Refined Humbert Invariants in Supersingular Isogeny Degree Analysis

Eda Kırımlı[1] and Gaurish Korpal[2]

[1] University of Birmingham, United Kingdom
[2] University of Auckland, New Zealand

Abstract. We focus on *refined Humbert invariants* of principally polarized superspecial abelian surfaces, introduced by Kani in 1994. The main contributions are to enumerate principal polarizations on a superspecial surface, and for each polarization, to compute the refined Humbert invariant of a principally polarized superspecial abelian surface. Then, we present several applications of computing this invariant for isogeny-based cryptography. First, we provide a decision algorithm to check if two given polarizations are isomorphic. Second, we present an efficient algorithm to determine the geometric type of a principally polarized superspecial surface. Third, we prove an upper bound on the largest minimal isogeny degree among pairs of supersingular elliptic curves, independent of their endomorphism-ring structures, and our experimental evidence verifies this claim up to $p = 659$, $p \equiv 11 \pmod{12}$. Fourth, we present experimental evidence for a minimum isogeny frequency within the proven upper bounds. Lastly, we provide a different perspective on the fixed isogeny degree problem using refined Humbert invariants and analyze it without explicit endomorphism rings.

Keywords: isogeny · superspecial surface · refined Humbert invariant · degree map

1 Introduction

The refined Humbert invariants of principally polarized superspecial surfaces underline several hard isogeny problems relevant to post-quantum cryptography [KM24], yet no prior work has computed them for superspecial surfaces or enumerated their principal polarizations. In this paper, we close this gap: we give the first computation of refined Humbert invariants of principally polarized superspecial surfaces, the first enumeration of their principal polarizations, and apply the resulting invariants to several isogeny problems.

Our strategy is based on refined Humbert invariants, whose definition and relevant properties we briefly summarize below. Let $\mathcal{A}$ be an abelian surface over $\overline{\mathbb{F}}_p$ and let $\mathrm{NS}(\mathcal{A})$ denote its Néron-Severi group. The intersection product $(D_1 \cdot D_2)$ of divisors D_1 and D_2 on $\mathcal{A}$ defines an integral quadratic form $q_{\mathcal{A}}$ on $\mathrm{NS}(\mathcal{A})$, Definition 3. Since $\mathrm{NS}(\mathcal{A}) \cong \mathbb{Z}^\rho$ where $\rho = \rho(\mathcal{A})$ is the Picard number of $\mathcal{A}$, the quadratic form[1] $q_{\mathcal{A}}$ is equivalent to an integral quadratic form q in ρ variables, so leading to an isomorphism $(\mathrm{NS}(\mathcal{A}), q_{\mathcal{A}}) \cong (\mathbb{Z}^\rho, q)$ of quadratic modules.

Let θ be a principal polarization on $\mathcal{A}$, see Definition 2. We define an integral quadratic form $\tilde{q}_{(\mathcal{A},\theta)}$ on $\mathrm{NS}(\mathcal{A})$ as

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

E-mail: e.kirimli@bham.ac.uk (Eda Kırımlı), gaurish.korpal@auckland.ac.nz (Gaurish Korpal)

[1] Throughout the paper, a quadratic form means always an integral quadratic form.

This work is licensed under a "CC BY 4.0" license.
Date of this document: 2026-07-28.

It follows that $\tilde{q}_{(\mathcal{A},\theta)}(D + n\theta) = \tilde{q}_{(\mathcal{A},\theta)}(D)$ for all $n \in \mathbb{Z}$, therefore we have a quadratic form $q_{(\mathcal{A},\theta)}$ defined on the quotient module $\mathrm{NS}(\mathcal{A},\theta) = \mathrm{NS}(\mathcal{A})/\mathbb{Z}\theta$, called the polarized Néron-Severi group. The form $q_{(\mathcal{A},\theta)}$ is a positive-definite quadratic form on the polarized Néron-Severi group $\mathrm{NS}(\mathcal{A},\theta) \cong \mathbb{Z}^{\rho-1}$, and called a *refined Humbert invariant*, see Section 2.1 for details.

The computation of refined Humbert invariants is a challenging problem; this has been thoroughly examined in [Kan94, Kan14, Kan16, Kan18, Kan19, Kan21]. The determination of a refined Humbert invariant is comparatively easier when $\mathcal{A} \cong E_1 \times E_2$ for elliptic curves E_1, E_2. In this case, there exists a relation between divisors in the Néron-Severi group and isogenies between E_1 and E_2. By using Theorem 1, we can represent divisors on $\mathrm{NS}(E_1 \times E_2)$ as $D = \mathcal{D}(a, b, \varphi)$ with two integers a, b and an isogeny φ. This representation allows us to compute the intersection number of divisors more easily. The relation between the refined Humbert invariant and the degree map is given by Lemma 2

$$q_{(E_1\times E_2,\theta_{E_1\times E_2})} \text{ is } \mathbb{Z}\text{-equivalent to } x^2 + 4q_{E_1,E_2}$$

where $\theta_{E_1\times E_2}$ is a product polarization and $q_{E_1,E_2} \in \mathbb{Z}[y_1, \ldots, y_n]$ is the degree map.

First, we develop a decision algorithm to determine whether two principal polarizations on a superspecial surface are isomorphic. Although this problem has a classical formulation as the equivalence problem for positive-definite binary quaternion Hermitian forms [IKO86, HI80], i.e., for a maximal quaternion order $\mathcal{O}$, testing equivalence of principal polarizations given by two uni-modular Hermitian matrices $g_1, g_2 \in \mathrm{GL}_2(\mathcal{O})$ requires finding a matrix $u \in \mathrm{GL}_2(\mathcal{O})$ satisfying $g_2 = u^* g_1 u$ where $*$ is the conjugate-transpose. This problem is computationally demanding, and, to the best of our knowledge, no decision algorithm has previously been given for the principal polarizations of superspecial abelian surfaces.

Secondly, we provide an explicit algorithm to determine the geometric type of a principally polarized superspecial abelian surface: whether it is the Jacobian of a genus-two curve with its canonical principal polarization or a product of two elliptic curves with the product polarization. This is achieved by the criterion in Proposition 2.

Thirdly, we prove that, for a generic prime p, the maximum of the minimum distances between supersingular elliptic curves is upper-bounded by $\sqrt{\frac{p}{2}}$, without prior explicit knowledge of their endomorphism rings. We first discuss previous proven bounds, improve the bound itself, and validate their correctness with experiments for primes $p < 660$, $p \equiv 11 \pmod{12}$, by assuming less information. Without refined Humbert invariants, verifying this heuristic for small examples would involve brute-force computations of isogenies or quaternion orders between pairs of elliptic curves. Our approach instead reduces the problem to simple checks on quadratic forms.

Fourthly, we run experiments on the frequency and distribution of isogeny degrees between supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. We run these experiments directly on the degree maps themselves, without computing isogenies or endomorphism rings.

Lastly, we give a different approach to the fixed-degree isogeny problem: given supersingular curves E_1, E_2 and a target degree N, we show that an efficient algorithm for computing refined Humbert invariants yields the degree map q_{E_1,E_2}, addressing the intermediate-degree range left open between lattice-reduction methods for small degrees and KLPT-type algorithms [KLPT14, FKL+20] for large ones. This bears directly on schemes such as SQIsign, whose verification step is non-deterministic because SigningKLPT does not guarantee a specific isogeny degree, slowing the protocol.

Contribution. We start with a supersingular product surface $\mathcal{A} = E_1 \times E_2$, and choose a principal polarization θ and an arbitrary divisor D on $\mathrm{NS}(E_1 \times E_2)$ to calculate the refined Humbert invariant, see Definition 6. Thus, we apply the irreducibility criterion, Proposition 2, of the refined Humbert invariant $q_{(\mathcal{A},\theta)}$ to decide whether it is a product of two elliptic curves or not. Later, we use the relation between the refined Humbert invariant

and the degree map (Definition 9), then pull out the degree map and check its minimum value. This same degree map underlies our experiments on isogeny-degree distributions and our treatment of the fixed-degree isogeny problem.

In terms of computational assumptions on the degrees of isogenies between supersingular elliptic curves, we want to investigate the minimal integer represented by such degree maps for different choices of principal polarizations θ, as they are exactly the minimum isogenies between two supersingular elliptic curves. Then, we aim to find the largest possible minimal degree that allows us to bound the maximum minimum isogeny degree reached by every pair of supersingular elliptic curves. That is, for a fixed prime p, we aim to understand the value

$$d \coloneqq \max_{E_1,E_2} \{\min\{N : q_{E_1,E_2}(t_1,t_2,t_3,t_4) = N \text{ for some } t_1,t_2,t_3,t_4 \in \mathbb{Z}\}\}. \tag{1}$$

This set ranges over different supersingular curves E_1 and E_2 over $\mathbb{F}_{p^2}$.

Outline. The paper is organized into preliminaries, computations, and applications. In Section 2, we summarize the theoretical preliminaries. In Section 3, we develop algorithms to compute refined Humbert invariants and degree maps, and present how computations were performed. In Section 4, we discuss the applications of our method, including the proof of the upper bound on the minimum isogeny degrees. We conclude the paper in Section 5.

2 Preliminaries

2.1 Refined Humbert invariant

In this section, we introduce the theory of refined Humbert invariants defined by Kani [Kan94] in 1994, which is the main tool of this paper. This invariant is very beneficial in the interplay between geometric and arithmetic problems. Many applications of these invariants can be found in [Kan14, Kan16]. This section mainly follows [Kan18, Kan19]. We only present essential facts of refined Humbert invariants here.

Definition 1. [Har77, p.357] Let $\mathcal{A}$ be an abelian surface over a field K. Let $\mathrm{Div}(\mathcal{A})$ be the set of divisors of $\mathcal{A}$. If D_1 and $D_2 \in \mathrm{Div}(\mathcal{A})$, then we say that D_1 is *numerically equivalent* to D_2, denoted by $D_1 \equiv D_2$, and if for all $D \in \mathrm{Div}(\mathcal{A})$ we have that

$$(D_1 \cdot D) = (D_2 \cdot D),$$

where $(\cdot)$ denotes the intersection number.

The intersection theory of abelian varieties is a vast subject; for technical details, we refer to [Sha13, Chapter 4.1] and [Har77, Chapter V.1]. Fortunately, we utilize a simple formula for the intersection formula in the case of $\mathcal{A} = E_1 \times E_2$ given by Theorem 1 below, and it is sufficient for our calculations.

2.1.1 Néron-Severi group.

Let $\mathcal{A}/K$ be an abelian surface. We define the *Néron-Severi group* $\mathrm{NS}(\mathcal{A})$ of $\mathcal{A}$ to be

$$\mathrm{NS}(\mathcal{A}) = \mathrm{Div}(\mathcal{A})/\equiv,$$

where $\equiv$ is the equivalence defined in Definition 1. This definition agrees with the usual definition of $\mathrm{NS}(\mathcal{A})$ in [Lan83, p.101] since the $\mathrm{Pic}^0(\mathcal{A})$-equivalence and the numerical equivalence coincide by the Corollary of Theorem V.1 in [Lan83].

Definition 2. Let $\mathcal{A}/K$ be an abelian surface. We define

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

to be *the set of principal polarizations* of $\mathcal{A}$.

By using the Nakai-Moishezon criterion [Har77, Theorem V.1.10], we see that if $D \in \mathrm{NS}(\mathcal{A})$ is ample, then $D' \in \mathrm{cl}(D)$ is ample.

Definition 3. 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 $\mathrm{NS}(\mathcal{A})$, called the *intersection form*:

$$q_{\mathcal{A}}(D) = \frac{1}{2}(D \cdot D) \text{ for all } D \in \mathrm{Div}(\mathcal{A}).$$

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

Definition 4. [Sil09, Corollary III.6.3] We define the *degree map* (or *degree quadratic form*)

$$q_{E_1,E_2}(\varphi) = \deg(\varphi) \text{ for } \varphi \in \mathrm{Hom}(E_1, E_2).$$

The degree map q_{E_1,E_2} is a positive definite quadratic form on $\mathrm{Hom}(E_1, E_2)$ in r variables, where $r = \mathrm{rank}(\mathrm{Hom}(E_1, E_2)) = \dim_{\mathbb{Q}}(\mathrm{End}^0(E_i))$.

