50-bit prime and measures the least splitting level k_0 with Algorithm 2; the second ranges over twenty primes of up to 1000 bits and measures the splitting degrees returned by Algorithm 3. Their samples were drawn separately.

The least level k_0 at a 50-bit prime. Fix $p = 2^{11} \cdot 3^{24} - 1$, of 50 bits, and $\ell = 2$. We sample 10,000 classes with irreducible polarization from the genus of $L_5 = (\mathbb{Z}^5, q_5)$ — refined Humbert invariants of determinant $16p^2$ — and compute k_0 for each.

The lattice minima are close to extremal. Here $(\det G_q)^{1/5} = 1.3987 \cdot 10^6$, so Hermite's bound $\gamma_5(\det G_q)^{1/5}$ with $\gamma_5 = 8^{1/5} = 1.5157$ is $2.1200 \cdot 10^6$, while the largest minimum in the sample is $\lambda_1 = 1.214(\det G_q)^{1/5}$. Every class therefore has a minimum within 20% of the smallest attainable by a rank-five lattice of this determinant, so the barrier k_1 of (2) is set by the forms themselves and not by slack in the bound.

Figure 4 gives the three distributions. The barrier is sharply concentrated: 73.27% of the classes have $k_1 = 10$ and 23.07% have $k_1 = 11$, the remaining 3.66% lying at 8 or 9. The leading term of (2) is $\frac{1}{5} \log_2 p = 9.81$ at this prime, so almost every class attains that estimate to within

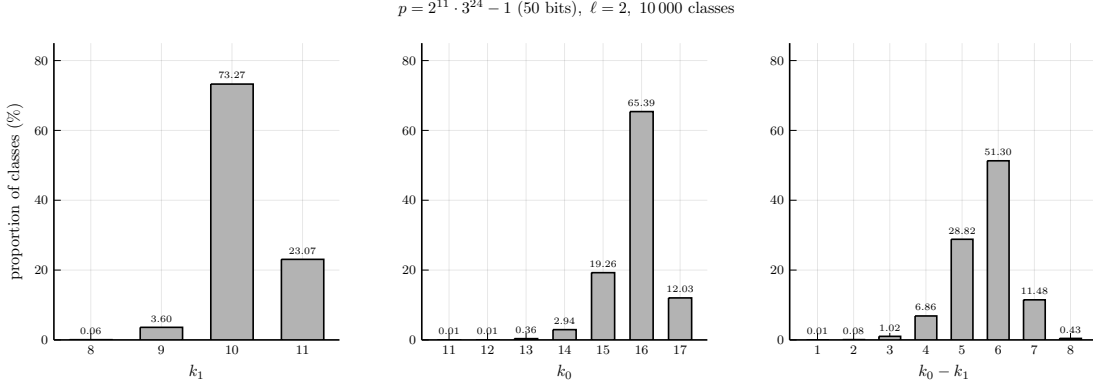


Fig. 4. The 10,000 sampled classes at $p = 2^{11} \cdot 3^{24} - 1$ with $\ell = 2$: the barrier k_1 of (2), the least splitting level k_0 , and their difference. The barrier concentrates on the leading term $\frac{1}{5} \log_2 p$; the level lies some six steps above it; the two never coincide.

one step. The level k_0 sits some six steps higher: 65.39% of the classes have $k_0 = 16$ and a further 31.29% have $k_0 = 15$ or 17, with a thin tail reaching down to $k_0 = 11$. The mean is 15.86, that is $0.32 \log_2 p$.

The third panel shows that the two never coincide. The smallest difference in the sample is $k_0 - k_1 = 1$, attained by one class in 10,000; the distribution is centred on 6 (51.30%) and 5 (28.82%), with mean 5.66. The reason is that the targets 4^k are sparse. The barrier certifies only that 4^{k_1} is not excluded by the lattice minimum, whereas a representation requires $r(L, 4^k) > 0$. For a rank-five lattice $r(L, m) \asymp m^{3/2} / \sqrt{\det G_q}$, so the shells of norm 4^k stay empty until $4^{3k/2} \gtrsim \sqrt{\det G_q}$, that is until $k \gtrsim \frac{1}{6} \log_2 \det G_q$; requiring the representing vector to be primitive removes a further thin set. Against $k_1 \approx \frac{1}{10} \log_2 \det G_q$ this predicts a difference growing like $\frac{1}{15} \log_2 \det G_q$, which is the order of magnitude observed.

The same count gives $k_0 \approx \frac{1}{6} \log_2 (16p^2)$, so k_0 should grow linearly in $\log_2 p$ with slope near $\frac{1}{3}$; the measured $0.32 \log_2 p$ agrees with this. The observed value falls far short of the diameter bounds of Section 2.2, which at this prime give $3 \log_2 p = 147$ conditionally and $4.20 \log_2 p = 206$ unconditionally, so the stopping criterion of Section 3.2 never binds in practice.

Unrestricted splitting degrees at cryptographic sizes. Next, we apply Algorithm 3 to the primes in [13, Table 6], drawing 100,000 classes independently for each prime.

Figure 5 carries the finding of most direct cryptographic relevance. In both panels the histogram of $\log_2 N$ concentrates on the dashed line $\log_2 p$, and the shape of the distribution is essentially unchanged between 50 and 1000 bits. The witness returned by Algorithm 3 therefore has N of roughly the size of p , so the (N, N) -splitting it detects has degree about p^2 , uniformly across the whole range of parameters we tested.

Write $P^*(N) = \max\{\ell^e : \ell^e \parallel N\}$ for the largest prime-power divisor of $N \geq 2$, with $P^*(1) = 1$. For $B \geq 2$, N is *B-power-smooth* if $P^*(N) \leq B$; this is the notion relevant to isogeny computation and the one tabulated below.

Table 3 records a negative result as much as a positive one. Up to 250 bits the smoothest witness found is genuinely power-smooth, with $\log_2 P^*(N)$ between 7.5 and 35.5. From 300 bits upward, however, the best of the 100 000 witnesses sampled at that prime still carries a prime factor of between 184 and 897 bits, and $\log_2 P^*(N)$ tracks $\log_2 N$ closely. In other words, Algo-

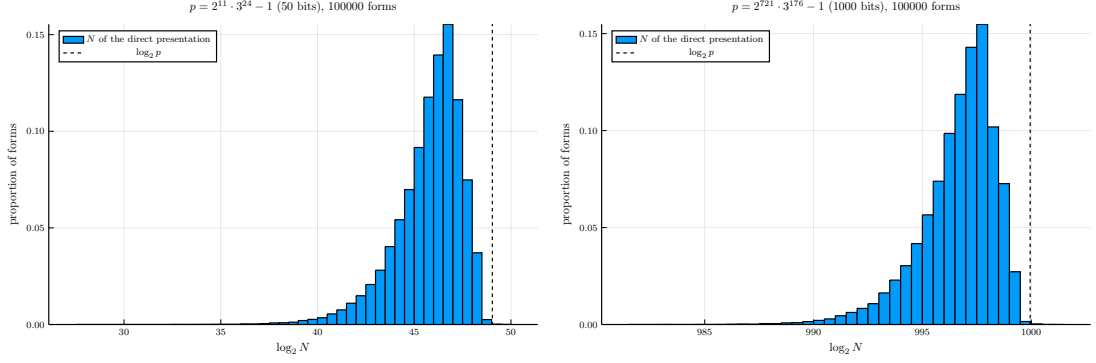


Fig. 5. The histogram of $\log_2 N$ at 50 bits (left) and 1000 bits (right), from the per-prime reports; the dashed line is $\log_2 p$. The same shape, shifted by 950 bits.

