Refined Humbert Invariants in Supersingular Isogeny Degree Analysis

Eda Kırımlı[1,2,3] and Gaurish Korpal[4]

[1] University of Bristol, UK
[2] Université de Neuchâtel, Switzerland
[3] University of Birmingham, UK
eda.kirimli@bristol.ac.uk
[4] University of Arizona, USA
gkorpal@arizona.edu

Abstract. In this paper, we discuss *refined Humbert invariants* of principally polarized superspecial abelian surfaces. Kani introduced the refined Humbert invariant of a principally polarized abelian surface in 1994. The main contribution of this paper is to calculate the refined Humbert invariant of a principally polarized superspecial abelian surface. We present three applications of computing this invariant in the context of isogeny-based cryptography. First, we discuss the maximum of the minimum degrees of isogenies between two uniformly random supersingular elliptic curves independent of their endomorphism ring structures. Second, we provide a different perspective on the fixed isogeny degree problem using refined Humbert invariants, and analyze this problem on average without endomorphism rings. Third, we give experimental evidence for the proven upper bounds that the minimum distance is $\approx \sqrt{p}$; our work verifies this claim up to $p = 727$.

Keywords: Isogenies · Superspecial abelian surfaces · Refined Humbert invariants · Degree maps · Fixed degree isogeny problem

1 Introduction

Isogeny-based cryptography is an active area of post-quantum cryptography that uses computing isogenies between given elliptic curves (or abelian varieties) over finite fields as the underlying mathematical hard problem. This work builds on and contributes to the computation of refined Humbert invariants of principally polarized superspecial surfaces to understand some heuristic assumptions related to the degree of an isogeny between two supersingular elliptic curves.

In our work, we compute refined Humbert invariants of principally polarized superspecial surfaces and then deploy three applications of these invariants to analyze isogeny degrees. To the best of our knowledge, this work presents the first computation of these invariants for principally polarized superspecial surfaces.

First, we show that the maximum of all the minimum distances between supersingular elliptic curves is $\approx 1.22\sqrt{\ell p}$ for a generic prime p, and $\approx 1.31\sqrt{p}$

where $p \equiv 3 \pmod 4$ without *any knowledge of endomorphism rings*. Without the machinery of refined Humbert invariants, of which we take advantage in this work, the most natural approaches to verifying this heuristic for small examples are to either brute-force compute all the isogenies or brute-force compute all the quaternion orders. In both cases, the most natural algorithm would look like listing every pair of vertices, then finding the minimum isogeny degree and the norm of the connecting ideal linking the two vertices. Our approach is conceptually simpler: the only computations required are simple checks on quadratic forms.

Secondly, we give a different approach to examine the fixed-degree isogeny problem. Lack of a security reduction between the general isogeny problem and the fixed-degree isogeny problem affects several isogeny schemes, for instance, KLPT-based SQIsign [13,14,4]. The verification step of SQIsign is not deterministic because SigningKLPT does not guarantee a specific isogeny degree, and this slows down the protocol, thereby affecting the performance [13, §5], [14, §4], [3, §6.2]. The improved algorithms for the fixed degree isogeny problem were given in [2], given the knowledge of endomorphism rings of E_1 and E_2. We, on the other hand, obtain the degree maps without depending on any given information $\mathrm{End}(E_i)$ for $i = 1, 2$, and we can test the *average* distribution of isogeny degree between supersingular elliptic curves over a finite field of characteristic p. Our method is not based on any knowledge of the endomorphism rings.

Thirdly, we run experiments on the average 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 needing any computations of isogenies or endomorphism rings. Our experiments verify that the complexity of a minimum isogeny between two supersingular elliptic curves is around $\approx \sqrt{p}$, as was previously known by [18, §4.2], and also by the proven bound is $2\sqrt{2p}/\pi$ by [6, Lemma 12]. To the best of the authors, this is the first experimental evidence of this kind. We discuss these proven bounds and validate their correctness with experiments by assuming less information.

Let $\mathcal{A}$ be an abelian surface over a finite field $\mathbb{F}_{p^k}$ for $k \geq 2$ and let $\mathrm{NS}(\mathcal{A})$ be 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[5] $q_{\mathcal{A}}$ is equivalent to an integral quadratic form q in ρ variables, so it leads to an isomorphism $(\mathrm{NS}(\mathcal{A}), q_{\mathcal{A}}) \cong (\mathbb{Z}^\rho, q)$ of quadratic modules.

Let $\mathcal{A}$ be an abelian surface and let θ be a principal polarization on $\mathcal{A}$, see Definition 2. Then the integral quadratic form $\tilde{q}_{(\mathcal{A},\theta)}$ on $\mathrm{NS}(\mathcal{A})$ is defined as

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

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 polarized Néron-Severi group. The form $q_{(\mathcal{A},\theta)}$ is a positive-definite quadratic

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

form on polarized Néron-Severi group $\mathrm{NS}(\mathcal{A},\theta) \cong \mathbb{Z}^{\rho-1}$, and it is 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 Kani's research [26,28,29,30,31,32] and recently in Kır's thesis [38,39,37]. Fortunately, 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 close relation between divisors in the Néron-Severi group and isogenies between E_1 and E_2. By using the isomorphism Theorem 1 below, 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 in an easier way. The relation between the refined Humbert invariant and the degree map, Definition 4, is given by Lemma 2 that

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

where $\theta_{E_1\times E_2}$ is a canonical product polarization and $q_{E_1,E_2} \in \mathbb{Z}[y_1, \ldots, y_n]$ is the degree map, see Definition 4.

1.1 Contribution

The main strategy is to start with a supersingular product surface $\mathcal{A} = E_1 \times E_2$. Then, we choose a principal polarization θ and a random divisor D on $\mathrm{NS}(E_1 \times E_2)$ to calculate the refined Humbert invariant, see Definition 6. Thus, we apply the irreducibility criteria, see Proposition 2, of the refined Humbert invariant $q_{(\mathcal{A},\theta)}$ of a principally polarized superspecial abelian surface to decide whether it is a product of two elliptic curves or not. Later, we use the relation of the refined Humbert invariant with the degree map, see Equation (8), then pull out the degree map and check the minimum value represented by it.

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 find a bound on the maximum value of the minimum isogeny degree reached by every pair of two supersingular elliptic curves. That is, for a fixed prime p, we aim to understand the value

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

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

The contributions of this paper are as follows. First, our experiments, see Section 3.4, show that the upper bound on the minimum degree of isogeny between two random supersingular elliptic curves is on average $\approx 1.22\sqrt{\ell p}$ for a generic prime p, and $\approx 1.31p^{1/2}$ for primes $p \equiv 3 \pmod 4$. Second, we give a different approach to the fixed degree isogeny problem by computing the degree maps on average from the intersection theory, unlike known methods the presumed knowledge of the endomorphism rings, and use the KLPT algorithm. We

directly compute degree maps from refined Humbert invariants, and our input does not depend on the chosen elliptic curves E_1 and E_2. That is, we can test the degree maps seen on average by varying over different elliptic curves. Third, we verify with our experiments that the minimum isogeny between two supersingular elliptic curves over $\mathbb{F}_{p^2}$ is roughly $\approx \sqrt{p}$ as shown previously in [18, §4.2], henceforth validating the proven upper bound given in [6, Lemma 12], and we demonstrate experiments up to $p = 727$.

1.2 Outline

In terms of organization, the paper is divided into preliminaries, computations of refined Humbert invariants and degree maps, and applications for supersingular isogeny degrees. In Section 2, we summarize the theory of refined Humbert invariants and superspecial abelian varieties. In Section 3, we develop various 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 and its impact on various isogeny-related problems, especially to analyze the supersingular isogeny degrees.

2 Preliminaries

2.1 Refined Humbert invariant

A refined Humbert invariant $q_{(\mathcal{A},\theta)}$ of a principally polarized abelian surface $(\mathcal{A}, \theta)$ is the main tool of this paper. In this section, we introduce the theory of refined Humbert invariants defined by Kani [26] in 1994. This invariant is very beneficial in the interplay between geometric and arithmetic problems. Many applications of these invariants can be found in [28,29]. This section mainly follows from Kani [30,31]. We only present essential facts of refined Humbert invariants here. For more details, see the PhD thesis [37] and the [41, §3] on the topic.

Definition 1. [20, 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 an abelian variety is an immense topic, and not possible to define the topic properly here due to space constraints. We refer the reader to Chapter 4.1 of [58] and Chapter V.1 of [20] for technical details. 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.

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 [45, p.101] since the $\mathrm{Pic}^0(\mathcal{A})$-equivalence and the numerical equivalence coincide by the Corollary of Theorem V.1 in [45].