For a fixed basis of $\mathrm{Hom}(E_1, E_2)$, the degree map q_{E_1,E_2} is an explicit positive definite quadratic form in r variables.

Definition 5. [Ful89, Corollary of Section 6.4] Let X and Y be varieties. If $h : X \to Y$ is a morphism of varieties, the graph of h, denoted by Γ_h is defined to be $\{(x, y) \in X \times Y | \quad y = h(x)\}$.

We now specialize in the case of products of two elliptic curves.

Theorem 1. [Kan16, Proposition 22] *Let $\mathcal{A} = E_1 \times E_2$ be a product of two elliptic curves. Then we have a group isomorphism*

$$\mathcal{D} := \mathcal{D}_{E_1,E_2} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{NS}(\mathcal{A}) \tag{2}$$

$$\mathcal{D}(a, b, \varphi) = (a - 1)\theta_1 + (b - \deg(\varphi))\theta_2 + \Gamma_{-\varphi} \tag{3}$$

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

$$(D_1 \cdot D_2) = ab' + a'b - \beta_d(\varphi, \varphi') \tag{4}$$

where β_d is the bilinear form associated with the q_{E_1,E_2} on $\mathrm{Hom}(E_1, E_2)$. Thus,[2]

$$(\mathcal{D}(a, b, \varphi) \cdot \mathcal{D}(a, b, \varphi)) = 2(ab - \deg(\varphi)), \quad (\mathcal{D}(a, b, \varphi) \cdot (x\theta_1 + y\theta_2)) = bx + ay. \tag{5}$$

Recall that a bilinear form β_d is defined by

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

Using the (4) above, we can easily calculate the intersection numbers of divisors on abelian product surfaces. Moreover, we can numerically characterize principal polarizations as follows.

[2]We would like to emphasize that there is no isogeny computation needed in the intersection formulas, and only the degrees of the isogenies are involved. This gives a different approach to the isogeny problem without computing an isogeny.

Corollary 1. [Kan16, Corollary 25] *Let $\mathcal{A}/K$ be an abelian surface and let $D = \mathcal{D}(a, b, \varphi) \in \mathrm{NS}(\mathcal{A})$, using the notation of* Theorem 1. *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 $\varphi \in \mathrm{Hom}(E_1, E_2)$ and $n_1, n_2 > 0$ with $n_1 n_2 - (\deg(\varphi)) = 1$.*

The relation between the intersection form (3) and the degree map (4) is given by

$$q_{\mathcal{A}}(x, y, \varphi) = xy - q_{E_1,E_2}(\varphi). \tag{6}$$

where xy denotes the quadratic form defined by the hyperbolic plane. Note that $q_{\mathcal{A}}$ is an indefinite integral quadratic form in $\rho = r + 2$ variables where ρ is the Picard number of $\mathcal{A}$, and r is the rank of $\mathrm{Hom}(E_1, E_2)$.

Lemma 1. [Kan19, Lemma 28] *The determinant of the Néron-Severi group of $E_1 \times E_2$ with respect to the intersection form is given by*

$$\det(\mathrm{NS}(E_1 \times E_2)) = (-1)^{\rho-1} \det(\mathrm{Hom}(E_1, E_2), \beta_d),$$

where $\rho = \mathrm{rank}(\mathrm{NS}(E_1 \times E_2)) = \mathrm{rank}(\mathrm{Hom}(E_1, E_2)) + 2$.

2.1.2 Polarized Néron-Severi group.

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

$$\mathrm{NS}(\mathcal{A}, \theta) \coloneqq \mathrm{NS}(\mathcal{A})/\mathbb{Z}\theta.$$

Kani discusses in [Kan94, §3] that there is a well-defined map on $\mathrm{NS}(\mathcal{A}, \theta)$, and this defines a positive-definite quadratic form on $\mathrm{NS}(\mathcal{A}, \theta)$. Suppose that $\mathcal{A}$ has a principal polarization $\theta \in \mathcal{P}(\mathcal{A})$. Then the quadratic form $\tilde{q}_{(\mathcal{A},\theta)}$ on $\mathrm{NS}(\mathcal{A})$ is

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

It is clear to see that $\tilde{q}_{(\mathcal{A},\theta)}(D + n\theta) = \tilde{q}_{(\mathcal{A},\theta)}(D)$ for all $n \in \mathbb{Z}$. As a consequence, $\tilde{q}_{(\mathcal{A},\theta)}$ actually leads to a quadratic form $q_{(\mathcal{A},\theta)}$ on the quotient module $\mathrm{NS}(\mathcal{A}, \theta)$.

Definition 6. Let $(\mathcal{A}, \theta)$ be a principally polarized abelian surface. A *refined Humbert invariant*[3] $q_{(\mathcal{A},\theta)}$ of $(\mathcal{A}, \theta)$ is a positive-definite quadratic form on $\mathrm{NS}(\mathcal{A}, \theta)$, or more precisely, the quadratic module $(\mathrm{NS}(\mathcal{A}, \theta), q_{(\mathcal{A},\theta)})$, satisfying, for all $\mathrm{cl}(D) \in \mathrm{NS}(\mathcal{A}, \theta)$

$$q_{(\mathcal{A},\theta)}(D) = (D \cdot \theta)^2 - 2(D \cdot D).$$

Proposition 1. [Kan19, Lemma 30] *Let $\rho = \mathrm{rank}(\mathrm{NS}(\mathcal{A}))$. Then the determinant of the quadratic module $(\mathrm{NS}(\mathcal{A}, \theta), q_{(\mathcal{A},\theta)})$ is related to that of the Néron–Severi group by the formula*

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

2.1.3 Irreducibility criterion.

One of the useful properties of a refined Humbert invariant $q_{(\mathcal{A},\theta)}$ of $(\mathcal{A}, \theta)$ is the following irreducibility criterion.

Definition 7. [Wei57, Satz 2] A polarization $\theta \in \mathcal{P}(\mathcal{A})$ is called *reducible* (or *decomposable*) if $\theta = \mathrm{cl}(E_1 + E_2)$ for some elliptic curves E_1 and E_2 on $\mathcal{A}$. The set of all reducible polarizations is denoted by $\mathcal{P}(\mathcal{A})^{\mathrm{red}}$.

[3] A refined Humbert invariant is considered up to equivalences, so mostly we refer it as the refined Humbert invariant up to isometries for a fixed principally polarized abelian surface $(\mathcal{A}, \theta)$

Proposition 2. [Kan16, Proposition 6] *Let $q_{(\mathcal{A},\theta)}$ the refined Humbert invariant of the principally polarized abelian surface $(\mathcal{A},\theta)$, then we have that*

$$\theta \text{ is reducible if and only if } q_{(\mathcal{A},\theta)} \text{ represents } 1. \tag{8}$$

Proposition 2 above allows us to decide whether a principally polarized abelian surface $\mathcal{A}$ is Jacobian of a curve $(\mathcal{J}(\mathcal{C}),\theta_{\mathcal{C}})$, or a product of two elliptic curves $(E_1\times E_2,\theta_{E_1\times E_2})$.

2.1.4 A necessary condition.

For a generic principally polarized abelian surface $(\mathcal{A},\theta)$, there exists a necessary condition for an integral quadratic form appearing as a refined Humbert invariant as follows.

Theorem 2. [Kır24, Theorem 3.1.1] *If an integral quadratic form f is equivalent to a refined Humbert invariant $q_{(\mathcal{A},\theta)}$ for some principally polarized abelian surface $(\mathcal{A},\theta)/K$, then $f\equiv 0,1 \pmod 4$.*

2.1.5 An equivalent definition.

Later, Kani generalized the definition of a refined Humbert invariant in [Kan19, Remark 16] as follows.

Definition 8. Let $\mathcal{A}$ be an abelian surface over a field K. If $\mathcal{A}$ has a principal polarization $\theta:\mathcal{A}\to\hat{\mathcal{A}}$ defined over K, then we define the additive subgroup $\mathrm{End}_\theta(\mathcal{A})$ of the ring $\mathrm{End}(\mathcal{A})=\mathrm{End}_K(\mathcal{A})$ of K-endomorphisms of $\mathcal{A}$ by:

$$\mathrm{End}_\theta(\mathcal{A})=\{\mu\in\mathrm{End}(\mathcal{A}):\hat{\mu}\circ\theta=\theta\circ\mu\}=\{\mu\in\mathrm{End}(\mathcal{A}):\mu=\mu'\},$$

where $\mu'=r_\theta(\mu)\coloneqq\theta^{-1}\circ\hat{\mu}\circ\theta$. Thus, $\mathrm{End}_\theta(\mathcal{A})$ consists of those endomorphisms which are symmetric with respect to the Rosati involution r_θ defined by θ.

Proposition 3. [Kan19, Proposition 14, Remark 16] *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 $\mu\in\mathrm{End}_\theta(\mathcal{A})$, we have that*

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

where tr *is the usual rational trace of an endomorphism as defined in* [Mum70, p.182].

There exists a close relation between the refined Humbert invariant $q_{(\mathcal{A},\theta)}$ $(\mathcal{A},\theta)$ and the degree map q_{E_1,E_2} when $\mathcal{A}=E_1\times E_2$ is the product surface, as follows.

Lemma 2. [Kan18, Lemma 21] *Let E_1/K and E_2/K be elliptic curves over an arbitrary field K, and let $\mathcal{A}=E_1\times E_2$ be the product surface with the product polarization $\theta_{\mathcal{A}}=\theta_{E_1}\otimes\theta_{E_2}$. For $a,b\in\mathbb{Z}$, and $\varphi\in\mathrm{Hom}(E_1,E_2)$, then*

$$q_{(\mathcal{A},\theta_{\mathcal{A}})}(\mathcal{D}(a,b,\varphi))=(a-b)^2+4q_{E_1,E_2}(\varphi), \tag{9}$$

q_{E_1,E_2} denotes the degree map on $\mathrm{Hom}(E_1,E_2)$.

More general statements can be given related to refined Humbert invariants by using elliptic subcovers and isogeny defects as follows.

Definition 9. Let $\mathcal{C}/K$ be a curve of genus 2. The presentation of $\mathcal{C}/K$ of degree N is the triple (E,E',ψ) which arises from a given elliptic subcover $F:\mathcal{C}\to E$ of degree N. This triple consists of E, another (isogenous) elliptic curve E'/K, and an isomorphism $\psi:E[N]\to E'[N]$ which is an anti-isometry with respect to the Weil pairing e_N.

Definition 10. Attached to ψ, an invariant, *the isogeny defect* m_ψ is defined as

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

Theorem 3. [Kan19, Theorem 3] *If $\mathcal{C}/K$ has a presentation (E, E', ψ) of degree N with $\mathrm{char}(K) \nmid N$ an isogeny defect $m = m_\psi$, and if $r = \mathrm{rank}(\mathrm{Hom}(E, E')) \geq 1$, then the refined Humbert invariant $q_\mathcal{C}$ is a positive definite quadratic form of rank $n = r + 1$, 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) $q_\mathcal{C}(x_1, \ldots, x_{r+1}) \equiv 0, 1 \pmod 4$, *for all* $x_1, \ldots, x_{r+1} \in \mathbb{Z}$.

(iv) $q_\mathcal{C}(x_1, \ldots, x_{r+1}) \neq 1$ *for any* $x_1, \ldots, x_{r+1} \in \mathbb{Z}$.

Theorem 4. [Kan19, Theorem 4] *If (E, E', ψ) is a presentation of the degree N of a curve $\mathcal{C}/K$ of genus 2 with $\mathrm{char}(K) \nmid N$, then $m_\psi = 1$ if and only if $\mathcal{J}(\mathcal{C}) \cong E \times E'$.*

The set $\mathcal{P}(\mathcal{A}, q)$ is defined as all the principal polarizations $\theta \in \mathcal{P}(\mathcal{A})$ which are equivalent to the refined Humbert invariant $q_{(\mathcal{A},\theta)}$

$$\mathcal{P}(\mathcal{A}, q) = \{\theta \in \mathcal{P}(\mathcal{A}) : q_{(\mathcal{A},\theta)} \sim q\}.$$

The set of reducible polarizations, as in Definition 7, can be written as the union of several sets of the form $\mathcal{P}(\mathcal{A}, q_i)$ by varying q_i's in the following way.