bits	p	class	$\log_2 N$	$\log_2 P^*(N)$	N
50	$2^{11} \cdot 3^{24} - 1$	89 352	42.1	7.5	$2^3 \cdot 3^3 \cdot 5 \cdot 23 \cdot 73 \cdot 103 \cdot 137 \cdot 181$
100	$2^{44} \cdot 3^{35} - 1$	71 177	94.8	15.5	$2 \cdot 131 \cdot 241 \cdot 269 \cdot 8219 \cdot 13177 \cdot 13229 \cdot 30113 \cdot 45893$
150	$2^{27} \cdot 3^{77} - 1$	87 317	147.3	24.5	$2 \cdot 223 \cdot 1511 \cdot 3323 \cdot 48029 \cdot 163433 \cdot 165041 \cdot 489761 \cdot 6480421 \cdot 24222791$
200	$2^{144} \cdot 3^{35} - 1$	41 518	195.3	28.4	$2 \cdot 23431 \cdot 363833 \cdot 505927 \cdot 1131103 \cdot 1143013 \cdot 3094361 \cdot 68911559 \cdot 69813571 \cdot 363789383$
250	$2^{181} \cdot 3^{43} - 1$	59 632	247.4	35.5	$2^6 \cdot 9293 \cdot 482753 \cdot 5258807 \cdot 23598691 \cdot 255769463 \cdot 849190603 \cdot 28251002411 \cdot 29155313437 \cdot 48311528479$
300	$5 \cdot 2^{193} \cdot 3^{66} - 1$	1 765	296.0	184.0	$2 \cdot 3^5 \cdot 11 \cdot 17 \cdot 179 \cdot 38821 \cdot 84011 \cdot 300491 \cdot 388253 \cdot 828967 \cdot \nu, \nu$ prime of 184 bits
350	$2^{201} \cdot 3^{94} - 1$	50 392	345.2	252.0	$23 \cdot 2153 \cdot 2677 \cdot 2789 \cdot 265613 \cdot 294461 \cdot 398287 \cdot \nu, \nu$ prime of 252 bits
400	$2^{231} \cdot 3^{106} - 1$	84 890	396.7	308.8	$2 \cdot 5 \cdot 263 \cdot 283 \cdot 541 \cdot 1423 \cdot 13691 \cdot 41729 \cdot 891893 \cdot \nu, \nu$ prime of 309 bits
450	$2^{204} \cdot 3^{155} - 1$	68 535	446.6	353.6	$3 \cdot 11 \cdot 17 \cdot 9137 \cdot 82267 \cdot 93323 \cdot 357169 \cdot 752351 \cdot \nu, \nu$ prime of 354 bits
500	$2^{113} \cdot 3^{244} - 1$	96 064	495.2	390.3	$5^4 \cdot 7 \cdot 37 \cdot 157 \cdot 15373 \cdot 34403 \cdot 114493 \cdot 134293 \cdot 182857 \cdot \nu, \nu$ prime of 391 bits
550	$2^{293} \cdot 3^{162} - 1$	31 012	548.9	446.0	$2^2 \cdot 17 \cdot 6203 \cdot 20939 \cdot 50231 \cdot 63709 \cdot 502087 \cdot 622861 \cdot \nu, \nu$ prime of 447 bits
600	$5 \cdot 2^{299} \cdot 3^{188} - 1$	22 865	590.7	490.3	$3 \cdot 71 \cdot 83 \cdot 107 \cdot 139 \cdot 1327 \cdot 8663 \cdot 28349 \cdot 36137 \cdot 528779 \cdot \nu, \nu$ prime of 491 bits
650	$2^{404} \cdot 3^{155} - 1$	51 632	645.8	526.2	$2^6 \cdot 3 \cdot 31 \cdot 103 \cdot 107 \cdot 197 \cdot 223 \cdot 3529 \cdot 30091 \cdot 47713 \cdot 95731 \cdot 701419 \cdot \nu, \nu$ prime of 527 bits
700	$2^{83} \cdot 3^{389} - 1$	7 620	694.5	598.8	$11 \cdot 151 \cdot 379 \cdot 1657 \cdot 12043 \cdot 28351 \cdot 279607 \cdot 667559 \cdot \nu, \nu$ prime of 599 bits
750	$2^{477} \cdot 3^{172} - 1$	61 730	745.6	659.2	$2^2 \cdot 1861 \cdot 4057 \cdot 7937 \cdot 41467 \cdot 50363 \cdot 200689 \cdot \nu, \nu$ prime of 660 bits
800	$2^{107} \cdot 3^{437} - 1$	36 022	795.1	707.3	$5 \cdot 53 \cdot 73 \cdot 79 \cdot 137 \cdot 1657 \cdot 44017 \cdot 83071 \cdot 207293 \cdot \nu, \nu$ prime of 708 bits
850	$2^{166} \cdot 3^{431} - 1$	49 054	845.4	751.0	$2 \cdot 5^7 \cdot 13 \cdot 59^2 \cdot 5279 \cdot 42677 \cdot 50527 \cdot 337217 \cdot \nu, \nu$ prime of 751 bits
900	$2^{172} \cdot 3^{459} - 1$	44 512	895.2	801.5	$2^5 \cdot 227 \cdot 823 \cdot 1931 \cdot 4127 \cdot 18341 \cdot 62861 \cdot 277897 \cdot \nu, \nu$ prime of 802 bits
950	$2^{536} \cdot 3^{261} - 1$	35 055	943.3	854.3	$137 \cdot 1433 \cdot 93337 \cdot 163411 \cdot 306407 \cdot 662713 \cdot \nu, \nu$ prime of 855 bits
1000	$2^{721} \cdot 3^{176} - 1$	57 274	997.2	896.7	$11 \cdot 197 \cdot 2797 \cdot 7499 \cdot 19051 \cdot 24337 \cdot 102983 \cdot 822761 \cdot \nu, \nu$ prime of 897 bits

Table 3. The witness of least $P^*(N)$ found at each prime, over the 100 000 classes sampled for that prime. The *class* column is the index of the class realizing it.

rithm 3 as it stands essentially never returns a power-smooth splitting degree at cryptographic size. Constraining Simon’s algorithm so that it does is the first of the open problems in Section 6.

6 Conclusion and future directions

We have shown that two structural questions about principally polarized superspecial abelian surfaces — whether a surface admits an (N, N) -splitting, and whether it carries real multiplication by a prescribed order — reduce to primitive-representation problems for the quintic refined Humbert invariant, and that both can be answered from the polarization data alone, without Igusa invariants, defining equations for a genus 2 curve, or any explicit chain of isogenies. Section 3 turns this into three algorithms: a sampler for principal polarizations that reaches far beyond exhaustive enumeration, an enumeration procedure for the least splitting level k_0 , and a reduction of the unrestricted splitting problem to finding an isotropic vector of an indefinite rank-six form. Lemma 2 places k_0 precisely: it is the length of the shortest good-extension walk from the surface to the split surface, and an upper bound for the distance in the Richelot graph.

The experiments support this in two regimes. For $11 \leq p \leq 251$, where every principal polarization is known, the automorphism counts obtained from $r_4(q_C)$ reproduce the counts of Ibukiyama–Katsura–Oort exactly at the level of column totals (Table 2 and Appendix C), and the irreducible polarizations of $E \times E$ turn out to realize *every* class in the genus of q_5 that does not represent 1. For large parameters, Algorithm 3 produced witnesses for primes of up to 1000 bits; the resulting splitting degrees satisfy $\log_2 N \approx \log_2 p$, with a distribution whose shape is essentially unchanged across the range, so the detected (N, N) -isogeny has degree about p^2 throughout. Table 3 records the corresponding negative result: power-smooth witnesses occur up to 250 bits and, among the 100 000 classes sampled per prime, not beyond 300.

Two limitations should be stated plainly. First, our method detects a splitting without constructing it: a primitive representation certifies that an (N, N) -isogeny to a product exists and fixes its degree, but yields neither the isogeny nor the identity of the surfaces involved. Second, the experiments in the sampled regime inherit whatever distribution Algorithm 1 induces on isomorphism classes, which we have not characterized; conclusions drawn from those samples should be read with that in mind.

One direction is to impose arithmetic conditions on the splitting degree N arising from primitive representations $q_{(\mathcal{A}, \theta)}(x) = N^2$. For isogeny computation, the most relevant cases are $N = \ell^k$ and, more generally, B -power-smooth N . If $N = \prod_i \ell_i^{e_i}$, then N is B -power-smooth when $\ell_i^{e_i} \leq B$ for every i ; this is stronger than B -smoothness, which only requires $\ell_i \leq B$. Our computations already produce primitive representations with B -power-smooth N at moderate size: among the 100,000 classes sampled per prime, the smoothest witness has $\log_2 P^*(N)$ between 7.5 and 35.5 for primes up to 250 bits, but from 300 bits upward none below 184 bits was found (Table 3). A natural problem is therefore to modify the randomized choices, reductions, and restarts in Simon’s algorithm [96, 101] so as to produce primitive solutions $q_{(\mathcal{A}, \theta)}(v) = N^2$ with N constrained to be an ℓ -power or B -power-smooth. This amounts to obtaining effective bounds for the smallest such N , together with an efficient algorithm for finding the corresponding primitive representation.

A second direction is to investigate whether the splittings via refined Humbert invariant can be used to improve and accelerate KLPT^2 , in the same spirit as the application of conversion of module representations by Page–Robert–Soumier [85]. Their approach passes from the Hermitian module representation to the underlying rank-8 integral quadratic lattice, where suitable primitive vectors are used to construct principal rank-1 submodules and corresponding splitting isogenies; as an application, this leads to an improved output-degree bound for KLPT^2 . Starting from the same IKO representation, the principal polarization determines the quintic refined

Humbert invariant $q_{(\mathcal{A},\theta)}$. A primitive representation $q_{(\mathcal{A},\theta)}(x) = N^2$ determines a splitting degree N , so the search for suitable values of N can instead be formulated directly as a primitive representation problem of N^2 by $q_{(\mathcal{A},\theta)}$. This separates the determination of the splitting degree from the explicit construction of the corresponding isogeny. It remains to determine whether the (N, N) -splitting detected by a primitive representation of $q_{\mathcal{C}}$ can also be constructed effectively at the level of explicit isogenies, and whether this approach can be used to obtain a comparable improvement of KLPT².

Acknowledgements: The authors used Claude (Anthropic) and ChatGPT (OpenAI) exclusively for text proofreading and minor code debugging. All mathematical formulations, proofs, and algorithmic contributions were developed independently by the authors.

References

1. Aikawa, Y., Tanaka, R., Yamauchi, T.: Isogeny graphs on superspecial abelian varieties: eigenvalues and connection to Bruhat–Tits buildings. *Canadian Journal of Mathematics* **76**(6), 1891–1916 (2024). <https://doi.org/10.4153/S0008414X23000676>
2. Bolza, O.: Zur Reduction hyperelliptischer Integrale erster Ordnung auf elliptische mittels einer Transformation dritten Grades. *Math. Ann.* **50**(2-3), 314–324 (1898). <https://doi.org/10.1007/BF01448072>
3. Briochi, F.: Sur la réduction de l’intégrale hyperelliptique à l’elliptique par une transformation du troisième degré. *Ann. Sci. École Norm. Sup. (3)* **8**, 227–230 (1891). <https://doi.org/10.24033/asens.357>
4. Castryck, W., Decru, T.: Multiradical isogenies. In: *Arithmetic, Geometry, Cryptography, and Coding Theory 2021, Contemporary Mathematics*, vol. 779, pp. 57–89. American Mathematical Society (2022). <https://doi.org/10.1090/conm/779/15671>
5. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: *Advances in Cryptology – EUROCRYPT 2023*. Springer Nature Switzerland (2023). https://doi.org/10.1007/978-3-031-30589-4_15
6. Castryck, W., Decru, T., Kutas, P., Laval, A., Petit, C., Ti, Y.B.: KLPT²: Algebraic pathfinding in dimension two and applications. In: *Advances in Cryptology – CRYPTO 2025: 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17–21, 2025, Proceedings, Part I. Lecture Notes in Computer Science*, vol. 16000, pp. 167–200. Springer, Cham (2025). https://doi.org/10.1007/978-3-032-01855-7_6
7. Castryck, W., Decru, T., Smith, B.: 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. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. In: *Advances in Cryptology – ASIACRYPT 2018. Lecture Notes in Computer Science*, vol. 11274, pp. 395–427. Springer (2018). https://doi.org/10.1007/978-3-030-03332-3_15
9. Charles, D.X., Goren, E.Z., Lauter, K.E.: Cryptographic hash functions from expander graphs. *Journal of Cryptology* **22**(1), 93–113 (2009). <https://doi.org/10.1007/s00145-007-9002-x>
10. Charles, D.X., Goren, E.Z., Lauter, K.E.: Families of Ramanujan graphs and quaternion algebras. In: Harnad, J., Winternitz, P. (eds.) *Groups and Symmetries: From Neolithic Scots to John McKay*, CRM Proceedings & Lecture Notes, vol. 47, pp. 53–80. American Mathematical Society, Providence, RI (2009). <https://doi.org/10.1090/crmp/047/05>
11. Chung, F.R.K., Faber, V., Manteuffel, T.A.: An upper bound on the diameter of a graph from eigenvalues associated with its Laplacian. *SIAM Journal on Discrete Mathematics* **7**(3), 443–457 (1994). <https://doi.org/10.1137/S0895480191217776>
12. Corte-Real Santos, M., Costello, C., Frengley, S.: An algorithm for efficient detection of (N, N) -splittings and its application to the isogeny problem in dimension 2. In: Tang, Q., Teague, V. (eds.) *Public-Key Cryptography – PKC 2024: 27th IACR International Conference on Practice and*