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 Nakai-Moishezon criterion [20, 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* 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. [60, 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. [17, 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. [29, Proposition 22] *Let $\mathcal{A} = E_1 \times E_2$ be a product of two elliptic curves. Then we have a group isomorphism*

$$\mathcal{D} := \mathcal{D}_{E_1,E_2} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{NS}(\mathcal{A}) \tag{1}$$

$$\mathcal{D}(a, b, \varphi) = (a-1)\theta_1 + (b - \deg(\varphi))\theta_2 + \Gamma_{-\varphi} \tag{2}$$

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*

$$(D_1 \cdot D_2) = ab' + a'b - \beta_d(\varphi, \varphi') \tag{3}$$

where β_d *is the bilinear form associated to the* q_{E_1,E_2} *on* $\mathrm{Hom}(E_1, E_2)$*. Thus,*[6]

$$(\mathcal{D}(a, b, \varphi) \cdot \mathcal{D}(a, b, \varphi)) = 2(ab - \deg(\varphi)), \quad (\mathcal{D}(a, b, \varphi) \cdot (x\theta_1 + y\theta_2)) = bx + ay. \tag{4}$$

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

Corollary 1. [29, 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 (Definition 3) and the degree map (Definition 4) is given by

$$q_{\mathcal{A}}(x, y, \varphi) = xy - q_{E_1,E_2}(\varphi). \tag{5}$$

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

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

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

[6] 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.

Kani discusses in [26, §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

$$\tilde{q}_{(\mathcal{A},\theta)}(D) = (D\cdot\theta)^2 - 2(D\cdot D), \text{ for } D \in \mathrm{NS}(\mathcal{A}). \tag{6}$$

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[7] *$q_{(\mathcal{A},\theta)}$ 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. [31, 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*

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

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. [66, 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 $\mathcal{P}(\mathcal{A})^{\mathrm{red}}$.*

Proposition 2. [29, Proposition 6] *Let $q_{(\mathcal{A},\theta)}$ the refined Humbert invariant of the principally polarized abelian surface $(\mathcal{A},\theta)$, then we have that*

$$\theta \textit{ is reducible if and only if } q_{(\mathcal{A},\theta)} \textit{ represents } 1. \tag{7}$$

The 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 $(E_1\times E_2, \theta_{E_1\times E_2})$.

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. [37, 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 $f \equiv 0, 1 \pmod 4$.*

[7] 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 $(\mathcal{A},\theta)$

An equivalent definition. Later, Kani generalized the definition of a refined Humbert invariant in [31, 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. [31, 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* [48, p.182].

There exists a close relation between the refined Humbert invariant $q_{(\mathcal{A},\theta)}$ of a principally polarized abelian surface $(\mathcal{A}, \theta)$ 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. [30, 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*

$$q_{(\mathcal{A},\theta_\mathcal{A})}(\mathcal{D}(a, b, \varphi)) = (a - b)^2 + 4q_{E_1,E_2}(\varphi), \tag{8}$$

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. [31, Theorem 3] *If $\mathcal{C}/K$ has a presentation (E, E', ψ) of degree N with $\mathrm{char}(K) \nmid N$ and 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. [31, Theorem 4] *If* (E, E', ψ) *is a presentation of 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. [33, 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

First, we shortly summarize elliptic curves for the sake of completeness.

An elliptic curve is an abelian variety of dimension 1. The isogenies of elliptic curves are non-trivial homomorphisms between them. Isogenies from an elliptic curve to itself are called endomorphisms. The set of all endomorphisms of an elliptic curve E together with the trivial map forms the endomorphism ring $\mathrm{End}(E)$. Let E_1 and E_2 be two elliptic curves over K. Two elliptic curves E_1,E_2 are isogenous $E_1 \sim E_2$ if and only if $\mathrm{End}^0(E_1) \simeq \mathrm{End}^0(E_2)$. An elliptic curve E defined over a finite field $\mathbb{F}_{p^n}$ is said to be *supersingular* if the endomorphism algebra, $\mathrm{End}^0_{\overline{\mathbb{F}}_p}(E)$, is isomorphic to 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 $\mathbf{ij} = -\mathbf{ji}$ with

$$(a, b) = \begin{cases} (-1, -1) & p = 2 \\ (-1, -p) & p \equiv 3 \pmod 4 \\ (-2, -p) & p \equiv 5 \pmod 8 \\ (-\ell, -p),\ \ell \equiv 3 \pmod 4,\ \left(\frac{p}{\ell}\right) = -1 & p \equiv 1 \pmod 8 \end{cases}$$

for some prime $\ell = O(\log^2 p)$, see [11, Proposition 1]. Note that there are infinitely many (a, b) values that can be used, but we will use $B_p = (-\ell, -p|\mathbb{Q})$ where ℓ is the smallest possible integer as stated above for $p \geq 3$.

We now give an overview of supersingular abelian varieties, mostly following [24,23,21]. We refer to the survey [22] on the correspondence between quaternion hermitian lattices and supersingular abelian varieties.

An abelian variety over $\mathbb{F}_{p^n}$ is said to be *supersingular* if it is isogenous to a product of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ [52], 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 [51, Theorem 6.2],[59, Theorem 3.5], and [46, 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.

From Theorem 1, it follows that the divisors $D \in \mathrm{NS}(E_1 \times E_2)$ can be seen of the form

$$\mathrm{NS}(E_1 \times E_2) = \left\{ \begin{pmatrix} u & \alpha \\ \overline{\alpha} & v \end{pmatrix} : u, v \in \mathbb{Z}_{>0},\ \alpha \in \mathcal{O} \subseteq B_p \right\}. \tag{9}$$

where $\mathcal{O}$ is a maximal order of B_p. The map in Theorem 1 (or using Corollary 2.9 of [24]) 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 we vary over all maximal orders $\mathcal{O}$ of B_p.

The natural question is how to choose a representative in the conjugacy (isomorphism) classes of principal polarizations on superspecial abelian surfaces, as there are too many of them to use in the computations. This issue has been considered by Hashimoto and Ibukiyama [21]. 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. [21, Proposition 22] *$\Lambda = (\mathcal{O}, \mathcal{O})T$ 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 with norm $\mathcal{O}$. 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. [21, 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.*

We 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 as in [21] 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 $u = (\mathrm{nrd}(\alpha) + 1)/v$.

This is incorporated in Algorithm 2.

Furthermore, Lemma 3 allows us to choose the representative of principal polarizations in the special form $\begin{pmatrix} u & \alpha \\ \overline{\alpha} & v \end{pmatrix}$ where $v \in \mathbb{Z}_{>0}$ and $\alpha \in O \coloneqq \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\mathbf{ij} \subsetneq \mathcal{O}$. This crucial fact lets us bypass working with $\alpha \in \mathcal{O} \setminus O$ as we can instead choose different values of v and then compute $\alpha \in O$ accordingly.

3 Computation of refined Humbert invariants and degree maps

A refined Humbert invariant $q_{(\mathcal{A},\theta)}$ corresponding to a principally polarized superspecial abelian surface $(\mathcal{A}, \theta)$ is an integral quadratic form in 5 variables, called *quintic refined Humbert invariants*[8].

Unless stated otherwise, let p be an odd prime and let $\mathcal{A} = E_1 \times E_2$ be a supersingular product surface with principal polarization θ, where E_1, E_2 are supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$. Recall that $\mathrm{End}^0_{\overline{\mathbb{F}}_p}(E_1) = \mathrm{End}^0_{\overline{\mathbb{F}}_p}(E_2) = B_p = (-\ell, -p|\mathbb{Q})$ where $B_p = \mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{ij}$ with $\mathbf{i}^2 = -\ell$ and $\mathbf{j}^2 = -p$.

Remark 1. The isogeny defect (Definition 10) $m_\psi = 1$ if and only if ψ is induced by an isogeny, see [31, Remark 21]. We are interested in the product surface $\mathcal{A} = E_1 \times E_2$ where E_1 and E_2 are supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and such curves are always isogenous to each other [43, Corollary 77], hence the isogeny defect is $m_\psi = 1$ in this case (also see Theorem 4).

[8] 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 by following Kani's terminology.

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 unknown supersingular elliptic curves E_1 and E_2.

Method 1: using Definition 6.