Proposition 4. [Kan24, Proposition 6] *If $\mathcal{A} = E \times E'$ is an abelian product surface, then*

$$\mathcal{P}(\mathcal{A})^{\mathrm{red}} = \coprod_{q \in \mathrm{Gen}(q_{E,E'})} \mathcal{P}(\mathcal{A}, x^2 \perp 4q)$$

where $\mathrm{Gen}(q)$ *is the set of isomorphism classes of integral quadratic forms q which are genus-equivalent to the integral quadratic form $q_{E,E'}$.*

2.2 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 $\mathrm{End}(E)$. If two elliptic curves E_1,E_2 are isogenous $E_1 \sim E_2$, then $\mathrm{End}^0(E_1) \simeq \mathrm{End}^0(E_2)$. An elliptic curve E defined over $\overline{\mathbb{F}}_p$ is said to be *supersingular* if the endomorphism algebra, $\mathrm{End}^0_{\overline{\mathbb{F}}_p}(E)$, 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 $(a, b) = (-1, -p)$ [EHL+18, 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 $\overline{\mathbb{F}}_p$ [Oor74], 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 unpolarizedabelian variety). A curve $\mathcal{C}$ is called *supersingular* (respectively, *superspecial*) if its Jacobian $\mathcal{A} = \mathcal{J}(\mathcal{C})$ is supersingular (respectively, *superspecial*).

Theorem 5. *(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 proof, see [Ogu79, Theorem 6.2],[Shi79, Theorem 3.5], and [LO98, Section 1.6].

In the case of dimension $g = 1$, there are many superspecial abelian varieties (i.e., supersingular elliptic curves), each with one principal polarization, but in the case of $g > 1$, there is one superspecial abelian variety with many principal polarizations.

The map in Theorem 1 (or using Corollary 2.9 of [IKO86]) induces a bijection between principal polarizations $\theta \in \mathcal{P}(E_1 \times E_2)$ and positive definite quaternion hermitian matrices with determinant 1

$$\mathcal{P}(E_1 \times E_2) = \left\{ \begin{pmatrix} u & \alpha \\ \overline{\alpha} & v \end{pmatrix} : u, v \in \mathbb{Z}_{>0},\ \alpha \in \mathcal{O},\ uv - \alpha\overline{\alpha} = 1 \right\} \tag{10}$$

where $\mathcal{O}$ is a maximal order of B_p.

The natural question is how to choose a representative in the conjugacy (isomorphism) class of a principal polarization on the superspecial abelian surface, as there are too many of them to use in the computations. This issue has been considered by Hashimoto and Ibukiyama [HI80]. Let $\mathcal{O}$ be a maximal order of B_p, $\mathcal{L}(\mathcal{O})$ be the set of all maximal $\mathcal{O}$-lattices, and $\mathcal{L}(\mathcal{O}; 0)$ be the principal genus. Then any $\mathcal{O}$-lattice in B_p^2 can be written as $\Lambda = (\mathcal{O}, \mathcal{O})G$ for $G \in \mathrm{GL}_2(B_p)$.

Proposition 5. [HI80, Proposition 22] *$\Lambda = (\mathcal{O}, \mathcal{O})G$ belongs to $\mathcal{L}(\mathcal{O}; 0)$ if and only if G satisfies the condition*

$$GG^* = r \begin{pmatrix} u & \alpha \\ \bar{\alpha} & v \end{pmatrix}; \quad u, v \in \mathbb{Z}_{>0}, \quad \alpha \in \mathcal{O}, \quad uv - \mathrm{nrd}(\alpha) = 1, \quad r \in \mathbb{Q}_+^\times. \tag{11}$$

Any maximal $\mathcal{O}$-lattice in $\mathcal{L}(\mathcal{O}, 0)$ is equivalent to a maximal $\mathcal{O}$-lattice. Therefore, one can reduce the problem of finding all representatives of the classes in the $\mathcal{L}(\mathcal{O}; 0)$, to the problem of finding all (u, v, α) satisfying (11) up to the equivalence by $\mathrm{GL}_2(\mathcal{O})$.

Lemma 3. [HI80, Lemma 13] *With the same notation as above, we have the following information regarding the conjugacy classes of any lattice $\Lambda \in \mathcal{L}(\mathcal{O}, 0)$.*

(i) The equivalence class of $\begin{pmatrix} u & \alpha \\ \overline{\alpha} & v \end{pmatrix}$ only depends on $\alpha \pmod v$ for fixed v.

(ii) If $\beta, \beta' \in \mathcal{O}^\times$, then $\begin{pmatrix} u & \alpha \\ \overline{\alpha} & v \end{pmatrix}$ and $\begin{pmatrix} u & \beta\alpha\beta' \\ \overline{\beta\alpha\beta'} & v \end{pmatrix}$ are equivalent.

(iii) $\begin{pmatrix} u & \alpha \\ \bar{\alpha} & v \end{pmatrix}$ and $\begin{pmatrix} u & \bar{\alpha} \\ \alpha & v \end{pmatrix}$ are equivalent.

Later, in Algorithm 2, we will apply Lemma 3 to find representatives in the conjugacy classes of principal polarizations. By using the basis of $\mathcal{O}$ over $\mathbb{Z}$, we can give an algorithm to find all triples (u, v, α) satisfying the condition in (11) as follows:

1. Let $v = 1, 2, 3, \ldots$
2. For each v, find all $\alpha \in \mathcal{O}/(v\mathcal{O})$ such that $\mathrm{nrd}(\alpha) + 1 = 0 \pmod v$
3. Compute $u = (\mathrm{nrd}(\alpha) + 1)/v$.

3 Computation

A refined Humbert invariant $q_{(\mathcal{A},\theta)}$, Definition 6, corresponding to a principally polarized superspecial abelian surface $(\mathcal{A}, \theta)$ is an integral quadratic form in 5 variables, called the *quintic refined Humbert invariant*[4].

[4]Kani refers to them as quintic quadratic forms, although many people in the literature use quinary integral form. We prefer to use quintic integral forms following Kani's terminology.

Unless stated otherwise, let p be an odd prime, let E be a fixed supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$, and let $\mathcal{A} = E \times E$ be a supersingular product surface with principal polarization θ. Assume that $p \equiv 11 \pmod{12}$ and $\mathrm{End}^0_{\overline{\mathbb{F}}_p}(E) = B_p := (-1, -p|\mathbb{Q})$ where $B_p = \mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{ij}$ where $\mathbf{i}^2 = -1$ and $\mathbf{j}^2 = -p$.

Remark 1. The isogeny defect $m_\psi = 1$ if and only if ψ is induced by an isogeny, see [Kan19, Remark 21]. Since we are interested in the product surface $\mathcal{A} = E_1 \times E_2$ where E_1 and E_2 are supersingular elliptic curves, and the fact that supersingular elliptic curves are all isogenous to each other, then the isogeny defect is $m_\psi = 1$ (also see Theorem 4).

3.1 Quintic integral quadratic forms as refined Humbert invariants

First, we will walk through the two methods available for computing the quintic refined Humbert invariant $q_{(\mathcal{A},\theta)}$ for a principally polarized superspecial abelian surface $(\mathcal{A}, \theta)$ where $\mathcal{A} = E_1 \times E_2$ for supersingular elliptic curves E_1 and E_2.

Recall from 5 that all superspecial abelian surfaces over a field of characteristic p are isomorphic if we ignore polarizations. Therefore, any principally polarized superspecial abelian surface $(\mathcal{A}, \lambda_\mathcal{A})$ is isomorphic to some fixed superspecial surface $\mathcal{A}_0 = E \times E$ equipped with a suitable principal polarization $\lambda_{\mathcal{A}_0}$. Explicitly, if $\vartheta : \mathcal{A}_0 \to \mathcal{A}$ is an unpolarized isomorphism, then we can take $\lambda_0 = \hat{\vartheta}\,\lambda_\mathcal{A}\,\vartheta$. A construction of Ibukiyama–Katsura–Oort [IKO86] encodes a principal polarization λ_0 on $\mathcal{A}_0$ by a matrix with coefficients in $\mathcal{O}_0$. Consider the map

$$\begin{aligned} \Upsilon : \mathcal{P}(E \times E) &\longrightarrow \mathrm{End}(\mathcal{A}_0) \\ \lambda_\mathcal{A} &\longmapsto \lambda_0^{-1}\lambda_\mathcal{A}, \end{aligned}$$

note that $\lambda_0^{-1}\lambda_\mathcal{A}$ may be viewed as an element of $M_2(\mathcal{O}_0)$. By specializing [IKO86, Corollary 2.9] to principal polarizations, the map Υ is injective. After translating it with the Deuring correspondence to the quaternion setting, we can define the set of polarizations, and its image is exactly the set

$$\mathrm{Pol}(\mathcal{A}_0) := \left\{ \begin{pmatrix} u & \alpha \\ \overline{\alpha} & v \end{pmatrix} \;\middle|\; u, v \in \mathbb{Z}_{>0},\ r \in \mathcal{O}_0,\ uv - \alpha\overline{\alpha} = 1 \right\} \subset \mathrm{GL}_2(\mathcal{O}_0).$$

Equivalently, Υ gives a bijection between $\mathcal{P}(E \times E)$ and $\mathrm{Pol}(\mathcal{A}_0)$.

Now, we fix our convention throughout the rest of the computations[5]. For $p \equiv 11 \pmod{12}$ and $B_p = (-1, -p|\mathbb{Q})$, we can fix $\mathcal{O} = \mathbb{Z}\langle 1, \beta_1, \beta_2, \beta_3\rangle = \mathbb{Z}\left\langle 1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{j}}{2}, \frac{1+\mathbf{ij}}{2} \right\rangle \cong \mathrm{End}(E)$, where $j(E) = 1728$. Then choosing $\alpha_0 = w_0 + x_0\beta_1 + y_0\beta_2 + z_0\beta_3 \in \mathcal{O}$, we get the integral quadratic form

$$g(w_0, x_0, y_0, z_0) = \mathrm{nrd}(\alpha_0) = w_0^2 + w_0 z_0 + x_0^2 + x_0 y_0 + \frac{p+1}{4} y_0^2 + \frac{p+1}{4} z_0^2, \tag{12}$$

such that $\det(g) = \det \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & \frac{p+1}{2} & 0 \\ 1 & 0 & 0 & \frac{p+1}{2} \end{pmatrix} = p^2$. We walk through the method for computing the quintic refined Humbert invariant, summarized in Algorithm 1.

1. Fix the principal polarization θ on the abelian surface $E \times E$ represented by a positive definite hermitian matrix of determinant 1

$$\theta := \begin{pmatrix} u_0 & w_0 + x_0\bar{\beta}_1 + y_0\bar{\beta}_2 + z_0\bar{\beta}_3 \\ w_0 + x_0\beta_1 + y_0\beta_2 + z_0\beta_3 & v_0 \end{pmatrix} = \begin{pmatrix} u_0 & \alpha_0 \\ \overline{\alpha}_0 & v_0 \end{pmatrix}$$

[5] In this computation, any maximal order of B_p can be chosen, and the computation can be modified with respect to the maximal order.

for fixed values of u_0, v_0 and $\alpha_0 \coloneqq w_0 + x_0\beta_1 + y_0\beta_2 + z_0\beta_3 \in \mathcal{O}$ such that $u_0 > 0$, $v_0 > 0$, and $u_0v_0 - \mathrm{nrd}(\alpha_0) = 1$, i.e. $u_0v_0 - w_0^2 - w_0z_0 - x_0^2 - x_0y_0 - \frac{p+1}{4}y_0^2 - \frac{p+1}{4}z_0^2 = 1$ (i.e. self-intersection number of θ is 2).