- Theory of Public-Key Cryptography, Proceedings. Lecture Notes in Computer Science, vol. 14603, pp. 157–189. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-57725-3_6
13. Corte-Real Santos, M., Costello, C., Frengley, S.: Efficient algorithms for the detection of (n, n) -splittings and endomorphisms. *Journal of Cryptology* **39**(1) (2026). <https://doi.org/10.1007/s00145-025-09552-7>
 14. Costello, C., Smith, B.: The supersingular isogeny problem in genus 2 and beyond. In: Ding, J., Tillich, J.P. (eds.) *Post-Quantum Cryptography – PQCrypto 2020*. pp. 151–168. Lecture Notes in Computer Science, Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-44223-1_9
 15. Couveignes, J.M.: Hard homogeneous spaces. *Cryptology ePrint Archive*, Paper 2006/291 (2006), <https://eprint.iacr.org/2006/291>
 16. De Feo, L., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology* **8**(3), 209–247 (2014). <https://doi.org/10.1515/jmc-2012-0015>
 17. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: compact post-quantum signatures from quaternions and isogenies. In: *Advances in Cryptology – ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security* (2020). https://doi.org/10.1007/978-3-030-64837-4_3
 18. Decker, W., Eder, C., Fieker, C., Horn, M., Joswig, M. (eds.): *The Computer Algebra System OSCAR: Algorithms and Examples, Algorithms and Computation in Mathematics*, vol. 32. Springer, 1 edn. (2025), <https://link.springer.com/book/9783031621260>
 19. Decru, T., Reijnders, K.: Expander properties of superspecial isogeny digraphs with level structure. In: Heninger, N., Rosulek, M. (eds.) *Advances in Cryptology – CRYPTO 2026*. pp. 478–505. Lecture Notes in Computer Science, Springer, Cham (2026). https://doi.org/10.1007/978-3-032-35398-6_16, *Cryptology ePrint Archive*, Paper 2026/500
 20. Delfs, C., Galbraith, S.D.: Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography* **78**(2), 425–440 (2016). <https://doi.org/10.1007/s10623-014-0010-1>
 21. Eichler, M.: Die Ähnlichkeitsklassen indefiniter Gitter. *Mathematische Zeitschrift* **55**, 216–252 (1952). <https://doi.org/10.1007/BF01268656>
 22. Einsiedler, M., Lindenstrauss, E., Mohammadi, A., Wieser, A.: Effective equidistribution of semisimple adelic periods and representations of quadratic forms. *arXiv:2503.21068* (2025), <https://arxiv.org/abs/2503.21068>
 23. Eisenträger, K., Hallgren, S., Lauter, K., Morrison, T., Petit, C.: Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In: *Advances in cryptology—EUROCRYPT 2018*. Part III, Lecture Notes in Comput. Sci., vol. 10822, pp. 329–368. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78372-7_11
 24. Ellenberg, J.S., Venkatesh, A.: Local-global principles for representations of quadratic forms. *Inventiones Mathematicae* **171**(2), 257–279 (2008). <https://doi.org/10.1007/s00222-007-0077-7>
 25. Fieker, C., Hart, W., Hofmann, T., Johansson, F.: Nemo/Hecke: Computer Algebra and Number Theory Packages for the Julia Programming Language. In: *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*. pp. 157–164. ISSAC ’17 (2017). <https://doi.org/10.1145/3087604.3087611>
 26. Fincke, U., Pohst, M.E.: Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of Computation* **44**(170), 463–471 (1985). <https://doi.org/10.1090/S0025-5718-1985-0777278-8>
 27. Florit, E., Smith, B.: An atlas of the Richelot isogeny graph. In: *Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties*, RIMS Kôkyûroku Bessatsu, vol. B90, pp. 195–219. Research Institute for Mathematical Sciences (RIMS), Kyoto University (2022), <http://hdl.handle.net/2433/276282>
 28. Florit, E., Smith, B.: Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph. In: *Arithmetic, Geometry, Cryptography, and Coding Theory, Contemporary Mathematics*, vol. 779, pp. 103–132. American Mathematical Society (2022). <https://doi.org/10.1090/conm/779/15672>

29. Flynn, E.V., Ti, Y.B.: Genus two isogeny cryptography. In: Post-Quantum Cryptography. pp. 286–306. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-25510-7_16
30. Goren, E.Z., Love, J.R.: Supersingular elliptic curves, quaternion algebras and applications to cryptography. In: Abelian Surfaces and Isogeny-Based Cryptography, pp. 123–200. NATO Science for Peace and Security Series - D: Information and Communication Security, IOS Press (2025). <https://doi.org/10.3233/NICSP250005>
31. Goursat, E.: Sur la réduction des intégrales hyperelliptiques. *Bull. Soc. Math. France* **13**, 143–162 (1885). <https://doi.org/10.24033/bsmf.300>
32. Hartshorne, R.: Algebraic Geometry. Springer, New York (2013). <https://doi.org/10.1007/978-1-4757-3849-0>
33. Hayashida, T., Nishi, M.: Existence of curves of genus two on a product of two elliptic curves. *Journal of the Mathematical Society of Japan* **17**, 1–16 (1965). <https://doi.org/10.2969/jmsj/01710001>
34. Hsia, J.S., Kitaoka, Y., Kneser, M.: Representations of positive definite quadratic forms. *Journal für die reine und angewandte Mathematik* **301**, 132–141 (1978). <https://doi.org/10.1515/crll.1978.301.132>
35. Humbert, G.: Sur les fonctions abéliennes singulières. Premier Mémoire. *Journal de Mathématiques Pures et Appliquées* (5) **5**, 233–350 (1899), http://www.numdam.org/item/JMPA_1899_5_5_233_0/
36. Ibukiyama, T., Katsura, T., Oort, F.: Supersingular curves of genus two and class numbers. *Compositio Mathematica* **57**, 127–152 (1986), http://www.numdam.org/item/CM_1986__57_2_127_0/
37. Igusa, J.I.: Arithmetic variety of moduli for genus two. *Ann. of Math.* (2) **72**, 612–649 (1960). <https://doi.org/10.2307/1970233>
38. Iwaniec, H.: Topics in Classical Automorphic Forms, Graduate Studies in Mathematics, vol. 17. American Mathematical Society, Providence, RI (1997). <https://doi.org/10.1090/gsm/017>
39. Jacobi, C.G.J.: Review of Legendre’s ‘Traité des fonctions elliptiques, troisième supplément’. *Journal für die reine und angewandte Mathematik* **8**, 413–417 (1832). <https://doi.org/10.1515/crll.1832.8.413>
40. Jao, D., Azarderakhsh, R., Campagna, M., Costello, C., De Feo, L., Hess, B., Hutchinson, A., Jalali, A., Karabina, K., Koziel, B., LaMacchia, B., Longa, P., Naehrig, M., Pereira, G., Renes, J., Soukharev, V., Urbanik, D.: Supersingular isogeny key encapsulation (2022), <https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/SIKE-spec.pdf>
41. Jöchner, M., Kitaoka, Y.: Representations of positive definite quadratic forms with congruence and primitive conditions. *Journal of Number Theory* **48**(1), 88–101 (1994). <https://doi.org/10.1006/jnth.1994.1055>
42. Jordan, B.W.: Isogeny graphs of superspecial abelian varieties. In: Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties, RIMS Kôkyûroku Bessatsu, vol. B90, pp. 131–144. Research Institute for Mathematical Sciences (RIMS), Kyoto University (2022), <http://hdl.handle.net/2433/276277>
43. Jordan, B.W., Zaytman, Y.: Isogeny graphs of superspecial abelian varieties and Brandt matrices. *Journal of the Mathematical Society of Japan* (2026). <https://doi.org/10.2969/jmsj/91629162>, advance publication
44. Kani, E.: Elliptic curves on abelian surfaces. *Manuscripta Mathematica* **84**, 199–223 (1994). <https://doi.org/10.1007/BF02567454>
45. Kani, E.: The existence of curves of genus two with elliptic differentials. *Journal of Number Theory* **64**(1), 130–161 (1997). <https://doi.org/10.1006/jnth.1997.2105>, <https://www.sciencedirect.com/science/article/pii/S0022314X97921053>
46. Kani, E.: The number of curves of genus two with elliptic differentials. *Journal für die reine und angewandte Mathematik* **485**, 93–122 (1997). <https://doi.org/10.1515/crll.1997.485.93>
47. Kani, E.: Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms. *Journal of Number Theory* **139**, 138–174 (2014). <https://doi.org/10.1016/j.jnt.2013.12.006>
48. Kani, E.: The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. *Collect. Math.* **67**, 21–54 (2016). <https://doi.org/10.1007/s13348-015-0148-9>