1. As in (10), fix the principal polarization θ on the abelian surface $E_1 \times E_2$ represented by a positive definite hermitian matrix of determinant 1

$$\theta \coloneqq \begin{pmatrix} u_0 & w_0 + x_0\mathbf{i} + y_0\mathbf{j} + z_0\mathbf{ij} \\ w_0 - x_0\mathbf{i} - y_0\mathbf{j} - z_0\mathbf{ij} & v_0 \end{pmatrix} = \begin{pmatrix} u_0 & \alpha_0 \\ \overline{\alpha}_0 & v_0 \end{pmatrix}$$

   for fixed values of u_0, v_0 and $\alpha_0 \coloneqq w_0 + x_0\mathbf{i} + y_0\mathbf{j} + z_0\mathbf{ij} \in \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\mathbf{ij}$ such that $u_0 > 0$, $v_0 > 0$, and $u_0v_0 - \mathrm{nrd}(\alpha_0) = 1$, i.e. $u_0v_0 - w_0^2 - \ell x_0^2 - py_0^2 - \ell p z_0^2 = 1$ (i.e. self-intersection number of θ is 2) [24, Corollary 2.9].
2. Choose a random divisor D on $E_1 \times E_2$ using (9).

$$D \coloneqq \begin{pmatrix} u & w + x\mathbf{i} + y\mathbf{j} + z\mathbf{ij} \\ w - x\mathbf{i} - y\mathbf{j} - z\mathbf{ij} & v \end{pmatrix} \in \mathrm{NS}(E_1 \times E_2) \subseteq M_2(B_p)$$

   for $u, v, w, x, y, z \in \mathbb{Z}$.
3. Compute the intersection of the divisors θ and D as in [19, §7.5].

$$\begin{aligned}
(D \cdot \theta) &= v_0u + u_0v + 2(\ell p z_0 z - w_0 w - \ell x_0 x - p y_0 y) \\
(D \cdot \theta)^2 &= v_0^2u^2 + 2u_0v_0uv - 4v_0w_0uw - 4\ell v_0x_0ux - 4pv_0y_0uy + 4\ell pv_0z_0uz \\
&\quad + u_0^2v^2 - 4u_0w_0vw - 4\ell u_0x_0vx - 4pu_0y_0vy + 4\ell pu_0z_0vz \\
&\quad + 4w_0^2w^2 + 8\ell w_0x_0wx + 8pw_0y_0wy - 8\ell pw_0z_0wz \\
&\quad + 4\ell^2x_0^2x^2 + 8\ell px_0y_0xy - 8\ell^2px_0z_0xz \\
&\quad + 4p^2y_0^2y^2 - 8\ell p^2z_0y_0yz \\
&\quad + 4\ell^2p^2z_0^2z^2
\end{aligned}$$

4. Compute the self-intersection of the divisor D as in [19, (7.8)].

$$(D \cdot D) = 2(uv - w^2 - \ell x^2 - py^2 - \ell pz^2)$$

5. Compute $\tilde{q}_{(E_1\times E_2,\theta)}(D) = (D \cdot \theta)^2 - 2(D \cdot D)$ as in (6).

$$\begin{aligned}
\tilde{q}_{(E_1\times E_2,\theta)}(D) &= v_0^2u^2 + 2(u_0v_0 - 2)uv - 4v_0w_0uw - 4\ell v_0x_0ux - 4pv_0y_0uy + 4\ell pv_0z_0uz \\
&\quad + u_0^2v^2 - 4u_0w_0vw - 4\ell u_0x_0vx - 4pu_0y_0vy + 4\ell pu_0z_0vz \\
&\quad + 4(w_0^2 + 1)w^2 + 8\ell w_0x_0wx + 8pw_0y_0wy - 8\ell pw_0z_0wz \\
&\quad + 4\ell(\ell x_0^2 + 1)x^2 + 8\ell px_0y_0xy - 8\ell^2px_0z_0xz
\end{aligned}$$

$$
\begin{aligned}
&+ 4p(py_0^2+1)y^2 - 8\ell p^2 z_0 y_0 yz \\
&+ 4\ell p(\ell p z_0^2+1)z^2 \\
&\coloneqq \frac{1}{2}X^t A X
\end{aligned}
$$

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

$$
A = \begin{pmatrix}
2v_0^2 & 2(u_0v_0-2) & -4v_0w_0 & -4\ell v_0x_0 & -4pv_0y_0 & 4\ell pv_0z_0 \\
2(u_0v_0-2) & 2u_0^2 & -4u_0w_0 & -4\ell u_0x_0 & -4pu_0y_0 & 4\ell pu_0z_0 \\
-4v_0w_0 & -4u_0w_0 & 8(1+w_0^2) & 8\ell w_0x_0 & 8pw_0y_0 & -8\ell pw_0z_0 \\
-4\ell v_0x_0 & -4\ell u_0x_0 & 8\ell w_0x_0 & 8\ell(1+\ell x_0^2) & 8\ell px_0y_0 & -8\ell^2 px_0z_0 \\
-4pv_0y_0 & -4pu_0y_0 & 8pw_0y_0 & 8\ell px_0y_0 & 8p(1+py_0^2) & -8\ell p^2 y_0z_0 \\
4\ell pv_0z_0 & 4\ell pu_0z_0 & -8\ell pw_0z_0 & -8\ell^2 px_0z_0 & -8\ell p^2 y_0z_0 & 8\ell p(1+\ell pz_0^2)
\end{pmatrix}
$$

with $\det(A) = 2^{16}\ell^2p^2\left(u_0v_0 - \mathrm{nrd}(\alpha_0) - 1\right) = 0$.

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 $q_{(E_1\times E_2,\theta)}$) by using [37, Proposition 2.1.3].

$$
q_{(E_1\times E_2,\theta)}(D) = \frac{1}{2}\begin{pmatrix} t_0 & t_1 & t_2 & t_3 & t_4 \end{pmatrix}^t (T^tAT) \begin{pmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix}
$$

Moreover, since the Picard number[9] $\rho(\mathcal{A}) = 6$, using Proposition 1 we get

$$
\det(T^tAT) = \frac{1}{2}(-4)^{\rho-1}\det(q_{E_1\times E_2}) = \frac{1}{2}(-4)^{6-1}(-2^4\ell^2p^2) = 2^{13}\ell^2p^2
$$

where the intersection form $q_{\mathcal{A}} = q_{E_1\times E_2} = \frac{1}{2}(D\cdot D) = uv - w^2 - \ell x^2 - py^2 - \ell pz^2$ by Definition 3.

Remark 2. In step 1, we choose $\alpha_0 = w_0 + x_0\mathbf{i} + y_0\mathbf{j} + z_0\mathbf{ij} \in O$ where $O \coloneqq \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\mathbf{ij} \subsetneq \mathcal{O} \subsetneq B_p = (-\ell, -p|\mathbb{Q})$, and $\mathcal{O}$ is a maximal order in B_p.

Consider the integral quadratic form $f(w_0,x_0,y_0,z_0) = \mathrm{nrd}(w_0 + x_0\mathbf{i} + y_0\mathbf{j} + z_0\mathbf{ij}) = w_0^2 + \ell x_0^2 + py_0^2 + \ell pz_0^2$ with $\det(f) = \det\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2\ell & 0 & 0 \\ 0 & 0 & 2p & 0 \\ 0 & 0 & 0 & 2\ell p \end{pmatrix} = 2^4\ell^2p^2$. Then α_0 above is a solution of f such that $f(w_0,x_0,y_0,z_0) = u_0v_0 - 1$ for fixed $u_0, v_0 \in \mathbb{Z}_{>0}$.

On the other hand, for $p \equiv 3 \pmod 4$ and $B_p = (-1, -p|\mathbb{Q})$, as in [2, §4], we can fix $\mathcal{O} = \mathbb{Z}\langle 1, \beta_1, \beta_2, \beta_3\rangle = \mathbb{Z}\left\langle 1, \mathbf{i}, \frac{\mathbf{i}(1+\mathbf{j})}{2}, \frac{1+\mathbf{j}}{2}\right\rangle$. Then choosing $\alpha_0 =$

[9] As $\mathrm{NS}(\mathcal{A}) \cong \mathbb{Z}^\rho$ where $\rho = \rho(\mathcal{A})$ is the Picard number of $\mathcal{A}$ by [48, p.60], and we obtain $\mathrm{NS}(\mathcal{A},\theta) \cong \mathbb{Z}^{\rho-1}$, and $q_{(E_1\times E_2,\theta)}$ is a quintic quadratic form [26, p.200].

$w_0 + x_0\beta_1 + y_0\beta_2 + z_0\beta_3 \in \mathcal{O}$ as in (10), we get the integral quadratic form $g(w_0, x_0, y_0, z_0) = \mathrm{nrd}(w_0 + x_0\beta_1 + y_0\beta_2 + z_0\beta_3) = w_0^2 + w_0z_0 + x_0^2 + x_0y_0 + \frac{p+1}{4}y_0^2 + \frac{p+1}{4}z_0^2$, such that $\det(g) = \det\begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & \frac{p+1}{2} & 0 \\ 1 & 0 & 0 & \frac{p+1}{2} \end{pmatrix} = p^2$. Then α_0 would be a solution of g such that $g(w_0, x_0, y_0, z_0) = u_0v_0 - 1$ for fixed $u_0, v_0 \in \mathbb{Z}_{>0}$.

Therefore, for $\ell = 1$, we get $\det(f) = 16\det(g)$ as expected, because of normalization. Moreover, in general, $\mathrm{disc}(O) = 16\ell^2p^2 = 16\ell^2\,\mathrm{disc}(\mathcal{O})$ and $[O : \mathcal{O}] = 4\ell$ see [63, §15.1].