2. Choose an arbitrary divisor D on $E \times E$

$$D \coloneqq \begin{pmatrix} u & w + x\beta_1 + y\beta_2 + z\beta_3 \\ w + x\bar{\beta}_1 + y\bar{\beta}_2 + z\bar{\beta}_3 & v \end{pmatrix} \in \mathrm{NS}(E \times E) \subseteq M_2(\mathcal{O})$$

for $u, v, w, x, y, z \in \mathbb{Z}$. Note that

$$w + x\beta_1 + y\beta_2 + z\beta_3 = \left(w + \frac{z}{2}\right) + \left(x + \frac{y}{2}\right)\mathbf{i} + \frac{y}{2}\mathbf{j} + \frac{z}{2}\mathbf{ij}.$$

3. Compute the intersection of the divisors θ and D

$$\begin{aligned}(D \cdot \theta) &= v_0u + u_0v + 2\left(p\frac{z_0z}{4} - \left(w_0 + \frac{z_0}{2}\right)\left(w + \frac{z}{2}\right) - \left(x_0 + \frac{y_0}{2}\right)\left(x + \frac{y}{2}\right) - p\frac{y_0y}{4}\right) \\ &= v_0u + u_0v - (2w_0 + z_0)w - (2x_0 + y_0)x - \left(x_0 + \frac{y_0(p+1)}{2}\right)y - \left(w_0 - \frac{z_0(p-1)}{2}\right)z,\end{aligned}$$

$$\begin{aligned}(D \cdot \theta)^2 = {} & v_0^2u^2 + 2u_0v_0uv - (4v_0w_0 + 2v_0z_0)uw - (4v_0x_0 + 2v_0y_0)ux - (2v_0x_0 + v_0y_0p + v_0y_0)uy + (v_0z_0p - 2v_0w_0 - v_0z_0)uz \\ & + u_0^2v^2 - (4u_0w_0 + 2u_0z_0)vw - (4u_0x_0 + 2u_0y_0)vx - (2u_0x_0 + u_0y_0p + u_0y_0)vy + (u_0z_0p - 2u_0w_0 - u_0z_0)vz \\ & + (4w_0^2 + 4w_0z_0 + z_0^2)w^2 + (8w_0x_0 + 4w_0y_0 + 4x_0z_0 + 2y_0z_0)wx + (4w_0x_0 + 2w_0y_0p + 2w_0y_0 + 2x_0z_0 + y_0z_0p + y_0z_0)wy + (4w_0^2 - 2w_0z_0p + 4w_0z_0 - z_0^2p + z_0^2)wz \\ & + (4x_0^2 + 4x_0y_0 + y_0^2)x^2 + (4x_0^2 + 2x_0y_0p + 4x_0y_0 + y_0^2p + y_0^2)xy + (4w_0x_0 + 2w_0y_0 - 2x_0z_0p + 2x_0z_0 - y_0z_0p + y_0z_0)xz \\ & + (x_0^2 + x_0y_0p + x_0y_0 + \tfrac{1}{4}y_0^2p^2 + \tfrac{1}{2}y_0^2p + \tfrac{1}{4}y_0^2)y^2 + (2w_0x_0 + w_0y_0p + w_0y_0 - x_0z_0p + x_0z_0 - \tfrac{1}{2}y_0z_0p^2 + \tfrac{1}{2}y_0z_0)yz \\ & + (w_0^2 - w_0z_0p + w_0z_0 + \frac{1}{4}z_0^2p^2 - \frac{1}{2}z_0^2p + \frac{1}{4}z_0^2)z^2.\end{aligned}$$

4. Compute the self-intersection of the divisor D

$$(D \cdot D) = 2\left(uv - wz - xy - w^2 - x^2\right) - \frac{(p+1)}{2}(z^2 + y^2).$$

5. Compute $\tilde{q}_{(E\times E,\theta)}(D) = (D \cdot \theta)^2 - 2(D \cdot D)$

$$\begin{aligned}\tilde{q}_{(E\times E,\theta)}(D) = {} & v_0^2u^2 + (2u_0v_0 - 4)uv + (-4v_0w_0 - 2v_0z_0)uw + (-4v_0x_0 - 2v_0y_0)ux + (-2v_0x_0 - v_0y_0p - v_0y_0)uy + (-2v_0w_0 + v_0z_0p - v_0z_0)uz \\ & + u_0^2v^2 + (-4u_0w_0 - 2u_0z_0)vw + (-4u_0x_0 - 2u_0y_0)vx + (-2u_0x_0 - u_0y_0p - u_0y_0)vy + (-2u_0w_0 + u_0z_0p - u_0z_0)vz \\ & + (4w_0^2 + 4w_0z_0 + z_0^2 + 4)w^2 + (8w_0x_0 + 4w_0y_0 + 4x_0z_0 + 2y_0z_0)wx + (4w_0x_0 + 2w_0y_0p + 2w_0y_0 + 2x_0z_0 + y_0z_0p + y_0z_0)wy + (4w_0^2 - 2w_0z_0p + 4w_0z_0 - z_0^2p + z_0^2 + 4)wz \\ & + (4x_0^2 + 4x_0y_0 + y_0^2 + 4)x^2 + (4x_0^2 + 2x_0y_0p + 4x_0y_0 + y_0^2p + y_0^2 + 4)xy + (4w_0x_0 + 2w_0y_0 - 2x_0z_0p + 2x_0z_0 - y_0z_0p + y_0z_0)xz \\ & + (x_0^2 + x_0y_0p + x_0y_0 + \tfrac{1}{4}y_0^2p^2 + \tfrac{1}{2}y_0^2p + \tfrac{1}{4}y_0^2 + p + 1)y^2 + (2w_0x_0 + w_0y_0p + w_0y_0 - x_0z_0p + x_0z_0 - \tfrac{1}{2}y_0z_0p^2 + \tfrac{1}{2}y_0z_0)yz \\ & + (w_0^2 - w_0z_0p + w_0z_0 + \frac{1}{4}z_0^2p^2 - \frac{1}{2}z_0^2p + \frac{1}{4}z_0^2 + p + 1)z^2 \\ \coloneqq {} & \frac{1}{2}X^tAX\end{aligned}$$

where $X = \begin{pmatrix} u \\ v \\ w \\ x \\ y \\ z \end{pmatrix}$ and A is the coefficient matrix given by

$$A = \begin{pmatrix} 2v_0^2 & 2u_0v_0 - 4 & -4v_0w_0 - 2v_0z_0 & -4v_0x_0 - 2v_0y_0 & -2v_0x_0 - v_0y_0p - v_0y_0 & -2v_0w_0 + v_0z_0p - v_0z_0 \\ 2u_0v_0 - 4 & 2u_0^2 & -4u_0w_0 - 2u_0z_0 & -4u_0x_0 - 2u_0y_0 & -2u_0x_0 - u_0y_0p - u_0y_0 & -2u_0w_0 + u_0z_0p - u_0z_0 \\ -4v_0w_0 - 2v_0z_0 & -4u_0w_0 - 2u_0z_0 & 8w_0^2 + 8w_0z_0 + 2z_0^2 + 8 & 8w_0x_0 + 4w_0y_0 + 4x_0z_0 + 2y_0z_0 & 4w_0x_0 + 2w_0y_0p + 2w_0y_0 + 2x_0z_0 + y_0z_0p + y_0z_0 & 4w_0^2 - 2w_0z_0p + 4w_0z_0 - z_0^2p + z_0^2 + 4 \\ -4v_0x_0 - 2v_0y_0 & -4u_0x_0 - 2u_0y_0 & 8w_0x_0 + 4w_0y_0 + 4x_0z_0 + 2y_0z_0 & 8x_0^2 + 8x_0y_0 + 2y_0^2 + 8 & 4x_0^2 + 2x_0y_0p + 4x_0y_0 + y_0^2p + y_0^2 + 4 & 4w_0x_0 + 2w_0y_0 - 2x_0z_0p + 2x_0z_0 - y_0z_0p + y_0z_0 \\ -2v_0x_0 - v_0y_0p - v_0y_0 & -2u_0x_0 - u_0y_0p - u_0y_0 & 4w_0x_0 + 2w_0y_0p + 2w_0y_0 + \frac{1}{2}y_0^2p + \frac{1}{2}y_0^2 + 2p + 2 & 4x_0^2 + 2x_0y_0p + 4x_0y_0 + y_0^2p + \frac{1}{2}y_0^2 + 2p + 2 & 2x_0^2 + 2x_0y_0p + 2x_0y_0 + \frac{1}{2}y_0^2p^2 + y_0^2p + \frac{1}{2}y_0^2 + 2p + 2 & 2w_0x_0 + w_0y_0p + w_0y_0 - x_0z_0p + x_0z_0 - \frac{1}{2}y_0z_0p^2 + \frac{1}{2}y_0z_0 \\ -2v_0w_0 + v_0z_0p - v_0z_0 & -2u_0w_0 + u_0z_0p - u_0z_0 & 4w_0^2 - 2w_0z_0p + 4w_0z_0 - z_0^2p + z_0^2 + 4 & 4w_0x_0 + 2w_0y_0p - 2x_0z_0p + 2x_0z_0 - y_0z_0p + y_0z_0 & 2w_0x_0 + w_0y_0p + w_0y_0 - x_0z_0p + x_0z_0 - \frac{1}{2}y_0z_0p^2 + \frac{1}{2}y_0z_0 & 2w_0^2 - 2w_0z_0p + 2w_0z_0 + \frac{1}{2}z_0^2p^2 - z_0^2p + \frac{1}{2}z_0^2 + 2p + 2 \end{pmatrix} \tag{13}$$

with $\det(A) = 2^{10}p^2\left(u_0v_0 - \mathrm{nrd}(\alpha_0) - 1\right) = 0$.

6. Find a 6×5 matrix T whose entries are integers such that the GCD of its 5×5 minors is 1 and T^tAT is the coefficient matrix of the positive-definite quintic form (refined Humbert invariant $q_{(E_1 \times E_2, \theta)}$)

$$q_{(E\times E,\theta)}(D) = \frac{1}{2}\begin{pmatrix} t_0 & t_1 & t_2 & t_3 & t_4 \end{pmatrix}(T^tAT)\begin{pmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix}.$$

Moreover, since the Picard number $\rho(\mathcal{A}) = 6$, using Propositon 1 we get

$$\det(T^tAT) = \frac{1}{2}(-4)^{\rho-1}\det(q_{E\times E}) = \frac{1}{2}(-4)^{6-1}(-p^2) = 2^9p^2 \tag{14}$$

where the intersection form $q_{\mathcal{A}} = q_{E\times E} = \frac{1}{2}(D \cdot D) = uv - wz - xy - w^2 - x^2 - \frac{(p+1)}{4}(z^2 + y^2)$.

We observe that $\tilde{q}_{(E\times E,\theta)}$ above is a positive semi-definite form and applying[6] Simon's indefiniteLLL[7] algorithm [Sim05, Wat13] quickly gives us positive definite quintic form $q_{(E\times E,\theta)}$. Moreover, we can ensure with the irreducibility criterion, Proposition 2 above, that the quintic form we obtained corresponds to a superspecial abelian surface $\mathcal{A} = E \times E$ over $\overline{\mathbb{F}}_p$ with a reducible principal polarization $\theta \in \mathcal{P}^{\text{red}}(E \times E)$ by using Kannan-Fincke-Pohst minVector[8] algorithm [Kan83, FE85, PS08] to check that 1 is the minimum value it represents. Therefore, Algorithm 1 below lets us compute the quintic refined Humbert invariants for principally polarized superspecial abelian surfaces.

Algorithm 1: RHI(p, θ)

Input: odd prime $p \equiv 11 \pmod{12}$ such that $B_p = (-1, -p|\mathbb{Q})$ and polarization $\theta = \left(\begin{smallmatrix} u_0 & \alpha_0 \\ \overline{\alpha}_0 & v_0 \end{smallmatrix}\right)$ where $\alpha_0 := w_0 + x_0\beta_1 + y_0\beta_2 + z_0\beta_3 \in \mathbb{Z} + \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 + \mathbb{Z}\beta_3$.
Output: coefficient matrix of quintic refined Humbert invariant $q_{(E\times E,\theta)}$.