49. Kani, E.: Elliptic subcovers of a curve of genus 2. II. The refined Humbert invariant. *Journal of Number Theory* **193**, 302–335 (2018). <https://doi.org/10.1016/j.jnt.2018.05.011>
50. Kani, E.: Elliptic subcovers of a curve of genus 2. I. The isogeny defect. *Annales mathématiques du Québec* **43**, 281–303 (2019). <https://doi.org/10.1007/s40316-018-0105-6>
51. Kani, E.: Generalized Humbert schemes and intersections of Humbert surfaces. Preprint (2019), <https://web.archive.org/web/20240312201114/https://mast.queensu.ca/~kani/papers/interHum11.pdf>, 35 pages
52. Kani, E.: Subcovers of curves and moduli spaces. *Contemporary Mathematics* **766**, 229–250 (2021). <https://doi.org/10.1090/conm/766/15384>, <https://web.archive.org/web/20250115230609/https://mast.queensu.ca/~kani/papers/SubcoversModuli2.pdf>
53. Kani, E.: Curves of genus 2 on abelian surfaces. Preprint, 37 pages (2023), <https://web.archive.org/web/20260827210959/https://mast.queensu.ca/~kani/papers/CurvesAS2.pdf>
54. Kani, E.: The refined Humbert invariant for abelian product surfaces with complex multiplication. Preprint, 24 pages (2025), <https://web.archive.org/web/20260827210959/https://mast.queensu.ca/~kani/papers/refHum5.pdf>
55. Kannan, R.: Improved algorithms for integer programming and related lattice problems. In: *Proceedings of the fifteenth annual ACM symposium on Theory of computing - STOC '83*. p. 193–206. ACM Press, New York, NY, USA (1983). <https://doi.org/10.1145/800061.808749>
56. Katsura, T., Oort, F.: Supersingular abelian varieties of dimension two or three and class numbers. In: *Algebraic Geometry, Sendai, 1985*, *Adv. Stud. Pure Math.*, vol. 10, pp. 253–281. North-Holland, Amsterdam (1987)
57. Katsura, T., Takashima, K.: Counting Richelot isogenies between superspecial abelian surfaces. In: Galbraith, S.D. (ed.) *Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS XIV)*, *The Open Book Series*, vol. 4, pp. 283–300. Mathematical Sciences Publishers, Berkeley, CA (2020). <https://doi.org/10.2140/obs.2020.4.283>
58. Kir, H.: *Curves of Genus 2 and Quadratic Forms*. Ph.D. thesis, Queen’s University at Kingston, Ontario, Canada (2024), <https://qspace.library.queensu.ca/items/119efd2b-59b4-4e19-9ff0-9eea3914560e>
59. Kir, H.: The refined Humbert invariant for an automorphism group of a genus 2 curve. In: *Arithmetic, Geometry, Cryptography and Coding Theory*, *Contemporary Mathematics*, vol. 832, pp. 89–126. American Mathematical Society, Providence, RI (2026). <https://doi.org/10.1090/conm/832/16608>, <https://www.ams.org/books/conm/832/>
60. Kırımlı, E., Korpál, G.: Refined Humbert invariants in supersingular isogeny degree analysis. *Cryptology ePrint Archive*, Paper 2025/1605 (2025), <https://eprint.iacr.org/2025/1605>
61. Kırımlı, E., Martindale, C.: The computational refined Humbert invariant problem is equivalent to the computational isogeny problem. *Cryptology ePrint Archive*, Paper 2025/1295 (2025), <https://eprint.iacr.org/2025/1295>
62. Kitaoka, Y.: Some remarks on representations of positive definite quadratic forms. *Nagoya Mathematical Journal* **115**, 23–41 (1989). <https://doi.org/10.1017/S0027763000001501>
63. Kitaoka, Y.: *Arithmetic of quadratic forms*, *Cambridge Tracts in Mathematics*, vol. 106. Cambridge University Press, Cambridge (1993). <https://doi.org/10.1017/CB09780511666155>
64. Kitaoka, Y.: The minimum and the primitive representation of positive definite quadratic forms. *Nagoya Mathematical Journal* **133**, 127–153 (1994). <https://doi.org/10.1017/S0027763000004773>
65. Kitaoka, Y.: The minimum and the primitive representation of positive definite quadratic forms II. *Nagoya Mathematical Journal* **141**, 1–27 (1996). <https://doi.org/10.1017/S002776300000550X>
66. Kohel, D.: *Endomorphism Rings of Elliptic Curves Over Finite Fields*. Ph.D. thesis, University of California, Berkeley (1996), <https://www.i2m.univ-amu.fr/perso/david.kohel/pub/thesis.pdf>
67. Kohel, D., Lauter, K., Petit, C., Tignol, J.P.: On the quaternion ℓ -isogeny path problem. *LMS Journal of Computation and Mathematics* **17**, 418–432 (2014). <https://doi.org/10.1112/S1461157014000151>
68. Krazer, A.: *Lehrbuch der Thetafunktionen*. Chelsea Reprint (1970), <https://archive.org/details/lehrbuchderthet00krazgoog>, original edition: B. G. Teubner, Leipzig, 1903

69. Kuhn, R.M.: Curves of genus 2 with split Jacobian. *Trans. Amer. Math. Soc.* **307**(1), 41–49 (1988). <https://doi.org/10.2307/2000749>
70. Kunzweiler, S., Shen, M.Y.: Endomorphisms via splittings. In: Bardet, M., Niederhagen, R. (eds.) *Post-Quantum Cryptography – PQCrypto 2026, Part II. Lecture Notes in Computer Science*, vol. 16492, pp. 3–38. Springer, Cham (2026). https://doi.org/10.1007/978-3-032-22698-3_1, Cryptology ePrint Archive, Paper 2026/215
71. Kutas, P., Shen, M.Y.: Splittings and endomorphism rings. *Cryptology ePrint Archive*, Paper 2026/1198 (2026), <https://eprint.iacr.org/2026/1198>
72. Lange, H.: Über die Modulvarietät der Kurven vom Geschlecht 2. *Journal für die reine und angewandte Mathematik* **281**, 80–96 (1976). <https://doi.org/10.1515/crll.1976.281.80>
73. Lange, H.: Kurven mit rationaler Abbildung. *Journal für die reine und angewandte Mathematik* **295**, 80–115 (1977). <https://doi.org/10.1515/crll.1977.295.80>
74. Li, K.Z., Oort, F.: *Moduli of Supersingular Abelian Varieties*, *Lecture Notes in Mathematics*, vol. 1680. Springer, Berlin (1998). <https://doi.org/10.1007/BFb0095931>
75. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: *Advances in Cryptology – EUROCRYPT 2023*. Springer Nature Switzerland (2023). https://doi.org/10.1007/978-3-031-30589-4_16
76. Mestre, J.F.: La méthode des graphes. exemples et applications. In: *Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields*, June 24–28, 1986, Katata, Japan, pp. 217–242. Department of Mathematics, Nagoya University, Nagoya, Japan (1986), <https://wstein.org/msri06/refs/mestre-method-of-graphs/mestre-fr.pdf>
77. Milne, J.: Abelian varieties. In: Cornell, G., Silverman, J. (eds.) *Arithmetic Geometry*, pp. 103–150. Springer (1986). https://doi.org/10.1007/978-1-4613-8655-1_5
78. Mumford, D.: *Abelian Varieties*, *Tata Institute of Fundamental Research Studies in Mathematics*, vol. 5. Oxford University Press, London (1970)
79. Murabayashi, N.: The moduli space of curves of genus two covering elliptic curves. *Manuscripta Mathematica* **84**(2), 125–133 (1994). <https://doi.org/10.1007/BF02567449>
80. Nicole, M.H.: *Superspecial Abelian Varieties, Theta Series and the Jacquet–Langlands Correspondence*. Ph.D. thesis, McGill University, Montréal, Québec, Canada (2005), <https://mcgill.scholaris.ca/items/8b0a9b24-4d90-408f-8709-deb29c6034c0>
81. Nitaj, A.: L’algorithme de Cornacchia. *Expositiones Mathematicae* **13**(4), 358–365 (1995), <https://nitaj.users.lmno.cnrs.fr/cornacchia.ps>
82. Ogus, A.: Supersingular $K3$ crystals. In: *Journées de Géométrie Algébrique de Rennes* (Rennes, 1978), Vol. II, *Astérisque*, vol. 64, pp. 3–86. Soc. Math. France, Paris (1979), http://www.numdam.org/item/AST_1979__64__3_0/
83. Oh, H.: Uniform pointwise bounds for matrix coefficients of unitary representations and applications to Kazhdan constants. *Duke Mathematical Journal* **113**(1), 133–192 (2002). <https://doi.org/10.1215/S0012-7094-02-11314-3>
84. Oort, F.: Subvarieties of moduli spaces. *Inventiones Mathematicae* **24**, 95–119 (1974). <https://doi.org/10.1007/BF01404301>
85. Page, A., Robert, D., Soumier, J.: On the conversion of module representations for higher dimensional supersingular isogenies. In: Heninger, N., Rosulek, M. (eds.) *Advances in Cryptology – CRYPTO 2026*. pp. 415–446. *Lecture Notes in Computer Science*, Springer, Cham (2026). https://doi.org/10.1007/978-3-032-35398-6_14, *Cryptology ePrint Archive*, Paper 2026/276
86. Page, A., Wesolowski, B.: The supersingular endomorphism ring and one endomorphism problems are equivalent. In: Joye, M., Leander, G. (eds.) *Advances in Cryptology – EUROCRYPT 2024, Part VI. Lecture Notes in Computer Science*, vol. 14656, pp. 388–417. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-58751-1_14, *Cryptology ePrint Archive*, Paper 2023/1399
87. Pizer, A.K.: Ramanujan graphs. In: Buell, D.A., Teitelbaum, J.T. (eds.) *Computational Perspectives on Number Theory* (Chicago, IL, 1995), *AMS/IP Studies in Advanced Mathematics*, vol. 7, pp. 159–178. American Mathematical Society, Providence, RI (1998). <https://doi.org/10.1090/amsip/007/08>, a co-publication of the AMS and International Press
88. Robert, D.: Breaking SIDH in polynomial time. In: *Advances in Cryptology – EUROCRYPT 2023*. pp. 472–503. Springer Nature Switzerland (2023). https://doi.org/10.1007/978-3-031-30589-4_17