Example 1. Let $p \equiv 3 \pmod 4$, leading to $\ell = 1$, and fix $\theta := \left(\begin{smallmatrix} 2 & \mathbf{i} \\ -\mathbf{i} & 1 \end{smallmatrix}\right)$ then the above method will lead to

$$\begin{aligned} \tilde{q}_{(E_1\times E_2,\theta)} &= u^2 - 4ux + 4v^2 - 8vx + 4w^2 + 8x^2 + 4py^2 + 4pz^2 \\ &= (u-2x)^2 + 4(v-x)^2 + 4w^2 + 4py^2 + 4pz^2 \\ &= \frac{1}{2}\begin{pmatrix} u & v & w & x & y & z \end{pmatrix}\begin{pmatrix} 2 & 0 & 0 & -4 & 0 & 0 \\ 0 & 8 & 0 & -8 & 0 & 0 \\ 0 & 0 & 8 & 0 & 0 & 0 \\ -4 & -8 & 0 & 16 & 0 & 0 \\ 0 & 0 & 0 & 0 & 8p & 0 \\ 0 & 0 & 0 & 0 & 0 & 8p \end{pmatrix}\begin{pmatrix} u \\ v \\ w \\ x \\ y \\ z \end{pmatrix}. \end{aligned}$$

Then we get $T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$, leading to

$$q_{(E_1\times E_2,\theta)}(D) = t_0^2 + 4(t_1^2 + t_2^2 + pt_3^2 + pt_4^2).$$

Note that the quintic refined Humbert invariant $q_{(E_1\times E_2,\theta)}$ satisfies the reducibility criteria stated in (2). Therefore, as per Lemma 2, the degree map is $q_{E_1,E_2} = t_1^2 + t_2^2 + pt_3^2 + pt_4^2$.

Method 2: using Proposition 3.

1. Let $\mathcal{A} = E_1 \times E_2$ be the abelian surface and take a principal polarization θ on $E_1 \times E_2$.
2. As in Definition 8, let

$$\mu := \begin{pmatrix} u & w + x\mathbf{i} + y\mathbf{j} + z\mathbf{ij} \\ w - x\mathbf{i} - y\mathbf{j} - z\mathbf{ij} & v \end{pmatrix} \in \mathrm{End}_\theta(E_1 \times E_2) \subseteq M_2(B_p)$$

   for $u, v, w, x, y, z \in \mathbb{Z}$.
3. Compute $\tilde{q}_{(E_1\times E_2,\theta)}(D) = \mathrm{tr}(\mu^2) - \frac{1}{4}(\mathrm{tr}(\mu))^2$, where tr is the sum of reduced trace of quaternion elements along the diagonal of the matrix representation.

$$\mu^2 = \begin{pmatrix} u^2 + w^2 + \ell x^2 + py^2 + \ell pz^2 & (u+v)(w + x\mathbf{i} + y\mathbf{j} + z\mathbf{ij}) \\ (u+v)(w - x\mathbf{i} - y\mathbf{j} - z\mathbf{ij}) & v^2 + w^2 + \ell x^2 + py^2 + \ell pz^2 \end{pmatrix}$$

$$\begin{aligned}\mathrm{tr}(\mu^2) &= \mathrm{trd}(u^2 + w^2 + \ell x^2 + py^2 + \ell pz^2) + \mathrm{trd}(v^2 + w^2 + \ell x^2 + py^2 + \ell pz^2) \\ &= 2(u^2 + v^2 + 2w^2 + 2\ell x^2 + 2py^2 + 2\ell pz^2)\end{aligned}$$

Moreover, $\mathrm{tr}(\mu) = \mathrm{trd}(u) + \mathrm{trd}(v) = 2(u + v)$. Therefore, we have

$$\begin{aligned}\tilde{q}_{(E_1\times E_2,\theta)}(D) &= 2(u^2 + v^2 + 2w^2 + 2\ell x^2 + 2py^2 + 2\ell pz^2) - \frac{1}{4}\left(2(u+v)\right)^2 \\ &= (u-v)^2 + 4w^2 + 4\ell x^2 + 4py^2 + 4\ell pz^2 \\ &\coloneqq \frac{1}{2}X^tAX\end{aligned}$$

where $X = \begin{pmatrix} u \\ v \\ w \\ x \\ y \\ z \end{pmatrix}$ and $A = \begin{pmatrix} 2 & -2 & 0 & 0 & 0 & 0 \\ -2 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 8\ell & 0 & 0 \\ 0 & 0 & 0 & 0 & 8p & 0 \\ 0 & 0 & 0 & 0 & 0 & 8\ell p \end{pmatrix}$ is the coefficient matrix with $\det(A) = 0$.

4. 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 [37, Proposition 2.1.3]

$$q_{(E_1\times E_2,\theta)}(D) = \frac{1}{2}\begin{pmatrix} t_0 & t_1 & t_2 & t_3 & t_4 \end{pmatrix}(T^tAT)\begin{pmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix}.$$

Here we get $T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$, such that $\det(T^tAT) = 2^{13}\ell^2p^2$, leading to

$$q_{(E_1\times E_2,\theta)}(D) = t_0^2 + 4(t_1^2 + \ell t_2^2 + pt_3^2 + \ell pt_4^2).$$

Note that $q_{(E_1\times E_2,\theta)}$ satisfies the reducibility condition stated in (2). Therefore, as per Lemma 2, the degree map (degree form) is $q_{E_1,E_2} = t_1^2 + \ell t_2^2 + pt_3^2 + \ell pt_4^2$.

Remark 3. Method 2 is a special case of Method 1, with $\theta \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, i.e. $\mathrm{nrd}(\alpha_0) = 0$.

We observe that $\tilde{q}_{(E_1\times E_2,\theta)}$ above is a positive semi-definite form and applying[10] Simon's indefiniteLLL[11] algorithm [61,65] quickly gives us positive definite quintic form $q_{(E_1\times E_2,\theta)}$. Moreover, we can ensure with the irreducibility criteria, Proposition 2 above, that the quintic form we obtained corresponds to a superspecial abelian surface $\mathcal{A} = E_1 \times E_2$ over $\overline{\mathbb{F}}_p$ with a reducible principal

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

polarization $\theta \in \mathcal{P}^{\mathrm{red}}(E_1 \times E_2)$ by using Kannan-Fincke-Pohst $\mathsf{minVector}$[12] algorithm [35,16,56] to check that 1 is the minimum value it represents. Therefore, the Algorithm 1 below lets us compute the quintic refined Humbert invariants for principally polarized superspecial abelian surfaces.

Algorithm 1 $\mathsf{RHI}(p, \ell, \theta)$

Input: odd prime p with ℓ such that $B_p = (-\ell, -p|\mathbb{Q})$ and polarization $\theta = \left(\begin{smallmatrix} u_0 & \alpha_0 \\ \overline{\alpha_0} & v_0 \end{smallmatrix}\right)$ where $\alpha_0 \coloneqq w_0 + x_0\mathbf{i} + y_0\mathbf{j} + z_0\mathbf{ij} \in \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\mathbf{ij}$

Output: coefficient matrix of quintic refined Humbert invariant $q_{(E_1 \times E_2, \theta)}$.

1: $A \leftarrow \begin{pmatrix} 2v_0^2 & 2(u_0v_0-2) & -4v_0w_0 & -4\ell v_0x_0 & -4pv_0y_0 & 4\ell pv_0z_0 \\ 2(u_0v_0-2) & 2u_0^2 & -4u_0w_0 & -4\ell u_0x_0 & -4pu_0y_0 & 4\ell pu_0z_0 \\ -4v_0w_0 & -4u_0w_0 & 8(1+w_0^2) & 8\ell w_0x_0 & 8pw_0y_0 & -8\ell pw_0z_0 \\ -4\ell v_0x_0 & -4\ell u_0x_0 & 8\ell w_0x_0 & 8\ell(1+\ell x_0^2) & 8\ell px_0y_0 & -8\ell^2 px_0z_0 \\ -4pv_0y_0 & -4pu_0y_0 & 8pw_0y_0 & 8\ell px_0y_0 & 8p(1+py_0^2) & -8\ell p^2 y_0z_0 \\ 4\ell pv_0z_0 & 4\ell pu_0z_0 & -8\ell pw_0z_0 & -8\ell^2 px_0z_0 & -8\ell p^2 y_0z_0 & 8\ell p(1+\ell pz_0^2) \end{pmatrix}$

2: // the coefficient matrix of $\tilde{q}_{(\mathcal{A},\theta)}$ with $\det(A) = 2^{16}\ell^2p^2\,(u_0v_0 - \mathrm{nrd}(\alpha_0) - 1) = 0$

3: $A' \leftarrow \mathsf{indefiniteLLL}(A)$

4: // A is 6×6 positive semidefinite and A' is 5×5 positive definite.

5: **if** $\det(A') = 2^{13}\ell^2p^2$ **then**

6: // Proposition 1 for $\rho = 6$ and $q_{\mathcal{A}} = uv - w^2 - \ell x^2 - py^2 - \ell pz^2$

7: $L \leftarrow$ Integer lattice with Gram matrix $A'/2$

8: **if** $\mathsf{minVector}(L) = 1$ **then**

9: // (2) and [16, §2]

10: **return** A'

11: **return** 0

3.2 Principal polarizations

We aim to determine all possible quintic refined Humbert invariants that are unique up to isometry. However, as per Proposition 4 above, for a given prime p, two distinct principal polarizations can lead to the same quintic refined Humbert invariant.