$A \leftarrow$ the 6×6 matrix as in (13);
// the coefficient matrix of $\tilde{q}_{(A,\theta)}$ with $\det(A) = 2^{10}p^2\,(u_0v_0 - \text{nrd}(\alpha_0) - 1) = 0$
$A' \leftarrow$ indefiniteLLL(A);
// A is 6×6 positive semi-definite; A' is 5×5 positive definite.
if $\det(A') = 2^9p^2$ **then**
    // Proposition 1 for $\rho = 6$ and $\det(q_A) = -p^2$
    $L \leftarrow$ integer lattice with Gram matrix $A'/2$;
    if minVector$(L) = 1$ **then**
        // Proposition 2 and [FE85, §2]
        return A';
return 0;

Remark 2. For $\theta = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ we get $T = \begin{pmatrix} 0&0&0&0&0 \\ 1&0&0&0&0 \\ 0&0&1&0&0 \\ 0&1&0&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \end{pmatrix}$, such that $\det(T^tAT) = 2^9p^2$, leading to

$$q_5(t_0,t_1,t_2,t_3,t_4) := q_{(E\times E,\theta)}(D) = t_0^2 + 4\left(t_1^2 + t_1t_3 + t_2^2 + t_2t_4 + \frac{p+1}{4}t_3^2 + \frac{p+1}{4}t_4^2\right).$$

[6] Ours is a very special case: https://github.com/Nemocas/Nemo.jl/pull/2011.
[7] https://github.com/thofma/Hecke.jl/blob/master/src/QuadForm/indefiniteLLL.jl
[8] https://github.com/thofma/Hecke.jl/blob/master/src/QuadForm/Enumeration.jl

Note that $q_{(E\times E,\theta)}$ satisfies the reducibility condition stated in (2). Therefore, as per Lemma 2, the degree map (degree form) is

$$q_4(t_1,t_2,t_3,t_4) := q_{E,E} = t_1^2 + t_1t_3 + t_2^2 + t_2t_4 + \frac{p+1}{4}t_3^2 + \frac{p+1}{4}t_4^2 \tag{15}$$

that matches the norm form given in (12). By Proposition 4, $\mathrm{Gen}(q_4)$ contains all unique degree forms and leads to all unique reducible refined Humbert invariants. It is computed via Kneser's neighbor method[9] [Kne57, Kir16, Voi23].

3.2 Principal polarizations

We aim to determine all possible quintic refined Humbert invariants that are not equivalent. However, two distinct principal polarizations can lead to the same quintic refined Humbert invariant. Indeed, we verified that for a given prime p, there are examples of principally polarized abelian superspecial surfaces $(\mathcal{A},\theta)$ and $(\mathcal{A}',\theta')$ leading to the equivalent refined Humbert invariants $q_{(\mathcal{A},\theta)} \sim q_{(\mathcal{A}',\theta')}$ in the experiments by using the count in Proposition 4.

We fix the definite quaternion algebra $B_p = (-1,-p|\mathbb{Q})$ and $p \equiv 11 \pmod{12}$, and a maximal order $\mathcal{O} \subset B_p$ with a chosen $\mathbb{Z}$-basis $\{1,\beta_1,\beta_2,\beta_3\}$. A principal polarization on a superspecial surface corresponds to a positive-definite unimodular Hermitian matrix (11), and we enumerate these matrices up to congruence. One can get all product polarizations $\left(\begin{smallmatrix} u_0 & \alpha_0 \\ \overline{\alpha_0} & v_0 \end{smallmatrix}\right)$ by varying $u_0,v_0 \in \mathbb{Z}_{>0}$ and taking $\alpha_0 = w_0 + x_0\beta_1 + y_0\beta_2 + z_0\beta_3 \in \mathbb{Z}\langle 1,\beta_1,\beta_2,\beta_3\rangle$ such that $0 \le w_0,x_0,y_0,z_0 \le v_0 - 1$ and $\mathrm{nrd}(w_0 + x_0\beta_1 + y_0\beta_2 + z_0\beta_3) = u_0v_0 - 1$. We start with eliminating easy isomorphic polarizations by Lemma 3.

We first recall some basics of quaternion hermitian forms from [Shi63]. Viewing B_p^2 as a left vector space over B_p, the *binary definite quaternion Hermitian form* on B_p^2 is defined as the unique form up to isometry, and explicitly given by $h(x,y) = \sum_{i=1}^{2} x_i\overline{y_i} = x_1\overline{y_1} + x_2\overline{y_2}$, for vectors $x = (x_1,x_2), y = (y_1,y_2) \in B_p^2$ where $\overline{\ }$ is the canonical involution of B_p.

The enumeration of principal polarizations on a superspecial abelian surface in Algorithm 2 relies on the following criterion for determining whether two principal polarizations are isomorphic. The method is adapted from Chisholm's PhD thesis [Chi14, §3.8.1], itself based on [GV14, Lemma 6.2] of Greenberg and Voight, specialized to a maximal order $\mathcal{O} \subset B_p$. Let h_θ be the quaternion binary Hermitian form associated with a principal polarization θ on $\mathcal{O}^2 \cong \mathbb{Z}^8$, and fix a $\mathbb{Q}$-basis $\{a_1,\ldots,a_4\}$ of B_p. Now, we define the associated integral trace forms in 8 variables by

$$F_i(x,y) = \mathrm{trd}(a_i h_\theta(x,y)) \text{ for } i = 1,\ldots,4. \tag{16}$$

Two principal polarizations θ and θ' are isomorphic if and only if their associated 4-tuples (F_1,F_2,F_3,F_4) and (F_1',F_2',F_3',F_4') of auxiliary trace forms are simultaneously isometric, that is, if there exists a $P \in \mathrm{GL}_8(\mathbb{Z})$ carrying each F_i to the corresponding trace form of the other polarization. This is the simultaneous-isometry criterion in [GV14, Lemma 6.2], which controls the $\mathcal{O}$-module structure. Therefore, Algorithm 2 below gives us a finite list of principal polarizations that will lead to an input θ to $\tilde{q}_{(E\times E,\theta)}$ given in (7).

3.3 Counting distinct forms

Knowing the expected number of unique (non-isometric) refined Humbert invariants will significantly improve the runtime of Algorithm 3 since it will allow us to stop computing new refined Humbert invariants once the target number of non-isometric quintic integral quadratic forms is found. Therefore, here we discuss our attempt to get a bound on this number.

[9] https://github.com/thofma/Hecke.jl/blob/master/src/QuadForm/Quad/GenusRep.jl

Algorithm 2: $\mathsf{polz}(p, V_{\max}, U_{\max}, T_{\max})$

Input: prime $p \equiv 11 \pmod{12}$; bounds $V_{\max}, U_{\max} \in \mathbb{Z}_{>0}$; theta coefficients cutoff $T_{\max} \in \mathbb{Z}_{>0}$.

Output: A list Reps of representatives of principal polarizations on $\mathcal{A} = E \times E$ up to equivalence, where $\theta = \left(\begin{smallmatrix} u & \alpha \\ \overline{\alpha} & v \end{smallmatrix}\right)$ with $u, v > 0$, $\alpha \in \mathcal{O}$, and $uv - \mathrm{nrd}(\alpha) = 1$.

```
Reps ← [];
Packets ← [];
Keys ← [];
for v ← 1 to V_max do
    foreach α' ∈ O/vO with nrd(α') ≡ −1 (mod v) do
        α ← ChooseLift(α', v);
        u ← (nrd(α) + 1)/v;
        if 0 < u ≤ U_max then
            θ ← (u, α; ᾱ, v);
            for i ← 1 to 4 do
                F_i ← AuxiliaryTraceGram(θ, a_i);
            (F'_1, P) ← LLLGramWithTransform(F_1);
            for i ← 2 to 4 do
                F'_i ← P F_i P^t;
            F'_θ ← (F'_1, F'_2, F'_3, F'_4);
            key ←
              (LocalGenus_{2,p}(F'_1), ThetaSeriesInitials(F'_1, T_max), min(F'_1), κ(F'_1));
            isNew ← true;
            for j ← 1 to |Packets| do
                if key = Keys[j] then
                    if ExactIsometric(F'_1, (Packets[j])_1) then
                        if ExactSimultaneousIsometric(F'_θ, Packets[j]) then
                            isNew ← false;
                            break;
            if isNew then
                append θ to Reps;
                append F'_θ to Packets;
                append key to Keys;
return Reps;
```

When $\mathcal{A}$ is a supersingular elliptic curve, Deuring showed that $\mathcal{A}$ has a model defined over $\overline{\mathbb{F}}_p$ and the class number $\mathbf{h}$ of $\mathrm{End}(\mathcal{A})$ is calculated by Eichler [Eic38], Deuring [Deu41], and Igusa [Igu58] as

$$\mathbf{h} = \frac{p-1}{12} + \frac{1}{4}\left(1 - \left(\frac{-1}{p}\right)\right) + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right). \tag{17}$$

The calculation of the number of isomorphism classes of principal polarizations on an abelian surface $\mathcal{A}$, especially the number of isomorphism classes of smooth genus 2 curves lying on $\mathcal{A}$, was calculated by Ibukiyama, Katsura, and Oort [IKO86] in 1986 when $\mathcal{A} = E \times E'$, where E and E' are supersingular elliptic curves.

Theorem 6. [IKO86, Theorem 2.10] *Let B_p^2 be a left B_p-vector space. The number of*

principal polarizations on $\mathcal{A} = E \times E$ up to automorphisms of $\mathcal{A}$ is equal to the class number $\mathbf{H}$ *of the principal genus of the quaternion Hermitian space* B_p^2.

Hashimoto and Ibukiyama [HI80, p. 1] gave a formula for $\mathbf{H}$. Later, Katsura and Oort gave [KO87, Theorem 3.3] simpler version of the formula for $\mathbf{H}$ as follows:

$$\begin{aligned}\mathbf{H} = &\frac{(p-1)(p+12)(p+23)}{2880} + \frac{2p+13}{96}\left(1-\left(\frac{-1}{p}\right)\right) + \frac{p+11}{36}\left(1-\left(\frac{-3}{p}\right)\right) \\ &+ \frac{1}{8}\left(1-\left(\frac{-2}{p}\right)\right) + \frac{1}{12}\left(1-\left(\frac{-3}{p}\right)\right)\left(1-\left(\frac{-1}{p}\right)\right) \\ &+ \begin{cases} 0 & p \equiv 1,2,3 \pmod 5 \\ \frac{4}{5} & p \equiv 4 \pmod 5. \end{cases}\end{aligned} \tag{18}$$

Neither $\mathbf{H}$ nor $\frac{\mathbf{h}(\mathbf{h}+\mathbf{1})}{\mathbf{2}}$ is an asymptotically tight bound for the number of unique refined Humbert invariants (up to isometry). The $\mathbf{H}$ serves as an upper bound on the number of all quintic refined Humbert invariants of a superspecial surface, while $\frac{\mathbf{h}(\mathbf{h}+\mathbf{1})}{\mathbf{2}}$ is an upper bound on the refined Humbert invariants constructed with reducible polarizations; Definition 7. If we take two supersingular product surfaces $\mathcal{A} = E_1 \times E_2$ and $\mathcal{A}' = E_1' \times E_2'$, then notice that two different principally polarized superspecial product abelian surfaces $(\mathcal{A}, \theta)$ and $(\mathcal{A}', \theta')$ can have the same refined Humbert invariants $q_{(\mathcal{A},\theta)} \sim q_{(\mathcal{A}',\theta')}$ (up to equivalence). This means that the number of principally polarized superspecial abelian surfaces over K is not equal to the number of refined Humbert invariants.

Algorithm 3 combines Algorithms 2 and 1 into a single pipeline. The first step calls $\mathsf{dynamicPolz}(p)$, which executes Algorithm 2 with a single bound $A_{\max}$ in place of the separate bounds $V_{\max}$ and $U_{\max}$, with $T_{\max}$ fixed at a small constant, growing $A_{\max}$ in stages until the stopping condition of total $|\mathrm{Reps}| = \mathbf{H}$ is met. We conjecture that $A_{\max} = O(p)$ at termination. The resulting list Θ of all $\mathbf{H}$ principal polarizations is then passed to Algorithm 1 once per polarization.

Of the $\mathbf{H}$ calls to $\mathsf{RHI}(p, \theta)$, only $\mathbf{h}(\mathbf{h}+1)/2$ return a non-zero output, where $\mathbf{h}$ is given by (17). These correspond to the refined Humbert invariants with reducible polarizations. For each non-zero output A, Algorithm 3 applies a two-step uniqueness check. First, it tests exact matrix equality $A = A'$ against every $A' \in Q$. If that fails, it constructs the integer lattices L_A and $L_{A'}$ with Gram matrices $A/2$ and $A'/2$ respectively, and calls $\mathsf{isIsometric}(L_A, L_{A'})$ via the Plesken–Souvignier algorithm[10] [PS97]. The list Q at termination collects all refined Humbert invariants with reducible polarizations up to isometry, and by Remark 2, $|Q|$ equals the number of genera of q_4 defined in (15).