89. Rostovtsev, A., Stolbunov, A.: Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Paper 2006/145 (2006), <https://eprint.iacr.org/2006/145>
90. Schnorr, C.P., Euchner, M.: Lattice basis reduction: improved practical algorithms and solving subset sum problems. Math. Programming **66**(2), 181–199 (1994). <https://doi.org/10.1007/BF01581144>
91. Serge Lang: Abelian varieties. Springer-Verlag New York (1983)
92. Serre, J.P.: A course in arithmetic, Graduate Texts in Mathematics, vol. No. 7. Springer-Verlag, New York-Heidelberg (1973). <https://doi.org/10.1007/978-1-4684-9884-4>, translated from the French
93. Serre, J.P.: Groupes algébriques et corps de classes, Actualités Scientifiques et Industrielles, vol. 1264. Hermann, Paris, 2 edn. (1997). <https://doi.org/10.3917/herm.serre.1997.02>, First edition 1959
94. Shaska, T., Völklein, H.: Elliptic subfields and automorphisms of genus 2 function fields. In: Algebra, arithmetic and geometry with applications, pp. 703–723. Springer (2004). https://doi.org/10.1007/978-3-642-18487-1_42
95. Shioda, T.: Supersingular K3 surfaces. In: Algebraic Geometry. Lecture Notes in Math., vol. 732, pp. 564–591. Springer Berlin (1979). <https://doi.org/10.1007/BFb0066664>
96. Simon, D.: Solving quadratic equations using reduced unimodular quadratic forms. Mathematics of Computation **74**(251), 1531–1543 (2005). <https://doi.org/10.1090/S0025-5718-05-01729-1>
97. Simon, D.: Quadratic equations in dimensions 4, 5 and more (2006), <https://simond.users.lmno.cnrs.fr/maths/Dim4.pdf>, preprint
98. Takashima, K.: Efficient Algorithms for Isogeny Sequences and Their Cryptographic Applications, pp. 97–114. Springer Singapore, Singapore (2018). https://doi.org/10.1007/978-981-10-5065-7_6
99. The OSCAR Team: OSCAR – Open Source Computer Algebra Research system, Version 1.2.2 (2024), <https://www.oscar-system.org>
100. Voight, J.: Quaternion algebras, Graduate Texts in Mathematics, vol. 288. Springer Cham (2021). <https://doi.org/10.1007/978-3-030-56694-4>
101. Watkins, M.: Some comments about indefinite LLL. In: Diophantine methods, lattices, and arithmetic theory of quadratic forms, Contemp. Math., vol. 587, pp. 233–243. Amer. Math. Soc., Providence, RI (2013). <https://doi.org/10.1090/comm/587/11674>
102. Weil, A.: Zum Beweis des Torellischen Satzes. Nachrichten der Akademie der Wissenschaften in Göttingen, Math.-Phys. Klasse IIa **1957**, 32–53 (1957)
103. Wesolowski, B.: The supersingular isogeny path and endomorphism ring problems are equivalent. In: 2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS). pp. 1100–1111. IEEE (2021). <https://doi.org/10.1109/FOCS52979.2021.00109>
104. Zaytman, Y.: Proving connectedness of isogeny graphs with strong approximation. In: Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties, RIMS Kôkyûroku Bessatsu, vol. B90, pp. 145–151. Research Institute for Mathematical Sciences (RIMS), Kyoto University (2022), <http://hdl.handle.net/2433/276278>

A Refined Humbert invariants

In this section, we introduce the refined Humbert invariants defined by Kani [44,48]. The refined Humbert invariant $q_{(\mathcal{A},\theta)}$ is the main tool of this paper. These invariants are very useful for the interplay between geometric and arithmetic problems. This section mainly follows Kani [47,48].

We first present some essential facts about the Néron-Severi groups of abelian varieties by following [48, Section 11].

Definition 2. *Let $\mathcal{A}$ be an abelian variety over a field K . The Néron-Severi group of $\mathcal{A}$ is defined as the quotient group $\text{NS}(\mathcal{A}) = \text{Pic}(\mathcal{A}) / \text{Pic}^0(\mathcal{A})$, which is a free $\mathbb{Z}$ -module of finite rank.*

Definition 3. [32, p.357] Let $\mathcal{A}$ be an abelian surface over a field K and let $\text{Div}(\mathcal{A})$ be the set of divisors on $\mathcal{A}$. For two divisors $D_1, D_2 \in \text{Div}(\mathcal{A})$, we say that D_1 is numerically equivalent to D_2 , denoted by $D_1 \equiv D_2$, if $(D_1 \cdot D) = (D_2 \cdot D)$ for all $D \in \text{Div}(\mathcal{A})$, where $(\cdot)$ denotes the intersection number.

Definition 4. Let $\mathcal{A}/K$ be an abelian surface. We define the set of principal polarizations of $\mathcal{A}$ as

$$\mathcal{P}(\mathcal{A}) = \{\text{cl}(D) \in \text{NS}(\mathcal{A}) : D \in \text{Div}(\mathcal{A}) \text{ is ample and } (D \cdot D) = 2\}.$$

For a divisor $D \in \text{Div}(\mathcal{A})$, we write $\text{cl}(D)$ for its class in $\text{NS}(\mathcal{A})$ and $\phi_D : \mathcal{A} \rightarrow \hat{\mathcal{A}}$ for the homomorphism associated to D . When $\text{cl}(D) \in \mathcal{P}(\mathcal{A})$, the map ϕ_D is an isomorphism. Throughout, we use the same symbol θ for a principal polarization class in $\text{NS}(\mathcal{A})$ and for the corresponding isomorphism $\theta : \mathcal{A} \xrightarrow{\sim} \hat{\mathcal{A}}$ when no confusion can arise.

If $\mathcal{A}$ has a principal polarization $\theta : \mathcal{A} \xrightarrow{\sim} \hat{\mathcal{A}}$ then $\text{NS}(\mathcal{A})$ can be interpreted as a subgroup of $\text{End}(\mathcal{A})$ [77, p. 126]. Moreover, if r_θ denotes the Rosati involution on $\text{End}(\mathcal{A})$, defined by $r_\theta(\mu) = \theta^{-1} \hat{\mu} \theta$, then by [78, p. 189, 190], the map $D \mapsto \theta^{-1} \phi_D$ defines an isomorphism

$$\Phi_\theta : \text{NS}(\mathcal{A}) \xrightarrow{\sim} \text{End}_\theta(\mathcal{A}) := \{\mu \in \text{End}(\mathcal{A}) : r_\theta(\mu) = \mu\}. \quad (6)$$

The intersection number $(D_1 \cdot D_2)$ of divisors D_1, D_2 on $\mathcal{A}$ defines an integral quadratic form as follows.

Definition 5. The intersection product $(D_1 \cdot D_2)$ of divisors D_1, D_2 on an abelian surface $\mathcal{A}$ defines an integral quadratic form $q_{\mathcal{A}}$ on $\text{NS}(\mathcal{A})$, called intersection form: $q_{\mathcal{A}}(D) = \frac{1}{2}(D \cdot D)$ for all $D \in \text{NS}(\mathcal{A})$.

Since $\text{NS}(\mathcal{A}) \cong \mathbb{Z}^\rho$ where $\rho = \rho(\mathcal{A})$ is the Picard number of $\mathcal{A}$, $q_{\mathcal{A}}$ is equivalent to an integral quadratic form q in ρ variables, therefore it leads to an isomorphism $(\text{NS}(\mathcal{A}), q_{\mathcal{A}}) \cong (\mathbb{Z}^\rho, q)$ of quadratic modules.

Definition 6. Let $\mathcal{A}/K$ be an abelian surface and let $\theta \in \mathcal{P}(\mathcal{A})$ be a principal polarization of $\mathcal{A}$. We define the polarized Néron-Severi group of $(\mathcal{A}, \theta)$ to be $\text{NS}(\mathcal{A}, \theta) := \text{NS}(\mathcal{A})/\mathbb{Z}\theta$.

If $\mathcal{A}$ has a principal polarization $\theta \in \mathcal{P}(\mathcal{A})$, then the quadratic form $\tilde{q}_{(\mathcal{A}, \theta)}$ on $\text{NS}(\mathcal{A})$ is defined by

$$\tilde{q}_{(\mathcal{A}, \theta)}(D) = (D \cdot \theta)^2 - 2(D \cdot D), \text{ for } D \in \text{NS}(\mathcal{A}). \quad (7)$$

It follows that $\tilde{q}_{(\mathcal{A}, \theta)}(D + n\theta) = \tilde{q}_{(\mathcal{A}, \theta)}(D)$ for all $n \in \mathbb{Z}$, therefore $\tilde{q}_{(\mathcal{A}, \theta)}$ actually gives a quadratic form $q_{(\mathcal{A}, \theta)}$ on the quotient module $\text{NS}(\mathcal{A}, \theta)$. Then, $q_{(\mathcal{A}, \theta)}$ is a positive definite form on $\text{NS}(\mathcal{A}, \theta) \cong \mathbb{Z}^{\rho-1}$ [44].

This is the refined Humbert invariant $q_{(\mathcal{A}, \theta)}$ of Definition 1.

For an integral quadratic form q on a lattice L , we say that q represents an integer n if $q(x) = n$ for some $x \in L$, and that q primitively represents n if such a vector x can be chosen primitive. We write $q \equiv 0, 1 \pmod{4}$ to mean that $q(x) \equiv 0$ or $1 \pmod{4}$ for every $x \in L$.

A necessary condition For a generic principally polarized abelian surface $(\mathcal{A}, \theta)$, any integral quadratic form arising as a refined Humbert invariant necessarily satisfies the following condition.

Theorem 6. If there exists $(\mathcal{A}, \theta)/K$ such that a given integral quadratic form q is equivalent to a refined Humbert invariant $q_{(\mathcal{A}, \theta)}$, then $q \equiv 0, 1 \pmod{4}$.

Proof. See [54, Theorem 1]. This result appeared in [58, Theorem 3.1.1] □

An equivalent definition: Kani generalized and extended the definition of a refined Humbert invariant in [50, Remark 16] later. By the isomorphism Φ_θ 6 above, the polarization class θ corresponds to the identity endomorphism $1_{\mathcal{A}}$. Hence Φ_θ induces an isomorphism $\text{NS}(\mathcal{A}, \theta) = \text{NS}(\mathcal{A})/\mathbb{Z}\theta \xrightarrow{\sim} \text{End}_\theta(\mathcal{A})/\mathbb{Z}1_{\mathcal{A}}$. Through this identification, we use the same notation $q_{(\mathcal{A}, \theta)}$ for the corresponding quadratic form on $\text{End}_\theta(\mathcal{A})/\mathbb{Z}1_{\mathcal{A}}$, and write $q_{(\mathcal{A}, \theta)}(\mu)$ for the value on the class of μ .

Proposition 2. *Let $(\mathcal{A}, \theta)$ be a principally polarized abelian surface over a field K and let $q_{(\mathcal{A}, \theta)}$ be a refined Humbert invariant of $(\mathcal{A}, \theta)$. Then for every $\mu \in \text{End}_\theta(\mathcal{A})$, we obtain*

$$q_{(\mathcal{A}, \theta)}(\mu) = \text{tr}(\mu^2) - \frac{1}{4}(\text{tr}(\mu))^2$$

where tr is the (rational) trace of an endomorphism as defined in [78, p.182].

Irreducibility criterion We first recall the distinction between reducible and irreducible polarizations on an abelian surface.

Definition 7. [102, Satz 2] *A polarization $\theta \in \mathcal{P}(\mathcal{A})$ is called reducible (or decomposable) if $\theta = \text{cl}(E_1 + E_2)$ for some elliptic curves E_1 and E_2 on $\mathcal{A}$.*

The refined Humbert invariant provides a convenient way to detect the geometric type of principally polarized abelian surface, whether it is a Jacobian surface $(\mathcal{J}(\mathcal{C}), \theta_{\mathcal{C}})$ or a split surface $(E_1 \times E_2, \theta_{E_1, E_2})$.