The discussion following Lemma 3 suggests that 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 $\alpha_0 = w_0 + x_0\mathbf{i} + y_0\mathbf{j} + z_0\mathbf{ij} \in \mathbb{Z}\langle 1, \mathbf{i}, \mathbf{j}, \mathbf{ij}\rangle$ such that $0 \le w_0, x_0, y_0, z_0 \le v_0 - 1$ and $\mathrm{nrd}(w_0 + x_0\mathbf{i} + y_0\mathbf{j} + z_0\mathbf{ij}) = u_0v_0 - 1$. Therefore, any representation of 1 by the intersection form $q_{\mathcal{A}} = q_{E_1 \times E_2} = uv - w^2 - \ell x^2 - py^2 - \ell pz^2$ will correspond to a principal polarization $\left(\begin{smallmatrix} u_0 & \alpha_0 \\ \overline{\alpha_0} & v_0 \end{smallmatrix}\right)$ with $\alpha_0 = w_0 + x_0\mathbf{i} + y_0\mathbf{j} + z_0\mathbf{ij}$ and $u_0v_0 - \mathrm{nrd}(\alpha_0) = 1$. Hence, we must carefully choose the principal polarizations to improve the chances of obtaining distinct non-isometric quintic refined Humbert invariants.

We begin by analyzing the symmetries in the coefficient matrix of $\tilde{q}_{(E_1 \times E_2, \theta)}$ in Algorithm 1. In general, $\theta = \left(\begin{smallmatrix} u_0 & \alpha_0 \\ \overline{\alpha_0} & v_0 \end{smallmatrix}\right)$ and $\theta' = \left(\begin{smallmatrix} v_0 & \alpha_0 \\ \overline{\alpha_0} & u_0 \end{smallmatrix}\right)$ will lead to the

[12] https://github.com/thofma/Hecke.jl/blob/master/src/QuadForm/Enumeration.jl

same quintic refined Humbert invariant. That is, it is enough to consider the principal polarizations with $u_0 = v_0 = m$ and vary the value of m such that $p \nmid \mathrm{nrd}(\alpha_0) = m^2 - 1$.

Therefore, the Algorithm 2 below gives us a finite list of principal polarizations that will lead to a distinct coefficient matrix of $\tilde{q}_{(E_1 \times E_1, \theta)}$.

Algorithm 2 $\mathsf{polz}(p, \ell, m)$

Input: odd prime p with ℓ such that $B_p = (-\ell, -p|\mathbb{Q})$ and positive integer m such that $m^2 \not\equiv 1 \pmod{p}$.

Output: polarizations $\theta = \left(\begin{smallmatrix} u_0 & \alpha_0 \\ \overline{\alpha_0} & v_0 \end{smallmatrix}\right)$ where $u_0 = v_0 = m$ and $\alpha_0 = w_0 + x_0\mathbf{i} + y_0\mathbf{j} + z_0\mathbf{ij} \in \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\mathbf{ij}$ with $0 \le w_0, x_0, y_0, z_0 \le m - 1$.

$P \leftarrow$ [] // initialize an empty list
$M \leftarrow m^2 - 1$
$N \leftarrow m - 1$
for $z = 0$ **to** N **do**
  if $\ell p z^2 > M$ **then**
    break
  for $y = 0$ **to** N **do**
    $s \leftarrow p(y^2 + \ell z^2)$
    if $s > M$ **then**
      break
    $r_1 \leftarrow M - s$
    for $x = 0$ **to** N **do**
      if $\ell x^2 > r_1$ **then**
        break
      $r_2 \leftarrow r_1 - \ell x^2$
      $w = \lfloor \sqrt{r_2} \rfloor$
      if $w^2 = r_2$ **and** $w \le N$ **then**
        P.append($[m, m, w, x, y, z]$)
return P

Special case: $p \equiv 3 \pmod 4$. Note that in SQIsign and other isogeny-based schemes we work with primes $p \equiv 3 \pmod 4$ with $B_p = (-1, -p|\mathbb{Q})$. Then $\ell = 1$ leads to further symmetries in the coefficient matrix of $\tilde{q}_{(E_1 \times E_2, \theta)}$ in Algorithm 1. In particular, $\theta = \begin{pmatrix} m & w_0 + x_0\mathbf{i} + y_0\mathbf{j} + z_0\mathbf{ij} \\ w_0 - x_0\mathbf{i} - y_0\mathbf{j} - z_0\mathbf{ij} & m \end{pmatrix}$ and $\theta' = \begin{pmatrix} m & x_0 + w_0\mathbf{i} + z_0\mathbf{j} + y_0\mathbf{ij} \\ x_0 - w_0\mathbf{i} - z_0\mathbf{j} - y_0\mathbf{ij} & m \end{pmatrix}$ will lead to the same quintic refined Humbert invariant. Therefore, it is sufficient to consider $\alpha_0 = w_0 + x_0\mathbf{i} + y_0\mathbf{j} + z_0\mathbf{ij}$ such that $0 \le w_0 \le x_0 \le m - 1$ and $0 \le y_0 \le z_0 \le m - 1$. This specialized version is given in Algorithm 3.

3.3 Counting distinct forms

Knowing the expected number of unique (non-isometric) refined Humbert invariants will significantly speed up the process of finding all the quintic forms

Algorithm 3 polzSQl(p, m)

Input: prime $p \equiv 3 \pmod 4$ and positive integer m such that $m^2 \not\equiv 1 \pmod p$
Output: polarizations $\theta = \left(\begin{smallmatrix} u_0 & \alpha_0 \\ \overline{\alpha_0} & v_0 \end{smallmatrix}\right)$ where $u_0 = v_0 = m$ and $\alpha_0 = w_0 + x_0\mathbf{i} + y_0\mathbf{j} + z_0\mathbf{ij} \in \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\mathbf{ij}$ with $0 \le w_0 \le x_0 \le m-1$ and $0 \le y_0 \le z_0 \le m-1$.

$P \leftarrow$ [] // initialize an empty list
$M \leftarrow m^2 - 1$
$N \leftarrow m - 1$
for $z = 0$ **to** N **do**
  if $pz^2 > M$ **then**
    break
  for $y = 0$ **to** z **do**
    $s \leftarrow p(y^2 + z^2)$
    if $s > M$ **then**
      break
    $r_1 \leftarrow M - s$
    for $x = 0$ **to** N **do**
      if $x^2 > r_1$ **then**
        break
      $r_2 \leftarrow r_1 - x^2$
      $w = \lfloor \sqrt{r_2} \rfloor$
      if $w^2 = r_2$ **and** $w \le x$ **then**
        P.append($[m, m, w, x, y, z]$)
return P

of interest, since it will allow us to stop computing new refined Humbert invariants once the target number of non-isometric quintic integral quadratic forms has been found. Therefore, here we discuss our attempt to get a bound on this number.

When $\mathcal{A}$ is a supersingular elliptic curve, Deuring showed that $\mathcal{A}$ has a model defined over $\mathbb{F}_{p^2}$ and the class number $\mathbf{h}$ of $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{A})$ was calculated by Eichler [10], Deuring [8], and Igusa [25].

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

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 $\mathcal{A}$ were calculated by Ibukiyama, Katsura and Oort [24] in 1986 when $\mathcal{A} = E \times E'$, where E and E' are supersingular elliptic curves.

Theorem 6. [24, 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 $H_2(p, 1)$ of the principal genus of the quaternion Hermitian space B_p^2.*

The class number $H_1(p, 1)$ was explicitly computed by Eichler [10]. The class number $H_2(p, 1)$ is calculated by Hashimoto and Ibukiyama [21]. By following the notation of [24], we set $\mathbf{h} = H_1(p, 1)$ and $\mathbf{H} = H_2(p, 1)$. Deuring [8] showed

that the number $\mathbf{h}$ is equal to the number of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ as in (12).

Corollary 2. [24, Corollary 2.12] *The number of isomorphism classes of non-singular irreducible curves of genus* 2 *whose Jacobian is isomorphic to a product of two supersingular elliptic curves is equal to* $\mathbf{H} - \frac{\mathbf{h}(\mathbf{h}+1)}{2}$.

Hashimoto and Ibukiyama [21, p.1] gave a formula for $\mathbf{H}$.

Later, Katsura and Oort gave [36, Theorem 3.3] simpler version of the formula for $\mathbf{H}$ as follows:

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

However, 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 principally polarized superspecial surface, while $\frac{\mathbf{h}(\mathbf{h}+\mathbf{1})}{\mathbf{2}}$ is an upper bound on the the refined Humbert invariants constructed with reducible polarizations, see 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 abelian surfaces $(\mathcal{A}, \theta)$ and $(\mathcal{A}', \theta')$ can end up having 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 $\overline{\mathbb{F}}_p$ given in Corollary 2 is not equal to the number of refined Humbert invariants. In fact, we obtain less refined Humbert invariants in our experiments (see Section 3.4). The number of genus 2 curves with a given refined Humbert invariant is counted in the case of a CM product surface, which has a ternary refined Humbert invariant, see [34]. Unfortunately, there are no similar closed formulas for quintic refined Humbert invariants.

Remark 4. Notice that the cardinality $|\operatorname{Aut}(\mathcal{A}) \setminus \mathcal{P}(\mathcal{A})^{\mathrm{red}}|$ of [33] is exactly $\frac{\mathbf{h}(\mathbf{h}+\mathbf{1})}{\mathbf{2}}$ in [24]. Kani examines the nature of principal polarizations by positive definite integral quadratic forms, while Ibukiyama does the same with the quaternion hermitian forms. Therefore, genera, class numbers, type numbers, and similar notions have to be taken in the correct language, and they should be carefully translated into another one.