3.4 Complexity analysis

We analyze the runtime and space complexity of Algorithms 2, 1, and 3 in the order in which Algorithm 3 invokes them. Analyzing Algorithms 2 and 1 first establishes the costs that feed directly into the analysis of Algorithm 3.

The implementation of Algorithm 2 departs from the pseudocode in three ways that affect complexity. First, the separate bounds $V_{\max}$ and $U_{\max}$ are collapsed into a single bound $A_{\max}$, since every candidate is normalized to $u \le v$, so bounding $v \le A_{\max}$ automatically bounds u. Second, rather than iterating over residue classes $\alpha' \in \mathcal{O}/v\mathcal{O}$ with a $\mathsf{ChooseLift}$ step 6, the implementation iterates directly over the order elements of exact reduced norm $N = uv - 1$ per (u, v) pair, selecting one representative per equivalence class under $\alpha \sim \beta\alpha\beta'$ for $\beta, \beta' \in \mathcal{O}^\times$, as given by Lemma 3(ii). Third, with $T_{\max} = 6$ fixed, all theta-series computations cost $O(T_{\max}^4) = O(1)$ per candidate. In practice, Algorithm 2 is executed as $\mathsf{dynamicPolz}$. Under the conjecture $A_{\max} = O(p)$, the largest reduced norm

[10] https://github.com/thofma/Hecke.jl/blob/master/src/QuadForm/Morphism.jl

Algorithm 3: allRHI(p)

Input: odd prime $p \equiv 11 \pmod{12}$ such that $B_p = (-1, -p|\mathbb{Q})$.
Output: coefficient matrices of all unique refined Humbert invariants for polarizations $\theta = \left(\begin{smallmatrix} u & \alpha_0 \\ \overline{\alpha}_0 & v \end{smallmatrix}\right)$.

$Q \leftarrow$ [];
// initialize the list of unique refined Humbert invariants
$\Theta \leftarrow$ dynamicPolz(p);
// running Algorithm 2 for various choices of parameters until **H** polarizations are obtained
foreach $\theta \in \Theta$ **do**
    $A \leftarrow$ RHI(p, θ);
    // running Algorithm 1 for each polarization
    if $A \neq 0$ **then**
        $s \leftarrow$ true;
        // assume unique
        foreach $A' \in Q$ **do**
            if $A = A'$ **then**
                $s \leftarrow$ false;
                // not unique
                break;
        $L_A \leftarrow$ integer lattice with Gram matrix $A/2$;
        if $s =$ true **then**
            foreach $A' \in Q$ **do**
                $L_{A'} \leftarrow$ integer lattice with Gram matrix $A'/2$;
                if isIsometric($L_A, L_{A'}$) = true **then**
                    $s \leftarrow$ false;
                    // not unique
                    break;
        if $s =$ true **then**
            Q.append(A);
return Q;

arising at termination is $N \leq A_{\max}^2 - 1 = O(p^2)$, and the total number of principal candidates, with results at each (u, v) pair cached so no work is repeated across stages, is

$$C = \sum_{1 \leq u \leq v \leq A_{\max}} O(uv) = O(A_{\max}^4) = O(p^4).$$

The dominant cost is enumerating all $\alpha \in \mathcal{O}$ with $\mathrm{nrd}(\alpha) = N = uv - 1$ for each (u, v) pair, carried out via the Fincke–Pohst algorithm [FE85] applied to a rank-4 integral quadratic form encoding twice the reduced norm on $\mathcal{O}$. In the integral basis of $\mathcal{O}$ in $B_p = (-1, -p|\mathbb{Q})$, two of the four coordinate directions of this form are scaled by $q_0 = (p+1)/4$, which is an integer since $p \equiv 11 \pmod{12}$ implies $p \equiv 3 \pmod{4}$. The Fincke–Pohst algorithm exploits this through its Cholesky preprocessing: those two directions have true extent $O(\sqrt{N/q_0})$ rather than $O(\sqrt{N})$, reducing the node count per (u, v) pair from the naive $O(N^2)$ of a brute-force scan to $O(N^2/q_0) = O(N^2/p)$. Summing

over all distinct norms N, each enumerated at most once by caching,

$$T_{\text{norms}} = \sum_{N=1}^{O(p^2)} O\left(\frac{N^2}{p}\right) = O(p^5).$$

The remaining per-candidate costs are subordinate. LLL reduction of the auxiliary form F_1 uses the Nguyen–Stehlé algorithm [NS09] on a fixed-rank Gram matrix with $O(\log p)$-bit entries, costing $O(\log p)$ per candidate and $O(p^4 \log p)$ in total. Computing the invariant key, consisting of local genus symbols at $\{2, p\}$ via Jordan decomposition, theta-series initials, minimum, and kissing number κ, costs $O(\log p)$ per candidate and $O(p^4 \log p)$ in total [CS99]. The exact isometry test via the Plesken–Souvignier algorithm [PS97] is called only between key-matching candidates, and since the invariant key separates almost all non-isometric pairs, the aggregate isometry cost is empirically $O(p^4)$. The overall expected runtime of dynamicPolz under the conjecture $A_{\max} = O(p)$ stated above is therefore $O(p^5)$, dominated by Fincke–Pohst enumeration, with space complexity $O(p^4)$ to store all candidates and their auxiliary forms across stages.

Algorithm 1 takes a fixed prime p and a single polarization θ as input, so all costs below are per-call. The first step constructs the 6×6 positive semi-definite matrix A over $\mathbb{Q}$, whose entries are polynomial in the polarization parameters $(u_0, v_0, w_0, x_0, y_0, z_0)$ and p. Under the conjecture $A_{\max} = O(p)$, we have $u_0, v_0 = O(p)$, and the principal condition $u_0 v_0 - \text{nrd}(\alpha_0) = 1$ forces $y_0, z_0 = O(\sqrt{p})$ and $w_0, x_0 = O(p)$, so the largest entries of A scale as $O(p^2)$ and carry $O(\log p)$ bits each. Assembly of A costs $O(\log p)$.

Since A has rank 5, Simon's indefiniteLLL [Sim05, Wat13] reduces $A/2$ to a form whose sixth row and column vanish, and A' is the top-left 5×5 positive definite submatrix of the result. The input is a rank-6 Gram matrix with $O(\log p)$-bit entries, so indefiniteLLL runs in $O(\log p)$ by the standard LLL complexity analysis. The output A' satisfies $\det(A') = 2^9 p^2$, with entries scaling as $O(p)$. The integer lattice L with Gram matrix $A'/2$ is then a rank-5 positive definite lattice with $\det(L) = O(p^2)$. minVector(L) is computed via the Fincke–Pohst algorithm with Cholesky preprocessing, as in [FE85, §2]. By the LLL–Minkowski bound, the minimum of L is at most $O(p^{4/5})$, and the Fincke–Pohst node count for a rank-5 lattice at this bound is $O\left((p^{4/5})^{5/2}/\sqrt{\det(L)}\right) = O(p)$. All other per-call costs are $O(\log p)$ or smaller. The per-call runtime of Algorithm 1 is therefore $O(p)$, dominated by the Fincke–Pohst minimum computation, with space complexity $O(1)$ as all matrices are of fixed size and no caches are maintained.

Algorithm 3 proceeds in two phases as described above. The first phase runs dynamicPolz(p) at a cost of $O(p^5)$ as established above. The second phase iterates over the resulting list Θ of $\mathbf{H}$ polarizations. The leading term of $\mathbf{H}$ is $(p-1)(p+12)(p+23)/2880$, so $|\Theta| = O(p^3)$. For each $\theta \in \Theta$, one call to RHI(p, θ) costs $O(p)$ as established above, giving a total cost of $O(p^4)$ for all RHI calls. Of these, $\mathbf{h}(\mathbf{h}+1)/2 = O(p^2)$ return a non-zero output, and the remaining $\mathbf{H} - \mathbf{h}(\mathbf{h}+1)/2 = O(p^3)$ calls return 0 and contribute no further cost.

For each non-zero output A, exact matrix equality tests against every $A' \in Q$ cost $O(1)$ per test since A and A' are fixed-size 5×5 integer matrices, giving a total exact-equality cost of $O(p^2 \cdot |Q|)$ over all non-zero outputs. If exact equality fails, isIsometric is called via the Plesken–Souvignier algorithm [PS97], with empirical total cost $O(p^2 \cdot |Q|)$ over all non-zero outputs. The overall runtime of Algorithm 3 is therefore $O(p^5)$, dominated by dynamicPolz, with all subsequent costs subordinate under the conjectured bounds. The space complexity is $O(p^3)$ to store Θ, plus $O(|Q|)$ for the list of unique invariants.

3.5 Experiment

We run Algorithm 3 for all primes $p \equiv 11 \pmod{12}$ with $10 < p < 660$, implemented in Julia using the `Oscar` package [The26, DEF+25] and its dependency `Nemo/Hecke` [FHHJ17]. The code and data are available at:

https://github.com/gkorpal/humbert-degree

Each run was allowed a maximum of two weeks of computation time. Table 1 records the results. Each row of Table 1 corresponds to one prime p. The column $\mathbf{H}$ is the total number of principal polarizations on $E \times E$ up to equivalence, given by the formula in (18). The column $\#\Theta$ is the number of polarizations that Algorithm 2 actually found within the time limit, so $\#\Theta \leq \mathbf{H}$ always, with equality when the computation finished. The column $\#\underset{\text{red}}{\text{RHI}}$ counts the polarizations $\theta \in \Theta$ for which Algorithm 1 returns a non-zero matrix, that is, the reducible refined Humbert invariants found. The column $\mathbf{h}(\mathbf{h}+1)/2$, where $\mathbf{h}$ is given by (17), is the conjectured total count of reducible refined Humbert invariants over all $\mathbf{H}$ polarizations. The column $\#\underset{\text{iso}}{\text{RHI}}$ is the number of isometry classes among those reducible refined Humbert invariants, found experimentally via Algorithm 3. The column $\#\text{Gen}(q_4)$ is the number of genera of the lattice q_4 defined in (15), which equals the true number of isometry classes of reducible refined Humbert invariants. Finally, d_{expt} is the value of d as defined in (1), computed from the experimental isometry classes in $\#\underset{\text{iso}}{\text{RHI}}$, and d_{gen} is the same quantity computed from the genus classes counted by $\#\text{Gen}(q_4)$.

When $\#\Theta = \mathbf{H}$, Algorithm 3 completed within the time limit and the experimental columns recover the conjectured values exactly: $\#\underset{\text{red}}{\text{RHI}}$ agrees with $\mathbf{h}(\mathbf{h}+1)/2$, $\#\underset{\text{iso}}{\text{RHI}}$ agrees with $\#\text{Gen}(q_4)$, and d_{expt} agrees with d_{gen}. When $\#\Theta < \mathbf{H}$, the computation did not finish within two weeks, and the experimental columns reflect only the polarizations found so far. In this case $\#\underset{\text{red}}{\text{RHI}} \leq \mathbf{h}(\mathbf{h}+1)/2$, $\#\underset{\text{iso}}{\text{RHI}} \leq \#\text{Gen}(q_4)$, and $d_{\text{expt}} \leq d_{\text{gen}}$, as the missing polarizations may contribute additional invariants and larger degree values.

4 Applications to isogeny problems

The efficient computation of refined Humbert invariants is an open avenue to work on a variety of isogeny problems[11]. They were first used in isogeny-based cryptography in [KM24], where their computations were shown to be equivalent to certain isogeny problems.

4.1 Testing isomorphism of two given principal polarizations

We now highlight the isomorphism test for principal polarizations used in steps 21–23 of Algorithm 2, which enumerates all principal polarizations on $\mathcal{A} = E \times E$.

For deciding the isomorphism of two principal polarizations $\theta \mapsto (F_1, F_2, F_3, F_4)$ and $\theta' \mapsto (F_1', F_2', F_3', F_4')$ as in (16), we declare that θ and θ' are equivalent if their packets are *simultaneously isometric*, i.e., if there exists a matrix $T \in \text{GL}_8(\mathbb{Z})$ such that $TF_iT^t = F_i'$ for all $i = 1, 2, 3, 4$. For computational simplicity, we replace the auxiliary trace forms (16) by their LLL-reduced forms. Since the first auxiliary form is positive definite, we first compare inexpensive isometry invariants, including the local genus, initial coefficients of the theta series, and the kissing number (κ). If any of these invariants differ, we reject the pair; otherwise, we proceed to an exact simultaneous isometry test.