Proposition 3. [48, Proposition 6] *Let $q_{(\mathcal{A}, \theta)}$ be the refined Humbert invariant of the principally polarized abelian surface $(\mathcal{A}, \theta)$, then we have that*

$$\theta \text{ is irreducible if and only if } q_{(\mathcal{A}, \theta)} \text{ does not represent } 1. \quad (8)$$

If $\mathcal{C}$ is a curve of genus 2, its Jacobian $\mathcal{J}(\mathcal{C})$ has the canonical principal polarization $\theta_{\mathcal{C}} \in \text{NS}(\mathcal{J}(\mathcal{C}))$. In this case, we simply denote its refined Humbert invariant by $q_{\mathcal{C}} := q_{(\mathcal{J}(\mathcal{C}), \theta_{\mathcal{C}})}$.

Definition 8. *The degree map is defined as a positive definite integral quadratic form (up to equivalence) denoted by q_{E_1, E_2} such that $q_{E_1, E_2}(\varphi) = \deg(\varphi)$ for any $\varphi \in \text{Hom}(E_1, E_2)$.*

The quadratic form q_{E_1, E_2} is intrinsic on $\text{Hom}(E_1, E_2)$; the phrase “up to equivalence” refers to its expression after choosing a $\mathbb{Z}$ -basis. For later use, let β_d denote its associated bilinear form,

$$\beta_d(\varphi, \varphi') = q_{E_1, E_2}(\varphi + \varphi') - q_{E_1, E_2}(\varphi) - q_{E_1, E_2}(\varphi').$$

Now we focus on the case of products of two elliptic curves. Let $\mathcal{A} = E_1 \times E_2$ and let $p_i : \mathcal{A} \rightarrow E_i$ be the natural projections. We write $\theta_i = p_i^*(0_{E_i})$ for $i = 1, 2$.

Theorem 7. [48, Proposition 23] *Let $\mathcal{A} = E_1 \times E_2$ be a product surface. We have a group isomorphism*

$$\mathcal{D} = \mathcal{D}_{E_1, E_2} : \mathbb{Z} \oplus \mathbb{Z} \oplus \text{Hom}(E_1, E_2) \longrightarrow \text{NS}(\mathcal{A}) \quad (9)$$

$$\mathcal{D}(a, b, \varphi) = (a - \deg(\varphi))\theta_1 + (b - 1)\theta_2 + \Gamma_{-\varphi} \quad (10)$$

where $\theta_i = p_i^*(0_{E_i})$, and $\Gamma_{-\varphi}$ is the graph of $-\varphi$. Then the rule $(a, b, \varphi) \rightarrow \mathcal{D}(a, b, \varphi) \in \text{NS}(\mathcal{A})$ defines a group isomorphism. Moreover, for two divisors $D_1 = \mathcal{D}(a, b, \varphi)$ and $D_2 = \mathcal{D}(a', b', \varphi')$ in $\text{NS}(\mathcal{A})$, the intersection number of the divisors is given by

$$(D_1 \cdot D_2) = ab' + a'b - \beta_d(\varphi, \varphi') \quad (11)$$

where β_d is the bilinear form associated to the q_{E_1, E_2} on $\text{Hom}(E_1, E_2)$. Thus

$$(\mathcal{D}(a, b, \varphi) \cdot \mathcal{D}(a, b, \varphi)) = 2(ab - \deg(\varphi)), \quad (\mathcal{D}(a, b, \varphi) \cdot (x\theta_1 + y\theta_2)) = bx + ay.$$

If $\mathcal{A} = E_1 \times E_2$ is a product surface, where $E_1 \sim E_2$ are isogenous, and elliptic curves E_i for $i \in \{1, 2\}$ have extra endomorphisms, then via the isomorphism $\mathcal{D}$ above, we can connect the intersection form $q_{\mathcal{A}}$ to the degree map q_{E_1, E_2} on $\text{Hom}(E_1, E_2)$ as

$$q_{\mathcal{A}}(\mathcal{D}(x, y, \varphi)) = xy - q_{E_1, E_2}(\varphi).$$

Note that $q_{\mathcal{A}}$ is an indefinite integral quadratic form in 6 variables in the case of our interest.

We can characterize principal polarizations in the following simple description.

Proposition 4. [48, Corollary 25] *Let $\mathcal{A} = E_1 \times E_2$ be a product surface. Let $D = \mathcal{D}(a, b, \varphi) \in \text{NS}(\mathcal{A})$. Then $D \in \mathcal{P}(\mathcal{A})$ if and only if $a > 0$ and $ab - \deg(\varphi) = 1$. Thus, every principal polarization of $\mathcal{A}$ has the form $\mathcal{D}(n_1, n_2, \varphi)$ with $\varphi \in \text{Hom}(E_1, E_2)$ and $n_1, n_2 > 0$ with $n_1 n_2 - \deg(\varphi) = 1$.*

For elliptic curves E/K and E'/K , let θ_E and $\theta_{E'}$ denote their canonical principal polarizations. We write $\theta_{\mathcal{A}} = \theta_E \otimes \theta_{E'}$ for the product principal polarization on $\mathcal{A} = E \times E'$. For a product surface with the reducible polarization, the refined Humbert invariant is expressed in terms of the degree quadratic form on $\text{Hom}(E, E')$ as follows.

Lemma 3. [49, Lemma 21] *Let E/K and E'/K be elliptic curves over an arbitrary field K , and let $\mathcal{A} = E \times E'$ be the product surface with the product polarization $\theta_{\mathcal{A}} = \theta_E \otimes \theta_{E'}$. For $a, b \in \mathbb{Z}$, and $\varphi \in \text{Hom}(E, E')$,*

$$q_{(\mathcal{A}, \theta_{\mathcal{A}})}(\mathcal{D}(a, b, \varphi) + \mathbb{Z}\theta_{\mathcal{A}}) = (a - b)^2 + 4q_{E, E'}(\varphi), \quad (12)$$

$q_{E, E'}$ denotes the degree form on $\text{Hom}(E, E')$.

We state some useful facts used in our computations.

Corollary 2. [50, Lemma 28] *The determinant of the Néron-Severi group of $E \times E'$ with respect to the intersection form is given by*

$$\det(\text{NS}(E \times E')) = (-1)^{\rho-1} \det(\text{Hom}(E, E'), \beta_d),$$

where $\rho = \text{rank}(\text{NS}(E \times E')) = \text{rank}(\text{Hom}(E, E')) + 2$.

Proposition 5. [50, Lemma 30] *Let $\rho = \text{rank}(\text{NS}(\mathcal{A}))$. Then the determinant of the quadratic module $(\text{NS}(\mathcal{A}, \theta), q_{(\mathcal{A}, \theta)})$ is related to that of the Néron-Severi group by the formula*

$$\det(\text{NS}(\mathcal{A}, \theta), q_{(\mathcal{A}, \theta)}) = \frac{1}{2}(-4)^{\rho-1} \det(\text{NS}(\mathcal{A}), (\cdot)).$$

We use three different integral quadratic forms: the intersection form $q_{\mathcal{A}}$, the refined Humbert invariant $q_{(\mathcal{A}, \theta)}$, and the degree map q_{E_1, E_2} with their corresponding geometric objects Néron-Severi group $\text{NS}(\mathcal{A})$, the polarized Néron-Severi group $\text{NS}(\mathcal{A}, \theta)$, and homomorphism module $\text{Hom}(E_1, E_2)$, respectively. If $\mathcal{A} = E_1 \times E_2$ and $\text{End}(E_i) \cong \mathcal{O}$ is a maximal order in a quaternion algebra B_p then the corresponding refined Humbert invariant $q_{(\mathcal{A}, \theta)}$ is a positive definite integral quadratic form in 5 variables, which we refer to as a *quintic* refined Humbert invariant.

Elliptic subcovers of abelian surfaces The curves with elliptic subcovers have a very long history⁹. The different perspectives of these curves were studied by Hayashida and Nishi [33], Lange [72, 73], Ibukiyama, Katsura, and Oort [36], Kuhn [69], Murabayashi [79], and Kani [44, 45, 46].

⁹ The history goes back to Legendre, Jacobi, Bolza, Humbert, Picard, Poincaré, and others. The classical method is given in terms of elliptic integrals in Legendre, Jacobi, Goursat [2, 3, 31, 39], and a summary is given by Krazer [68, Chapter XI].

Definition 9. Let $\mathcal{C}$ be a smooth, projective curve of genus 2 over a field K . An elliptic subcover is defined as a finite morphism $f : \mathcal{C} \rightarrow E$ to an elliptic curve E/K not factoring over a non-trivial isogeny of E . If $f' : \mathcal{C} \rightarrow E'$ is another elliptic subcover, then f' is called equivalent to f if there exists an isomorphism $\varphi : E \xrightarrow{\sim} E'$ such that $f' = \varphi \circ f$.

We can suppose that f is minimal¹⁰. There is a bijection between the set of equivalence classes of elliptic subcovers $\mathcal{E}(\mathcal{C})$ of a genus 2 curve $\mathcal{C}$ and the set of maximal elliptic subfields of the function field $F = K(\mathcal{C})$ of $\mathcal{C}$. By [2], we know that $\mathcal{E}(\mathcal{C})$ has either 0 or 2 or infinitely many elements. For the case that $\mathcal{C}$ has infinitely many elliptic subcovers, it occurs when the Jacobian $\mathcal{J}(\mathcal{C})$ of $\mathcal{C}$ is K -isogenous to $E \times E$ for some elliptic curve E/K . The set $\mathcal{E}(\mathcal{C})$ was first studied by Kani [44] in the case $K = \overline{K}$; he proved that the refined Humbert invariant $q_{\mathcal{C}}$ provides a theoretical understanding of $\mathcal{E}(\mathcal{C})$ [44, Theorem 4.5]. Furthermore, Kani [50] later extended this result to any field as follows. Recall that the Jacobian $\mathcal{J}(\mathcal{C})$ is called (N, N) -split if and only if $\mathcal{C}$ has an elliptic subcover of degree N . The criterion this yields is Theorem 3, stated in Section 2 because our algorithms rest on it throughout.