We use the Plesken-Souvignier isIsometric[13] algorithm [55] to collect the unique (up to isometry) refined Humbert invariants obtained from Algorithm 1

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

for various polarizations obtained from Algorithm 2 or Algorithm 3. That is, we fix bounds a and b, run $\mathsf{RHI}(p, \ell, \theta)$ for all θ's produced by $\mathsf{polz}(p, \ell, m)$ for $a \leq m \leq b$ and $p \nmid (m^2 - 1)$, and save the non-isometric quintic forms which represent 1 (see Algorithm 4).

Algorithm 4 $\mathsf{allRHI}(p, \ell, a, b)$

Input: odd prime p with ℓ such that $B_p = (-\ell, -p|\mathbb{Q})$, and $a, b \in \mathbb{Z}_{\geq 1}$.
Output: coefficient matrices of all unique refined Humbert for polarizations $\theta = \left(\begin{smallmatrix} m & \alpha_0 \\ \bar{\alpha_0} & m \end{smallmatrix}\right)$ with $a \leq m \leq b$

$Q \leftarrow$ [] // initialize the list of unique refined Humbert invariants
for $m = a$ **to** b **do**
  if $m^2 \not\equiv 1 \pmod{p}$ **then**
    if $\ell = 1$ **then**
      $\Theta_m \leftarrow \mathsf{polzSQI}(p, m)$
    else
      $\Theta_m \leftarrow \mathsf{polz}(p, \ell, m)$
    for $\theta \in \Theta_m$ **do**
      $A \leftarrow \mathsf{RHI}(p, \ell, \theta)$
      if $A \neq 0$ **then**
        $s \leftarrow$ **true** // assume unique
        for $A' \in Q$ **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**
          for $A' \in Q$ **do**
            $L_{A'} \leftarrow$ Integer lattice with Gram matrix $A'/2$
            if $\mathsf{isIsometric}(L_A, L_{A'}) =$ **true then**
              $s \leftarrow$ **false** // not unique
              break
        if $s =$ **true then**
          Q.append(A)
return Q

Observation. Recall that in our notation, ℓ is the smallest positive integer such that $B_p = (-\ell, -p|\mathbb{Q})$. Also, note that the number of isometry classes in the genus of integer quadratic forms is finite [57, Theorem 6.10]. Moreover, we can use Kneser's neighbor method[14] [42,64] to obtain the representatives of all the isometry classes.

Table 1 below supports the choice of executing Algorithm 4 for $2\ell p \leq m \leq 2\ell p + p$ such that $p \nmid (m^2 - 1)$, because:

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

1. $\#\Theta \gg \mathbf{H}$: That is, we are checking a lot more polarizations than the total possible, up to isomorphism. Furthermore, consistently, about 10% of polarizations Θ lead to a quintic refined Humbert invariant which represents 1.
2. $\#\underset{\text{iso}}{\text{RHI}} = \#\underset{\text{red}}{\text{Gen}}(q_5) = \#\,\text{Gen}(q_4)$: Here $q_5(t_0,t_1,t_2,t_3,t_4) = t_0^2 + 4(t_1^2 + \ell t_2^2 + pt_3^2 + \ell p t_4^2)$ is the diagonal form we obtained using Method 2 above, with $\det(q_5) = \det\begin{pmatrix} 2&0&0&0&0\\ 0&8&0&0&0\\ 0&0&8\ell&0&0\\ 0&0&0&8p&0\\ 0&0&0&0&8\ell p \end{pmatrix} = 2^{13}\ell^2p^2$. We can then obtain all the representatives of the isometry classes in the genus of quadratic form q_5, which represent 1.
   Next, using Lemma 2, we also obtain the degree map $q_4(t_1,t_2,t_3,t_4) = \text{nrd}(t_1+t_2\mathbf{i}+t_3\mathbf{j}+t_4\mathbf{ij}) = t_1^2+\ell t_2^2+pt_3^2+\ell pt_4^2$ with $\det(q_4) = \det\begin{pmatrix} 2&0&0&0\\ 0&2\ell&0&0\\ 0&0&2p&0\\ 0&0&0&2\ell p \end{pmatrix} = 2^4\ell^2p^2$. We can then obtain the representatives of the isometry classes in the genus of quadratic form q_4.
   Therefore, for our choice of $a = 2\ell p$ and $b = 2\ell p + p$, we obtain all the quintic form representatives with determinant $2^{13}\ell^2p^2$ and minimum value 1.
3. $\#\underset{\text{iso}}{\text{RHI}} \gg \frac{\mathbf{h}(\mathbf{h}+1)}{2}$: That is, we have computed a superset of the desired quintic refined Humbert invariants, as in Proposition 4.

Table 1. Comparing the results of $\mathsf{allRHI}(p,\ell,2\ell p,2\ell p+p)$ for the first 9 primes $p > 20$, with the isometry class representatives found using Kneser's neighbor method. Here Θ is the set of polarizations checked, $\underset{\text{red}}{\text{RHI}}$ is the set of quintic refined Humbert invariants which represent 1, and $\underset{\text{iso}}{\text{RHI}} \subseteq \underset{\text{red}}{\text{RHI}}$ is the set of isometry class representatives which represent 1.

p	ℓ	$\mathbf{H}$	$\#\Theta$	$\#\underset{\text{red}}{\text{RHI}}$	$\#\underset{\text{iso}}{\text{RHI}}$	$\#\underset{\text{red}}{\text{Gen}}(q_5)$	$\#\,\text{Gen}(q_4)$	$\frac{\mathbf{h}(\mathbf{h}+1)}{2}$
23	1	16	986	108	13	13	13	6
29	2	24	8714	953	22	22	22	6
31	1	26	1737	187	19	19	19	6
37	2	37	13595	1383	36	36	36	6
41	3	50	29995	2901	129	129	129	10
43	1	55	3384	374	25	25	25	10
47	1	72	3967	397	39	39	39	15
53	2	93	28091	2887	60	60	60	15
59	1	125	6153	642	47	47	47	21

Complexity analysis. We consider the simplest case $p \equiv 3 \pmod 4$, and study the time complexity of $\mathsf{allRHI}(p,1,2p,3p)$. It makes $O(p)$ calls to $\mathsf{polzSQI}$ leading to the set of polarizations Θ_m, and $\#\Theta_m = O(p^4)$ calls to RHI.

- $\mathsf{polzSQI}(p, m)$. This essentially uses modular arithmetic to solve $w^2 + x^2 + py^2 + pz^2 = m$ over $\mathbb{Z}/m\mathbb{Z}$. Since there are three nested loops of size $O(m)$, the overall complexity is $O(m^3)$. However, since $2p \leq m \leq p$, we get $m = O(p)$ and overall runtime complexity of $O(p^3)$. However, on average, the break statements lead to a runtime complexity of $O(m^2) = O(p^2)$.
- $\mathsf{RHI}(p, 1, \theta)$. It starts by constructing a 6×6 matrix A with entries of size $O(p^4)$. Then it makes at most one call to each of $\mathsf{indefiniteLLL}$ and $\mathsf{minVector}$.
  - $\mathsf{indefiniteLLL}(A)$. The input is a 6-dimensional positive semi-definite Gram matrix A. First, it uses Hermite normal form to remove the kernel from A and obtain a 5-dimensional positive definite Gram matrix $\tilde{A}$ [5, §2.4.3]. Next it applies the Lenstra-Lenstra-Lovász (LLL) algorithm to $\tilde{A}$ to output A' [5, §2.6]. Due to the fixed dimension of the input matrices, the overall computation complexity is dominated by the size of the entries of the input matrix. Therefore, the runtime of this step is $O(\log^k(N))$ where k is some constant and $N = O(p^4)$ is the size of the entries, i.e., overall time complexity is $O(\log^k(p))$.
  - $\mathsf{minVector}(L_{A'})$. The input is the LLL-reduced 5-dimensional positive definite lattice $L_{A'}$. The lattice enumeration step dominates overall complexity with exponential time complexity $O(c^n)$ where $c > 1$ depends on the lattice geometry and $n = 5$ is the dimension of the lattice [5, §2.7.3].
- $\mathsf{isIsometric}(L_A, L_{A'})$. The first step requires the enumeration of (many) short lattice vectors. For small dimensions, this is made practical by considering (geometric) invariants to improve the search [68, §9.4]. We can say that it has exponential time complexity $O(\exp(f(a, b)))$ in the worst case, where f is a function of a (the number of short vectors) and b (the size of the automorphism group of the lattices).

Therefore, our algorithm has a complicated exponential time complexity, which is dominated by $\mathsf{isIsometric}$ that is called $O(p^5)$ times.