4.2 Type of a principally polarized superspecial abelian surface

The geometric type of a principally polarized superspecial abelian surface can be effectively detected using its refined Humbert invariant and the irreducibility criterion, corresponding exactly to steps 5–6 of Algorithm 1.

[11] The potential advantage that we expect from a refined Humbert invariant $q_{(\mathcal{A},\theta)}$ of a principally polarized abelian surface $(\mathcal{A}, \theta)$ is that it uses the intersection theory of divisors on surfaces, see [Har77, §V.1] and [Sha13, §4.1], and only the degrees of isogenies are used rather than isogenies themselves in the intersection formulas.

Table 1: We get the following results for $\mathsf{allRHI}(p)$ for primes $p \equiv 11 \pmod{12}$ with $10 < p < 660$ and a time limit of two weeks. Further explanation in text.

p	$\#\Theta$	$\mathbf{H}$	$\#\mathrm{RHI}_{\mathrm{red}}$	$\frac{\mathbf{h}(\mathbf{h}+1)}{2}$	$\#\mathrm{RHI}_{\mathrm{iso}}$	$\#\mathrm{Gen}(q_4)$	d_{expt}	d_{gen}
11	5	5	3	3	3	3	2	2
23	16	16	6	6	6	6	3	3
47	72	72	15	15	15	15	4	4
59	125	125	21	21	21	21	5	5
71	198	198	28	28	28	28	5	5
83	296	296	36	36	29	29	6	6
107	581	581	55	55	39	39	6	6
131	1008	1008	78	78	67	67	7	7
167	1978	1978	120	120	94	94	8	8
179	2404	2404	136	136	97	97	9	9
191	2886	2886	153	153	123	123	9	9
227	4708	4712	206	210	131	135	10	10
239	5458	5460	229	231	175	177	10	10
251	6275	6281	247	253	176	181	10	10
263	7173	7182	268	276	180	186	10	11
311	11592	11644	347	378	259	286	11	12
347	15770	15993	412	465	229	265	12	12
359	17210	17654	418	496	279	346	12	12
383	20264	21310	468	561	289	361	12	13
419	24753	27692	515	666	316	423	13	14
431	25768	30072	484	703	306	471	13	14
443	27240	32585	585	741	316	405	12	13
467	29288	38024	550	820	305	469	13	14
479	29323	40958	529	861	351	597	13	15
491	2527	44037	93	903	59	543	10	14
503	31476	47268	564	946	334	594	13	15
563	33555	65808	617	1176	346	681	14	15
587	20151	74405	413	1275	229	699	13	16
599	33866	78972	594	1326	364	832	14	16
647	33331	99102	595	1540	347	916	13	16
659	33230	104620	556	1596	321	933	14	17

More precisely, the irreducibility criterion (Proposition 2) shows that $q_{(\mathcal{A},\theta)}$ represents 1 if and only if $(\mathcal{A}, \theta)$ is a product of elliptic curves with product polarization; otherwise, it is the Jacobian of a genus-2 curve with its canonical principal polarization. This efficient criterion can be incorporated into the KLPT^2 algorithm [CDK+25, PRS26] to distinguish the relevant types of principally polarized abelian surfaces[12].

4.3 Improvement on the upper bound on minimum isogeny degrees

Recall from (1) that d is the maximum of the minimum isogeny degree, taken over all pairs (E_1, E_2) of supersingular elliptic curves. Goren–Lauter [GL09] showed that this minimum degree is bounded above by $\frac{2\sqrt{2}}{\pi}\sqrt{p}$, a bound later reproved in [DLRW24, Lemma 12]. We prove a sharper bound.

[12]No direct algorithm is currently known for computing these invariants from curve equations; the criterion therefore applies only when a principal polarization is given as input.

Proposition 6. *Let E and E' be supersingular elliptic curves over $\overline{\mathbb{F}}_p$, let $\mathcal{A} = E \times E'$, let $q_{E,E'}$ be the degree map as in Definition 4, and suppose the refined Humbert invariant of $(\mathcal{A}, \theta)$ satisfies $q_{(\mathcal{A},\theta)}(x, \varphi) = x^2 + 4q_{E,E'}(\varphi)$ as in Lemma 2. Then $\min q_{E,E'}(\varphi) \leq \sqrt{\frac{p}{2}}$, where the minimum is taken over all nonzero $\varphi \in \mathrm{Hom}(E, E')$. In particular, $d \leq \sqrt{\frac{p}{2}}$.*

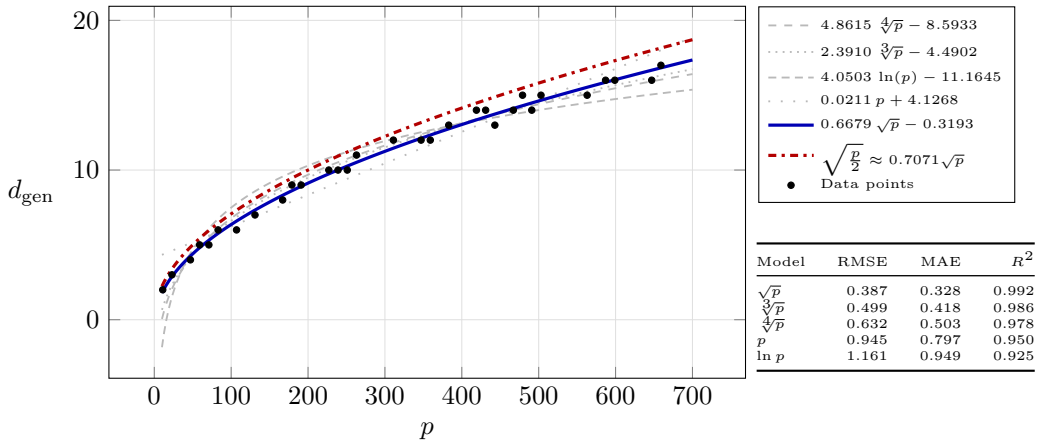
Proof. Let $L = L_{q_{(\mathcal{A},\theta)}}$ denote the rank-5 lattice associated with $q_{(\mathcal{A},\theta)}$, and let $e = (1, 0) \in \mathbb{Z} \oplus \mathrm{Hom}(E, E')$. Then $q_{(\mathcal{A},\theta)}(e) = 1$, and the decomposition $q_{(\mathcal{A},\theta)}(x, \varphi) = x^2 + 4q_{E,E'}(\varphi)$ gives an orthogonal decomposition $L = \mathbb{Z}e \perp M$, where $M = e^{\perp} \cap L$ has rank 4 and $q_{(\mathcal{A},\theta)}|_M = 4q_{E,E'}$. Since $q_{(\mathcal{A},\theta)}$ is an integral quadratic form that represents 1, it represents no smaller positive value, so $\lambda_1(L) = 1$. Every vector of L linearly independent of e has the form $ae + v$ with $a \in \mathbb{Z}$ and $0 \neq v \in M$, and by orthogonality $q_{(\mathcal{A},\theta)}(ae + v) = a^2 + q_{(\mathcal{A},\theta)}(v) \geq q_{(\mathcal{A},\theta)}(v)$.

On the other hand, every nonzero vector of M is linearly independent of e, so $\lambda_2(L) = \lambda_1(M)$. Since $q_{(\mathcal{A},\theta)}|_M = 4q_{E,E'}$, it follows that $\lambda_2(L) = \lambda_1(M) = 4 \min q_{E,E'}(\varphi)$, where the minimum is taken over all nonzero $\varphi \in \mathrm{Hom}(E, E')$. By (14), we have $\det(q_{(\mathcal{A},\theta)}) = 2^9 p^2$. The orthogonal decomposition $L = \mathbb{Z}e \perp M$ with $q_{(\mathcal{A},\theta)}(e) = 1$ then gives $\det(M) = \frac{\det(q_{\mathcal{A},\theta})}{2} \cdot 2^{-4} = 2^4 p^2$. Applying Minkowski's inequality [Mar03, Theorem 2.6.8] in dimension 4 with Hermite constant $\gamma_4 = \sqrt{2}$ [CS99, Table 3.1] gives

$$\lambda_1(M) \leq \gamma_4 \det(M)^{1/4} = \sqrt{2} \cdot (4p)^{1/2} = 2\sqrt{2p}.$$

Therefore, $4 \min q_{E,E'}(\varphi) \leq 2\sqrt{2p}$, and hence $\min q_{E,E'}(\varphi) \leq \sqrt{\frac{p}{2}}$. □

Our computational experiment verifies the proven bound. For primes $p \equiv 11 \pmod{12}$, the maximum, over all pairs of supersingular elliptic curves E_1, E_2, of the minimum degree of an isogeny between E_1 and E_2 is approximately $0.67\sqrt{p}$. We observe that $d < \sqrt{\frac{p}{2}}$, which is illustrated by the plot in Figure 1. Moreover, the computations of Goren–Lauter also support that the constant in our bound is close to optimal. Indeed, among the examples reported in [GL09, Table 1], the largest observed ratio is attained at $p = 10007$; this gives $\frac{70}{\sqrt{10007}} \approx 0.6998$, which is very close to our theoretical constant $\frac{1}{\sqrt{2}} \approx 0.7071$.



Model	RMSE	MAE	R^2
$\sqrt{p}$	0.387	0.328	0.992
$\sqrt[3]{p}$	0.499	0.418	0.986
$\sqrt[4]{p}$	0.632	0.503	0.978
p	0.945	0.797	0.950
$\ln p$	1.161	0.949	0.925

Figure 1: Visualizing the data collected in Table 1 for first 31 primes $p > 10$ and $p \equiv 11$ mod 12 and comparing with our bound in Proposition 6. Among the tested two-parameter models, the square-root form gives the best fit. Lower root mean square error (RMSE) and mean absolute error (MAE) are better; higher coefficient of determination (R^2) is better.

4.4 The minimum isogeny degree frequency

The minimum isogeny degree is approximately $\sqrt{p}$, a bound that can be established through several different methods. In particular, Galbraith, Petit, Shani, and Ti showed that an isogeny of degree $\lesssim \sqrt{p}$ is, with high probability, the shortest isogeny between the two curves it connects [GPST16, §4.2]. Their argument relies on properties of Ramanujan graphs together with a counting argument, but it does not account for collisions. Love and Boneh, however, show that collisions are rare for degrees $\leq \sqrt{p}$ [LB20].

Our data on degree maps lets us examine how frequently the minimum isogeny degree is achieved, and we find that repetitions are common. For every prime $p \leq 659$ with $p \equiv 11 \pmod{12}$, we computed the complete set of degree maps, and the resulting distributions of minimum isogenies confirm these bounds, as illustrated by the case $p = 659$ in Figure 2.

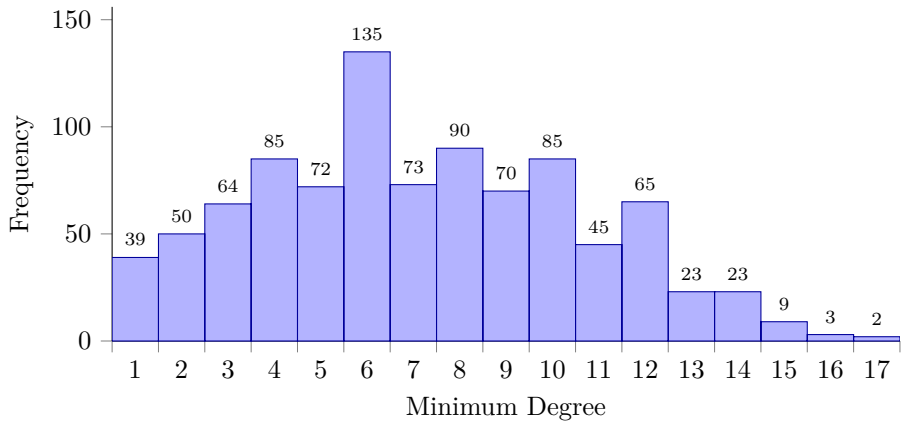


Figure 2: For $p = 659$, $\mathbf{H} = 104,620$ unique polarizations would lead to $\frac{\mathbf{h}(\mathbf{h}+1)}{2} = 1596$ reducible refined Humbert invariants belonging to one of the $\#\,\mathrm{Gen}(q_4) = 933$ isometry classes of the form $t_0^2 + 4q_{E_1,E_2}(t_1, t_2, t_3, t_4)$. Here we see the distribution of minimum values of all the degree maps q_{E_1,E_2} we obtained via genus computation.