Definition 10. A presentation (E, E', ψ) of degree N of $\mathcal{C}/K$ for a given elliptic subcover $f : \mathcal{C} \rightarrow E$ of degree N is a triple containing E , another (isogenous) elliptic curve E'/K and an isomorphism $\psi : E[N] \rightarrow E'[N]$ which is an anti-isometry with respect to the Weil e_N pairings. An invariant m_{ψ} , called the isogeny defect corresponding to ψ , is defined by

$$m_{\psi} := \min\{m \geq 1 : m \circ \psi = \varphi|_{E[N]} \text{ for some } \varphi \in \text{Hom}(E, E')\}.$$

Recall that $q_{E, E'}$ denotes the degree map on $\text{Hom}(E, E')$, defined by $q_{E, E'}(\varphi) = \deg(\varphi)$ for $\varphi \in \text{Hom}(E, E')$, and let $\det(q_{E, E'})$ denote its determinant.

Theorem 8. [50, Theorem 3] If $\mathcal{C}/K$ has a presentation (E, E', ψ) of degree N with $\text{char}(K) \nmid N$ and isogeny defect $m = m_{\psi}$, and if $r = \text{rank}(\text{Hom}(E, E')) \geq 1$, then the refined Humbert invariant $q_{\mathcal{C}}$ is a positive definite quadratic form of rank $r + 1$ which satisfies properties

- (i) $\det(q_{\mathcal{C}}) = 2^{2r+1} m^2 \det(q_{E, E'})$.
- (ii) $q_{\mathcal{C}}$ primitively represents N^2 .
- (iii) $q_{\mathcal{C}}(x_1, \dots, x_{r+1}) \equiv 0, 1 \pmod{4}$, for all $x_1, \dots, x_{r+1} \in \mathbb{Z}$.
- (iv) $q_{\mathcal{C}}(x_1, \dots, x_{r+1}) \neq 1$ for all $x_1, \dots, x_{r+1} \in \mathbb{Z}$.

Theorem 9. [50, Theorem 4] If (E, E', ψ) is a presentation of degree N of a curve $\mathcal{C}/K$ of genus 2 with $\text{char}(K) \nmid N$, then $m_{\psi} = 1$ if and only if $\mathcal{J}(\mathcal{C}) \cong E \times E'$.

Corollary 3. [50, Corollary 5] If $\mathcal{C}/K$ has an elliptic subcover $f : \mathcal{C} \rightarrow E$ with $\text{char}(K) \nmid \deg(f)$, if $\rho = \text{rank}(\text{NS}(\mathcal{J}(\mathcal{C}))) \geq 3$, and if $\det(q_{\mathcal{C}})/2^{2\rho-3}$ is square-free, then $\mathcal{J}(\mathcal{C}) \cong E \times E'$ for some elliptic curve E'/K .

Automorphism groups The refined Humbert invariant $q_{\mathcal{C}}$ of a genus 2 curve $\mathcal{C}$ has a close relation to the automorphism group of the curve $\mathcal{C}$, see [59, 53]. Kani [53] showed that the automorphism group $\text{Aut}(\mathcal{C})$ of a genus 2 curve $\mathcal{C}$ can be determined from its refined Humbert invariant $q_{\mathcal{C}}$ as follows.

Proposition 6. [53, Proposition 26] Let G be a finite group, and let $\iota(G) := |\{g \in G : \text{ord}(g) = 2\}|$ denote the number of involutions of G . For any integer n , let $r_n(q_{\mathcal{C}}) = |R_n(q_{\mathcal{C}})|$, where $R_n(q_{\mathcal{C}}) = \{D \in \text{NS}(\mathcal{J}(\mathcal{C}), \theta_{\mathcal{C}}) : q_{\mathcal{C}}(D) = n\}$. If $\mathcal{C}/K$ is a curve of genus 2, then $\iota(\text{Aut}(\mathcal{C})) - 1 = r_4(q_{\mathcal{C}})$, the difference being non-negative because the hyperelliptic involution always lies in $\text{Aut}(\mathcal{C})$. Thus, if $r_4(q_{\mathcal{C}}) > 0$, then $\mathcal{J}(\mathcal{C}) \sim E_1 \times E_2$ for some elliptic curves E_i/K , $i = 1, 2$. Moreover, if $r_4(q_{\mathcal{C}}) \geq 3$, then $E_1 \sim E_2$.

¹⁰ Note that these morphisms are called *maximal* by Serre [93], and called *optimal* by Kuhn [69].

The list of possibilities for $\text{Aut}(\mathcal{C})$ for any genus 2 curve is given in the first row of Table 4, see [94, Theorem 2]. The number $r_4(q_{\mathcal{C}})$ is given in the second row of Table 4.

Table 4. Automorphism groups of a curve $\mathcal{C}$ of genus 2 with $r_4(q_{\mathcal{C}})$

$\text{Aut}(\mathcal{C})$	C_2	C_{10}	$\text{C}_2 \times \text{C}_2$	D_4	D_6	$\text{C}_3 \rtimes \text{D}_4$	$\text{GL}_2(\mathbb{F}_3)$
$r_4(q_{\mathcal{C}})$	0	0	2	4	6	8	12

A.1 Real Multiplication, Humbert Surfaces, and Generalized Humbert Sets

Humbert [35] defined an integer invariant for abelian surfaces $\mathcal{A}/\mathbb{C}$ with $\text{End}(\mathcal{A}) \supsetneq \mathbb{Z}$, known as the *Humbert invariant*, giving rise to Humbert surfaces $\mathcal{H}_N$. The refined Humbert invariant $q_{(\mathcal{A}, \theta)}$, Definition 1, is an algebraic refinement of this classical invariant and gives an algebraic description of the Humbert surfaces $\mathcal{H}_N$. Let $\mathfrak{A}_2(K)$ denote the moduli space of principally polarized abelian surfaces over K .

Definition 11 (Classical Humbert surface). [44, Definition 3.7] *For a positive integer N , the Humbert surface of discriminant N is $\mathcal{H}_N := \{(\mathcal{A}, \theta) \in \mathfrak{A}_2(K) : q_{(\mathcal{A}, \theta)} \text{ primitively represents } N\}$. This is precisely the classical Humbert surface of discriminant (or invariant) N .*

This formulation can be deduced from [51, §2, Equation 8]. Therefore, for a positive non-square discriminant D , the condition that $q_{(\mathcal{A}, \theta)}$ primitively represents D is equivalent to the existence of an optimal embedding $\mathcal{O}_D \hookrightarrow \text{End}(\mathcal{A})$ with image contained in $\text{End}_{\theta}(\mathcal{A})$. Hence, $\mathcal{H}_D$ is precisely the locus of principally polarized abelian surfaces admitting real multiplication by $\mathcal{O}_D$.

This description of Humbert surfaces in terms of primitive representations by the refined Humbert invariant extends naturally to positive definite quadratic forms in several variables. Using the refined Humbert invariant, Kani [48] introduced subsets of the moduli space $\mathfrak{A}_2$ of principally polarized abelian surfaces $(\mathcal{A}, \theta)$, called the *generalized Humbert scheme/set* $\mathcal{H}(q)$, indexed by positive definite integral quadratic forms q in $n \geq 1$ variables. If $n = 1$, they are exactly the Humbert surfaces, and $\mathcal{H}(q)$ helps to determine the components of the intersection of Humbert surfaces. Every $\mathcal{H}(q)$ is contained in any Humbert surface $\mathcal{H}_N$ such that q primitively represents N [52, Proposition 5.2].

Theorem 10. *Let $(\mathcal{A}, \theta)$ be a principally polarized abelian surface over an algebraically closed field K , and let $D > 0$ be a fundamental discriminant. Then $q_{(\mathcal{A}, \theta)}$ primitively represents D if and only if there exists an embedding $\xi : \mathcal{O}_D \hookrightarrow \text{End}(\mathcal{A})$ such that $\xi(\mathcal{O}_D) \subseteq \text{End}_{\theta}(\mathcal{A})$.*

This follows from [50, Proposition 14 and Remark 16].

Remark 4. The formulation of Humbert surfaces used by Kani differs from that adopted by Kumar mainly in the choice of moduli-theoretic description. Kani defines the Humbert surface $\mathcal{H}_D \subset \mathfrak{A}_2$ intrinsically in terms of a principally polarized abelian surface $(\mathcal{A}, \theta)$, requiring the associated Humbert invariant quadratic form $q_{(\mathcal{A}, \theta)}$ to represent D primitively. Kumar instead emphasizes the equivalent real multiplication interpretation, viewing $\mathcal{H}_D$ as the image in $\mathfrak{A}_2$ of the Hilbert modular surface parameterizing principally polarized abelian surfaces equipped with a compatible action of the quadratic order of discriminant D . In the square discriminant case, Kumar further restricts attention to the Jacobian locus to relate $\mathcal{H}_{N^2}$ to genus 2 curves admitting degree- N elliptic subcovers. Thus, Kani's definition is intrinsic to the principally polarized abelian surface and applies independently of whether the polarization is reducible or irreducible, whereas Kumar's genus 2 interpretation concerns the intersection of the Humbert surface with the Jacobian locus.

B Proof of Theorem 5

Proof (Theorem 5). By the preceding paragraph, we may take $q = q_5$ and must show: for every odd prime ν and $t \in \mathbb{Z}_\nu$ there is $\alpha \in \mathbb{Z}_\nu^5 \setminus \nu\mathbb{Z}_\nu^5$ with $q_5(\alpha) = t$; and for $\nu = 2$, $p \equiv 3 \pmod{4}$, such α exists exactly when $t \equiv 0, 1 \pmod{4}$. We use two facts from the classification of quadratic forms over $\mathbb{Z}_\nu$ in [63, Ch. 5], where the matrix G_q appears as the matrix $(B(e_i, e_j))$ of the bilinear form B with $q(y) = B(y, y)$, and a form q in n variables is called *unimodular* over $\mathbb{Z}_\nu$ when $\det G_q \in \mathbb{Z}_\nu^\times$. Two forms are *equivalent over $\mathbb{Z}_\nu$* if one is obtained from the other by a substitution $y = Uy'$ with $U \in \mathrm{GL}_n(\mathbb{Z}_\nu)$; this multiplies $\det G_q$ by $(\det U)^2$ and maps $\mathbb{Z}_\nu^n \setminus \nu\mathbb{Z}_\nu^n$ onto itself.