3.4 Experiment

We start with a supersingular product surface $\mathcal{A} = E_1 \times E_2$ where E_1 and E_2 are unknown supersingular elliptic curves. We choose a principal (canonical) product polarization $\theta_{E_1 \times E_2}$, and a random divisor D on $E_1 \times E_2$. We then calculate the refined Humbert invariant by using Algorithm 1 with the use of intersection formulas for various principal polarizations from Algorithm 2 or Algorithm 3, and then use Equation (8) to extract the degree map. Hence, checking the existence of N-isogenies between two supersingular elliptic curves E_1 and E_2 over $\overline{\mathbb{F}}_p$ is equivalent to checking the existence of a solution of the degree map for a given fixed p and varying N, and no explicit solution is needed.

Thus, in terms of the bound on the maximum of minimum degrees of supersingular isogenies, we would like to find the minimum values represented by such degree maps, as they are exactly the minimum degree isogenies between two supersingular elliptic curves. That is, we seek to understand how the following

value varies as we vary p:

$$d := \max_{q_{E_1,E_2}} \{\min\{N : q_{E_1,E_2}(t_1,t_2,t_3,t_4) = N \text{ for some } t_1,t_2,t_3,t_4 \in \mathbb{Z}\}\}. \quad (14)$$

Here, we directly compute the degree maps from refined Humbert invariants without KLPT, and our input does not depend on the chosen elliptic curves E_1 and E_2. Hence, we can test the degree maps (see Definition 4) on average varying over different elliptic curves.

We implemented all the algorithms from Section 3 using a Julia package called `OSCAR` [62,7], especially using its dependency package `Nemo/Hecke` [15]. The code and data are available at:

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

Our experiment involves running Algorithm 4 for $a = 2\ell p$ and $b = 2\ell p + p$, which serve as the lower and upper bounds on the m values in the principal polarization $\theta = \left(\begin{smallmatrix} m & \alpha_0 \\ \overline{\alpha_0} & m \end{smallmatrix}\right)$. We then use (8) to extract the degree map and compute the value of d defined in (14).

Table 2 below summarizes our findings for all primes $20 < p < 200$. We observe that $d^2 \approx \ell p$, which is illustrated by the plot in Figure 1.

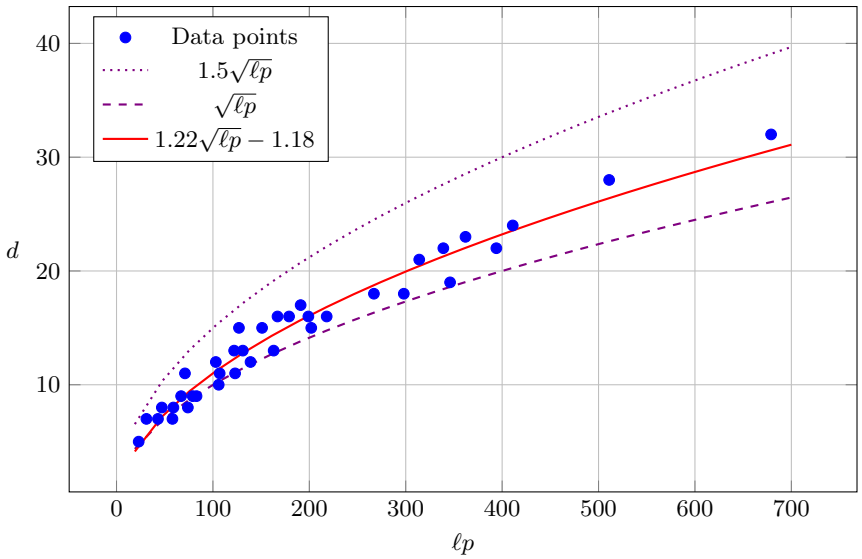

Fig. 1. Visualizing the data collected in Table 2 for all primes up to 200 (except $p = 193$).

Special case: $p \equiv 3 \pmod 4$. Note that in SQIsign-variants and other isogeny schemes, we mostly work with primes $p \equiv 3 \pmod 4$ with $B_p = (-1, -p|\mathbb{Q})$.

Table 2. We get the following results for $\mathsf{allRHI}(p, \ell, 2\ell p, 2\ell p + p)$ for primes $20 < p < 200$. Here, d is the maximum of all minimum degrees. The primes marked with * are the ones for which a new quintic refined Humbert invariant was obtained for $m \approx 2\ell p + p$.

p	ℓ	$\mathbf{H}$	$\#\Theta$	$\#\mathrm{RHI}_{\mathrm{red}}$	$\#\mathrm{RHI}_{\mathrm{iso}}$	$\frac{\mathbf{h}(\mathbf{h}+1)}{2}$	d	p	ℓ	$\mathbf{H}$	$\#\Theta$	$\#\mathrm{RHI}_{\mathrm{red}}$	$\#\mathrm{RHI}_{\mathrm{iso}}$	$\frac{\mathbf{h}(\mathbf{h}+1)}{2}$	d
23	1	16	986	108	13	6	5	107	1	581	19811	1999	116	55	11
29	2	24	8714	953	22	6	7	109	2	600	116970	12245	218	45	16
31	1	26	1737	187	19	6	7	113	3	668	227036	21225	871	55	22
37	2	37	13595	1383	36	6	8	127	1	918	27928	2703	165	66	15
41	3	50	29995	2901	129	10	11	131	1	1008	29643	2952	182	78	13
43	1	55	3384	374	25	10	7	137	3	1134	331472	30693	1255	78	24
47*	1	72	3967	397	39	15	8	139*	1	1179	33245	3263	187	78	12
53	2	93	28091	2887	60	15	10	149	2	1433	217553	21793	394	91	18
59	1	125	6153	642	47	21	8	151	1	1484	39203	3817	228	91	15
61	2	128	37004	3893	80	15	13	157	2	1648	240719	24759	464	91	21
67	1	166	8066	841	52	21	9	163	1	1838	45867	4542	246	105	13
71*	1	198	8939	892	75	28	11	167	1	1978	47627	4588	307	120	16
73	7	204	186550	16889	1451	21	28	173	2	2176	292760	30318	524	120	19
79	1	256	10909	1086	75	28	9	179	1	2404	54447	5304	305	136	16
83	1	296	12023	1223	79	36	9	181	2	2461	318911	32417	578	120	23
89	3	352	139886	12898	546	36	18	191	1	2886	62475	5947	397	153	17
97	7	436	327338	29563	2514	36	32	193	11	2952	—	—	2519	136	55
101	2	493	100944	10092	196	45	15	197	2	3141	377338	37975	662	153	22
103	1	518	18476	1827	123	45	12	199	1	3230	67288	6515	389	153	16

Our second experiment involves running Algorithm 4 for $a = 2p$ and $b = 3p$, which serve as the lower and upper bounds on the m values in the principal polarization $\theta = \left(\begin{smallmatrix} m & \alpha_0 \\ \overline{\alpha_0} & m \end{smallmatrix}\right)$. Table 3 below summarizes our findings for all primes $200 < p < 730$ such that $p \equiv 3 \pmod 4$. We observe that the minimum isogeny degree d has an average complexity of $p^{1/2}$ (see Figure 2).

Furthermore, we can use our data to study the minimum degree distribution for a given prime. For example, Figure 3 contains the frequency bar graph for $p = 647$.

Remark 5. Most of the data in this paper was obtained using a high-performance computing cluster, as there were a lot of computations involved. This is because we wanted to push the computational limits for finding all refined Humbert invariants up to different bounds. We tried to find all integral quadratic forms satisfying the conditions, but there were simply too many of them that couldn't be handled by a classical computer.

Table 3. We get the following results for $\mathsf{allRHI}(p, 1, 2p, 3p)$ where p is one of the 43 primes $p > 200$ and $p \equiv 3 \pmod 4$. The primes marked with * are the ones for which a new quintic refined Humbert invariant was obtained for $m \approx 3p$.

p	$\mathbf{H}$	$\#\Theta$	$\#\mathrm{RHI}_{\mathrm{red}}$	$\#\mathrm{RHI}_{\mathrm{iso}}$	$\frac{\mathbf{h}(\mathbf{h}+1)}{2}$	d	p	$\mathbf{H}$	$\#\Theta$	$\#\mathrm{RHI}_{\mathrm{red}}$	$\#\mathrm{RHI}_{\mathrm{iso}}$	$\frac{\mathbf{h}(\mathbf{h}+1)}{2}$	d
211	3814	75944	7378	390	171	16	467	38024	366216	34548	1846	820	25
223	4466	84610	8163	475	190	17	479	40958	384495	36110	2181	861	28
227	4712	87649	8418	468	210	18	487	42966	399110	37537	1986	861	27
239	5460	96478	9251	594	231	20	491	44037	404169	38187	2046	903	27
251*	6281	106861	10337	589	253	19	499	46146	417908	39560	2047	903	28
263	7182	116991	11195	667	276	19	503	47268	423320	39858	2281	946	29
271	7812	125139	11921	690	276	21	523	52967	459780	43388	2294	990	27
283	8851	135598	13039	704	300	21	547	60430	502191	47454	2445	1081	28
307	11198	158914	15200	825	351	20	563	65808	530513	50238	2661	1176	29
311	11644	162544	15507	985	378	21	571	68563	545586	51682	2665	1176	31
331	13927	185313	17682	928	406	23	587	74405	577500	54265	2857	1275	28
347	15993	203905	19309	1020	465	23	599	78972	600362	56507	3204	1326	30
359	17654	217351	20594	1243	496	24	607	82082	616645	57955	3098	1326	30
367	18800	227167	21443	1193	496	24	619	86955	641079	60539	3164	1378	29
379	20647	242478	23050	1201	528	24	631	92016	666927	62661	3324	1431	32
383	21310	246557	23088	1362	561	24	643	97270	—	—	3435	1485	33
419	27692	294345	27909	1528	666	25	647	99102	699249	65693	3650	1540	35
431	30072	311390	29520	1735	703	25	659	104620	—	—	3623	1596	32
439	37052	323986	30569	1693	703	27	683	116261	—	—	3778	1711	31
443	32585	329752	31172	1633	741	27	691	120286	—	—	3896	1711	32
463	37052	359620	34194	1815	780	25	719	135296	—	—	4612	1891	36
							727	139748	—	—	4418	1891	33