4.5 The fixed degree isogeny problem

The *fixed-degree isogeny problem* asks: given supersingular elliptic curves E_1 and E_2 defined over the finite field $\mathbb{F}_{p^2}$, and given a positive integer N, find an isogeny $\varphi : E_1 \to E_2$ of degree N, if it exists. Finding a fixed-degree isogeny is only known to be equivalent to endomorphism ring computation when the isogeny degree is smaller than $\sqrt{p}$, where $p = \mathrm{char}(K)$ [GPST16]. Heuristically, there exists an isogeny of smooth degree $\approx p$, yet no efficient algorithm is known for finding one of that size. For isogenies of degree much larger than p, the problem can be solved efficiently using the KLPT algorithm [KLPT14] or its generalization [FKL+20], while for small degrees, standard lattice-reduction techniques suffice. The intermediate range of isogeny degrees was investigated in [BKM+24], which gave improved algorithms for the fixed-degree isogeny problem. Furthermore, [EL24] provides a heuristic algorithm that runs in polynomial time for any degree N, under certain conditions. The fixed-degree isogeny problem can, in turn, be improved by an efficient algorithm for computing refined Humbert invariants, since this allows us to obtain degree maps.

5 Conclusion

We summarize our contributions. First, we give an algorithm to enumerate principal polarizations and compute refined Humbert invariants of principally polarized superspecial abelian surfaces. Second, we give an algorithm to determine the type of a given principally polarized superspecial abelian surface. Third, we prove that the upper bound on the minimum isogeny degree between two arbitrary supersingular elliptic curves is $\sqrt{\frac{p}{2}}$ for a generic prime p, improving on the bounds of [GL09, Section 5.4.1] and [DLRW24, Lemma 12], and support this bound experimentally. Fourth, we present experiments on the frequency of minimum isogeny degrees across degree maps over $\overline{\mathbb{F}}_p$ for primes up to $p = 659$ with $p \equiv 11 \pmod{12}$. Finally, we give a different approach to the fixed-degree isogeny problem by computing degree maps directly from polarization data.

References

[BKM+24] Benjamin Bencina, Péter Kutas, Simon-Philipp Merz, Christophe Petit, Miha Stopar, and Charlotte Weitkämper. Improved algorithms for finding fixed-degree isogenies between supersingular elliptic curves. In *Advances in Cryptology - CRYPTO 2024*, volume 14924 of *LNCS*, pages 183–217. Springer, 2024.

[CDK+25] Wouter Castryck, Thomas Decru, Péter Kutas, Abel Laval, Christophe Petit, and Yan Bo Ti. KLPT^2: Algebraic pathfinding in dimension two and applications. In *Advances in Cryptology – CRYPTO 2025*, volume 16000 of *Lecture Notes in Computer Science*, pages 167–200. Springer, 2025. doi:10.1007/978-3-032-01855-7_6.

[Chi14] Sarah Chisholm. *Algorithmic Enumeration of Quaternionic Lattices*. Ph.D. thesis, University of Calgary, 2014. URL: http://hdl.handle.net/11023/1920.

[CS99] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der mathematischen Wissenschaften, Fundamental Principles of Mathematical Sciences*. Springer-Verlag, New York, 3 edition, 1999.

[DEF+25] Wolfram Decker, Christian Eder, Claus Fieker, Max Horn, and Michael Joswig, editors. *The Computer Algebra System OSCAR: Algorithms and Examples*, volume 32 of *Algorithms and Computation in Mathematics*. Springer, 1 edition, 2025.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[DLRW24] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. SQIsignHD: New Dimensions in Cryptography. In *Advances in Cryptology - EUROCRYPT 2024*, volume 14651 of *LNCS*, pages 3–32. Springer, 2024.

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *Advances in cryptology—EUROCRYPT 2018. Part III*, volume 10822 of *Lecture Notes in Comput. Sci.*, pages 329–368. Springer, Cham, 2018.

[Eic38] Martin Eichler. Über die idealklassenzahl total definiter quaternionenalgebren. *Mathematische Zeitschrift*, 43:102–109, 1938.

[EL24] Jonathan Komada Eriksen and Antonin Leroux. Computing orientations from the endomorphism ring of supersingular curves and applications. *IACR Communications in Cryptology*, 1(3), 2024. doi:10.62056/ae0fhbmo.

[FE85] Ulrich Fincke and Michael E.Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of Computation*, 44(170):463–471, 1985. URL: https://doi.org/10.1090/S0025-5718-1985-0777278-8.

[FHHJ17] Claus Fieker, William Hart, Tommy Hofmann, and Fredrik Johansson. 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*, ISSAC '17, pages 157–164, 2017.

[FKL+20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In *Advances in Cryptology - ASIACRYPT 2020*, volume 12491 of *LNCS*, pages 64–93. Springer, 2020.

[Ful89] William Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[GL09] Eyal Z. Goren and Kristin E. Lauter. The distance between superspecial abelian varieties with real multiplication. *Journal of Number Theory*, 129(6):1562–1578, 2009. doi:10.1016/j.jnt.2008.07.005.

[GPST16] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In *Advances in cryptology—ASIACRYPT 2016. Part I*, volume 10031 of *Lecture Notes in Comput. Sci.*, pages 63–91. Springer, Berlin, 2016.

[GV14] Matthew Greenberg and John Voight. Lattice methods for algebraic modular forms on classical groups. In Gebhard Böckle and Gabor Wiese, editors, *Computations with Modular Forms*, volume 6 of *Contributions in Mathematical and Computational Sciences*, pages 147–179. Springer, Cham, 2014. arXiv:1209.2460, doi:10.1007/978-3-319-03847-6_6.

[Har77] Robin Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1977.

[HI80] Kiichiro Hashimoto and Tomoyoshi Ibukiyama. On class numbers of positive definite binary quaternion Hermitian forms. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 27(3):549–601, 1980.

[Igu58] Jun-ichi Igusa. Class number of a definite quaternion with prime discriminant. *Proc. Nat. Acad. Sci. U.S.A.*, 44:312–314, 1958.

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

[Kan83] Ravi Kannan. Improved algorithms for integer programming and related lattice problems. In *Proceedings of the fifteenth annual ACM symposium on Theory of computing - STOC '83*, page 193–206, New York, NY, USA, 1983. ACM Press.

[Kan94] Ernst Kani. Elliptic curves on abelian surfaces. *Manuscripta mathematica*, 84:199–223, 1994.

[Kan14] Ernst Kani. Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms. *Journal of Number Theory*, page 139:138–174, 2014.

[Kan16] Ernst Kani. The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. *Collect. Math.*, 67:21–54, 2016.

[Kan18] Ernst Kani. Elliptic subcovers of a curve of genus 2. II. The refined Humbert invariant. *Journal of Number Theory*, 193:302–335, 2018.

[Kan19] Ernst Kani. Elliptic subcovers of a curve of genus 2. I. The isogeny defect. *Annales mathématiques du Québec*, 43:281–303, 2019.

[Kan21] Ernst Kani. Subcovers of curves and moduli spaces. In *Geometry at the frontier—symmetries and moduli spaces of algebraic varieties*, volume 766 of *Contemp. Math.*, pages 229–250. Amer. Math. Soc., 2021.

[Kan24] Ernst Kani. Principal polarizations on abelian product surfaces. *Preprint*, 2024. https://mast.queensu.ca/~kani/papers/prinpol5.pdf.

[Kir16] Markus Kirschmer. *Definite quadratic and hermitian forms with small class number*. Habilitation thesis, RWTH Aachen University, 2016. Available at https://www.math.uni-bielefeld.de/~mkirschm/papers/herm.pdf.

[Kır24] Harun Kır. *Curves of Genus 2 and Quadratic Forms*. PhD thesis, Queen's University at Kingston, Ontario, Canada, 2024. https://qspace.library.queensu.ca/items/119efd2b-59b4-4e19-9ff0-9eea3914560e.

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ-isogeny path problem. *LMS J. Comput. Math.*, 17:418–432, 2014.

[KM24] Eda Kırımlı and Chloe Martindale. The computational refined Humbert invariant problem is equivalent to the computational isogeny problem. *Preprint*, 2024. URL: https://eprint.iacr.org/2025/1295.

[Kne57] Martin Kneser. Klassenzahlen definiter quadratischer Formen. *Arch. Math.*, 8:241–250, 1957.

[KO87] Toshiyuki Katsura and Frans Oort. Supersingular abelian varieties of dimension two or three and class numbers. In *Algebraic geometry, Sendai, 1985*, volume 10 of *Adv. Stud. Pure Math.*, pages 253–281. North-Holland, Amsterdam, 1987.

[Lan83] Serge Lang. *Abelian varieties*. Springer-Verlag New York, 1983.

[LB20] Jonathan Love and Dan Boneh. Supersingular curves with small noninteger endomorphisms. In *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *Open Book Ser.*, pages 7–22. Math. Sci. Publ., Berkeley, CA, 2020.

[LO98] Ke-Zheng Li and Frans Oort. *Moduli of Supersingular Abelian Varieties*, volume 1680 of *Lecture Notes in Mathematics*. Springer, Berlin, 1998.

[Mar03] Jacques Martinet. *Perfect lattices in Euclidean spaces*, volume 327 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 2003. doi:10.1007/978-3-662-05167-2.

[Mum70] D. Mumford. *Abelian Varieties*. Oxford University Press, Oxford, 1970.

[NS09] Phong Q. Nguyen and Damien Stehlé. Low-dimensional lattice basis reduction revisited. *ACM Trans. Algorithms*, 5(4):Art. 46, 48, 2009.

[Ogu79] Arthur Ogus. Supersingular $K3$ crystals. In *Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. II*, volume 64 of *Astérisque*, pages 3–86. Soc. Math. France, Paris, 1979.

[Oor74] Frans Oort. Subvarieties of moduli spaces. *Inventiones mathematicae*, 24:95–120, 1974.

[PRS26] Aurel Page, Damien Robert, and Julien Soumier. On the conversion of module representations for higher dimensional supersingular isogenies. Cryptology ePrint Archive, Paper 2026/276, 2026.

[PS97] Wilhelm Plesken and Bernd Souvignier. Computing isometries of lattices. *J. Symbolic Comput.*, 24(3-4):327–334, 1997. Computational algebra and number theory (London, 1993).

[PS08] Xavier Pujol and Damien Stehlé. Rigorous and efficient short lattice vectors enumeration. In *Advances in Cryptology—ASIACRYPT 2008*, volume 5350 of *Lecture Notes in Computer Science*, pages 390–405. Springer, Berlin, 2008. URL: https://doi.org/10.1007/978-3-540-89255-7_24.

[Sha13] Igor R. Shafarevich. *Basic algebraic geometry. 1*. Springer, Heidelberg, third edition, 2013. Varieties in projective space.

[Shi63] Goro Shimura. Arithmetic of alternating forms and quaternion hermitian forms. *Journal of the Mathematical Society of Japan*, 15(1):33 – 65, 1963.

[Shi79] Tetsuji Shioda. Supersingular $K3$ surfaces. In *Algebraic Geometry*, volume 732 of *Lecture Notes in Math.*, pages 564–591. Springer Berlin, 1979.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, vol. 106. Springer, New York, 2009.

[Sim05] Denis Simon. Solving quadratic equations using reduced unimodular quadratic forms. *Math. Comp.*, 74(251):1531–1543, 2005.

[The26] The OSCAR Team. OSCAR – Open Source Computer Algebra Research system, Version 1.8.0, 2026. URL: https://www.oscar-system.org.

[Voi23] John Voight. Kneser's method of neighbors. *Arch. Math. (Basel)*, 121(5-6):537–557, 2023.

[Wat13] Mark Watkins. Some comments about indefinite LLL. In *Diophantine methods, lattices, and arithmetic theory of quadratic forms*, volume 587 of *Contemp. Math.*, pages 233–243. Amer. Math. Soc., Providence, RI, 2013.

[Wei57] André Weil. Zum beweis des torellischen satzes. *Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-Physikalische Klasse IIa*, pages 33–55, 1957.