(i) *Odd ν .* Put $q_3(x_0, x_1, x_2) := q_5(x_0, x_1, x_2, 0, 0) = x_0^2 + 4x_1^2 + 4x_2^2$. Then $G_{q_3} = \mathrm{diag}(1, 4, 4)$ has determinant 16, so q_3 is unimodular over $\mathbb{Z}_\nu$ for every odd ν , including $\nu = p$. By [63, Theorem 5.2.4 and the proof of Corollary 5.2.2], a unimodular form in three variables over $\mathbb{Z}_\nu$, ν odd, whose matrix has determinant d is equivalent over $\mathbb{Z}_\nu$ to $2y_1y_2 - dy_3^2$; so there is $U \in \mathrm{GL}_3(\mathbb{Z}_\nu)$ with $q_3(Uy) = 2y_1y_2 - 16y_3^2$. For $t \in \mathbb{Z}_\nu$ take $y = (1, \frac{t}{2}, 0)$, which lies in $\mathbb{Z}_\nu^3$ because 2 is a unit and outside $\nu\mathbb{Z}_\nu^3$ because its first coordinate is 1; then $q_3(Uy) = t$ and $Uy \notin \nu\mathbb{Z}_\nu^3$, so $\alpha := (Uy, 0, 0) \in \mathbb{Z}_\nu^5 \setminus \nu\mathbb{Z}_\nu^5$ satisfies $q_5(\alpha) = t$.

(ii) $\nu = 2$, $p \equiv 3 \pmod{4}$. Put

$$q_4(y_1, y_2, y_3, y_4) := 2y_1^2 + 2y_1y_2 + \frac{p+1}{2}y_2^2 + 2y_3^2 + 2y_3y_4 + \frac{p+1}{2}y_4^2,$$

so that $q_5(x) = x_0^2 + 2q_4(x_1, x_3, x_2, x_4)$ identically. The matrix G_{q_4} is block diagonal with two blocks $\begin{pmatrix} 2 & 1 \\ 1 & (p+1)/2 \end{pmatrix}$ of determinant p , so q_4 is unimodular over $\mathbb{Z}_2$; and $(p+1)/2$ is even because $p \equiv 3 \pmod{4}$, so q_4 takes only even values. By [63, Theorem 5.2.5], a unimodular form in four variables over $\mathbb{Z}_2$ taking only even values is equivalent over $\mathbb{Z}_2$ either to $2y_1y_2 + 2y_3y_4$ or to $2y_1y_2 + 2y_3^2 + 2y_3y_4 + 2y_4^2$. The matrices of these two forms are $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, of determinants $(-1)^2 = 1$ and $(-1) \cdot 3 = -3$. The second is impossible for q_4 , since $\det G_{q_4} = p^2$ and $p^2/(-3) \equiv 5 \pmod{8}$ is not the square of a 2-adic unit. Hence $q_4(Uy) = 2y_1y_2 + 2y_3y_4$ for some $U \in \mathrm{GL}_4(\mathbb{Z}_2)$, and the substitution $x_0 = y_0$, $(x_1, x_3, x_2, x_4) = Uy$ shows that q_5 is equivalent over $\mathbb{Z}_2$ to

$$\tilde{q}_5(y_0, y_1, y_2, y_3, y_4) := y_0^2 + 4y_1y_2 + 4y_3y_4.$$

Since the substitution maps vectors outside $2\mathbb{Z}_2^5$ to vectors outside $2\mathbb{Z}_2^5$, it suffices to decide which t are values of $\tilde{q}_5$ at such vectors. If $t \equiv 0 \pmod{4}$ then $t = \tilde{q}_5(0, 1, t/4, 0, 0)$, and if $t \equiv 1 \pmod{4}$ then $t = \tilde{q}_5(1, 1, (t-1)/4, 0, 0)$, with $t/4, (t-1)/4 \in \mathbb{Z}_2$; both vectors have second coordinate 1, so lie outside $2\mathbb{Z}_2^5$. Conversely $\tilde{q}_5(y) \equiv y_0^2 \pmod{4}$ for every $y \in \mathbb{Z}_2^5$, and the square of a 2-adic integer is $\equiv 0$ or $1 \pmod{4}$; so $\tilde{q}_5$ takes no value $\equiv 2, 3 \pmod{4}$ at all. Hence q_5 takes the value t at a vector outside $2\mathbb{Z}_2^5$ if and only if $t \equiv 0, 1 \pmod{4}$.

The last assertions follow, as $t > 0$ and every square is $\equiv 0, 1 \pmod{4}$.

Remark 5. Part (i) uses only the ternary form $q_3 = x_0^2 + 4x_1^2 + 4x_2^2$ obtained from q_5 by setting $x_3 = x_4 = 0$; it is unimodular at every odd prime, including p . The hypothesis $p \equiv 3 \pmod{4}$ enters only in (ii), to make q_4 even-valued; for $p \equiv 1 \pmod{4}$ the cited classification of unimodular $\mathbb{Z}_2$ -lattices does not apply, and we make no claim either way. This costs us nothing: the standing assumption $p \equiv 11 \pmod{12}$ of this paper implies $p \equiv 3 \pmod{4}$, and is also what makes $B_p = (-1, -p \mid \mathbb{Q})$ and the base curve $j = 1728$ available in Section 3. Of $t = \ell^{2k}$, only the fact that it is a square is used.

C The counts of Ibukiyama–Katsura–Oort

For the reader's convenience, we reproduce the explicit values of $a_G(p)$ of Theorem 2, taken from [36, Theorem 3.3], since Table 2 compares against them directly. Let $p \geq 7$ and write

$\varepsilon_d = 1 - \left(\frac{-d}{p}\right)$ for $d = 1, 2, 3$, so that $\varepsilon_d \in \{0, 2\}$. Then

$$\begin{aligned} a_1(p) &= \frac{(p-1)(p^2-35p+346)}{2880} - \frac{\varepsilon_1}{32} - \frac{\varepsilon_2}{8} - \frac{\varepsilon_3}{9} - \begin{cases} 0 & p \equiv 1, 2, 3 \pmod{5}, \\ \frac{1}{5} & p \equiv 4 \pmod{5}, \end{cases} \\ a_{C_2}(p) &= \frac{(p-1)(p-17)}{48} + \frac{\varepsilon_1}{8} + \frac{\varepsilon_2}{2} + \frac{\varepsilon_3}{2}, \\ a_{C_2 \times C_2}(p) &= \frac{p-1}{8} - \frac{\varepsilon_1}{8} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{2}, \quad a_{S_3}(p) = \frac{p-1}{6} - \frac{\varepsilon_2}{2} - \frac{\varepsilon_3}{3}, \\ a_{D_6}(p) &= \frac{\varepsilon_3}{2} = \begin{cases} 0 & p \equiv 1 \pmod{6}, \\ 1 & p \equiv 5 \pmod{6}, \end{cases} \quad a_{S_4}(p) = \frac{\varepsilon_2}{2} = \begin{cases} 0 & p \equiv 1, 3 \pmod{8}, \\ 1 & p \equiv 5, 7 \pmod{8}, \end{cases} \\ a_{C_5}(p) &= \begin{cases} 0 & p \equiv 1, 2, 3 \pmod{5}, \\ 1 & p \equiv 4 \pmod{5}. \end{cases} \end{aligned}$$

The counts $\mathbf{h}(p)$ and $\mathbf{H}(p)$: The two counts used throughout are also classical. The class number $\mathbf{h}$ of a maximal order of B_p , equivalently the number of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ up to isomorphism, is

$$\mathbf{h} = \frac{p-1}{12} + \frac{1}{4} \left(1 - \left(\frac{-1}{p}\right)\right) + \frac{1}{3} \left(1 - \left(\frac{-3}{p}\right)\right), \quad (13)$$

due to Eichler, Deuring and Igusa; and the number $\mathbf{H}$ of principal polarizations on $E \times E$ up to automorphism, equivalently the number of principally polarized superspecial abelian surfaces up to isomorphism, is

$$\begin{aligned} \mathbf{H} &= \frac{(p-1)(p+12)(p+23)}{2880} + \frac{2p+13}{96} \left(1 - \left(\frac{-1}{p}\right)\right) + \frac{p+11}{36} \left(1 - \left(\frac{-3}{p}\right)\right) \\ &\quad + \frac{1}{8} \left(1 - \left(\frac{-2}{p}\right)\right) + \frac{1}{12} \left(1 - \left(\frac{-3}{p}\right)\right) \left(1 - \left(\frac{-1}{p}\right)\right) + \begin{cases} 0 & p \equiv 1, 2, 3 \pmod{5}, \\ \frac{4}{5} & p \equiv 4 \pmod{5}, \end{cases} \end{aligned} \quad (14)$$

by [56, Theorem 3.3]; see also [60, §2.2], from which we take this form of both statements. At $p = 251$ these give $\mathbf{h} = 22$ and $\mathbf{H} = 6281$, so $\frac{\mathbf{h}(\mathbf{h}+1)}{2} = 253$ and $\mathbf{H} - \frac{\mathbf{h}(\mathbf{h}+1)}{2} = 6028$, reproducing the first three count columns of Table 2. Since $\mathbf{h} = \frac{p}{12} + O(1)$ and $\mathbf{H} = \frac{p^3}{2880} + O(p^2)$, the proportion of principal polarizations that are reducible is

$$\frac{\mathbf{h}(\mathbf{h}+1)/2}{\mathbf{H}} = \frac{10}{p} + O(p^{-2}). \quad (15)$$

The automorphism counts: Here D_6 denotes the dihedral group of order 12, written D_{12} in [36]. The reduced automorphism group determines the full automorphism group of the curve: the correspondence $\text{RA}(\mathcal{C}) \mapsto \text{Aut}(\mathcal{C})$ used in Table 2 is $1 \mapsto C_2, C_2 \mapsto C_2 \times C_2, C_2 \times C_2 \mapsto D_4, S_3 \mapsto D_6, D_6 \mapsto C_3 \rtimes D_4, S_4 \mapsto \text{GL}_2(\mathbb{F}_3), C_5 \mapsto C_{10}$, which is compatible with the involution counts of Table 4.

As a check, take $p = 251$, so $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{-2}{p}\right) = 1$, $\left(\frac{-3}{p}\right) = -1$, that is $(\varepsilon_1, \varepsilon_2, \varepsilon_3) = (2, 0, 2)$, and $p \equiv 1 \pmod{5}$. The formulas give $a_1 = 4736$, $a_{C_2} = 1220$, $a_{C_2 \times C_2} = 30$, $a_{S_3} = 41$, $a_{D_6} = 1$, $a_{S_4} = 0$ and $a_{C_5} = 0$, which sum to $6028 = \mathbf{H}(251) - \frac{\mathbf{h}(\mathbf{h}+1)}{2}$ and reproduce the corresponding row of Table 2.