4 Applications to supersingular isogeny degrees

The efficient computation of refined Humbert invariants is an open avenue to work on a variety of isogeny problems. The first appearance of refined Humbert invariants in isogeny-based cryptography appeared in [41], where it was shown that the computational refined Humbert invariant problem is equivalent to the computational isogeny problem (for SQIsign and CSIDH). Another application of refined Humbert invariants is developed in [40] to understand the splitting behaviors of principally polarized superspecial abelian surfaces.

We would like to stress that the efficient computation of refined Humbert invariants of principally polarized abelian surfaces is very effective in detecting the product polarizations, as done above by using irreducibility criteria. Proposition 2. This might have a great potential for certain applications in isogeny-based schemes of abelian surfaces. Unfortunately, there is no direct algorithm to compute these invariants starting from the elliptic curve equations in the literature yet.

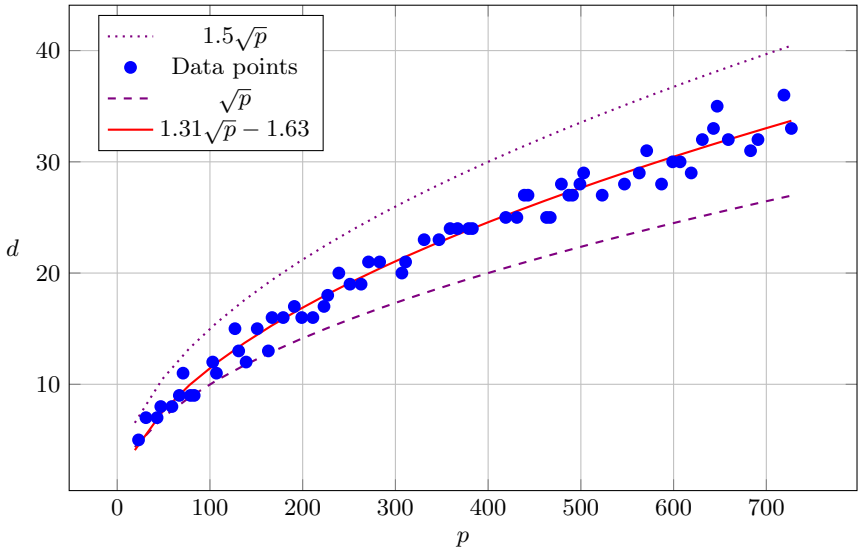

Fig. 2. Visualizing the data collected in Table 2 and Table 3 for first 63 primes $p > 20$ and $p \equiv 3 \pmod 4$.

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 allows us to use the intersection theory of divisors on surfaces, see [20, §V.1] and [58, §4.1], and only the degrees of isogenies are used rather than isogenies themselves in the intersection formulas. At first sight, it might appear that we are just considering the degree map q_{E_1,E_2} on $\mathrm{Hom}(E_1, E_2)$ by the equivalence given in (8). However, to the best of our knowledge, there is no generic method to understand degree maps on q_{E_1,E_2} on $\mathrm{Hom}(E_1, E_2)$ without knowing the equations defining E_1 and E_2.

What is known about the degrees of isogenies can be summarized as follows. The output of the KLPT algorithm [44] gives an equivalent ideal of norm too big, i.e., an isogeny of big degree, which is roughly around $\approx p^{15/4}$. Later, it was improved to $\approx p^3$ in [54]. This issue was reconsidered in SQIsign [13] by designing a new algorithm with a slightly bigger output, the Generalized KLPT algorithm, and tailoring it for their new signature scheme [3, §2.5]. In KLPT-based SQIsign, signature isogenies are required to have smooth degrees. However, the isogeny of the smallest degree between two supersingular elliptic curves typically does not meet this smoothness requirement. As a result, small isogeny degrees cannot be directly used for generating signatures. To eliminate this problem, signature schemes including isogenies between abelian surfaces are designed [6,49,1,9] by using a technical result [27, Theorem 2.3] due to Kani.

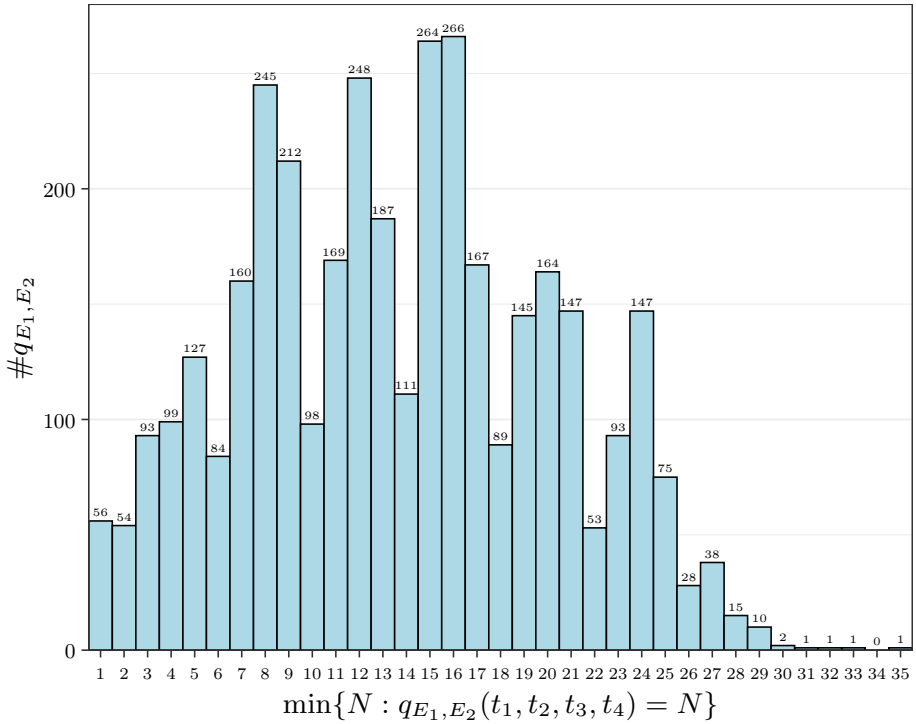

Fig. 3. For $p = 647$ and $\ell = 1$, we checked $699,249$ polarizations leading to $65,693$ quintic refined Humbert invariants belonging to one of the $3,650$ isometry classes of the form $t_0^2 + 4q_{E_1,E_2}(t_1,t_2,t_3,t_4)$. Here we see the distribution of minimum values of all the degree maps q_{E_1,E_2} we obtained.

Assumption on the upper bound on minimum isogeny degrees without endomorphism rings. We show that the upper bound on the minimum degree of an isogeny that is attained by any pair of supersingular elliptic curves is as small as $\approx 1.22\sqrt{\ell p}$. If one can compute the refined Humbert invariant $q_{(\mathcal{A},\theta)}$ of a principally polarized superspecial abelian surface $\mathcal{A} = E_1 \times E_2$ without the knowledge of either $\mathrm{End}(E_i)$ for $i = 1, 2$, then it is possible to find the smallest degree of an isogeny between E_1 and E_2. The advantage of refined Humbert invariants is that this problem can be worked on in average. Our experiments, see Section 3.4, show that the maximum of all the minimum degree isogenies attained with every pair of supersingular elliptic curves for the primes of the form $p \equiv 3 \pmod 4$, it is upper bounded on average by $\approx 1.31p^{1/2}$.

Our approach to studying degree forms using refined Humbert invariants enables us to obtain the minimum degree frequency distribution, as shown in the histogram in Figure 3 for $p = 647$. Such frequency distributions illustrate the well-known results, like:

1. random pairs of supersingular elliptic curves over $\mathbb{F}_{p^2}$ are unlikely to be connected by isogenies of degrees significantly smaller than $\sqrt{p}$ [18, §4.2]; and
2. there is always a minimum isogeny degree value smaller than $\approx 0.9\sqrt{p}$ [6, Lemma 12], [12, §2.1].

The fixed degree isogeny problem. In isogeny-based cryptography, two key computational problems are the pure isogeny problem and the endomorphism ring problem. Wesolowski [67] established a security reduction between computing an isogeny between supersingular elliptic curves and determining their endomorphism ring. Later, it was shown that finding non-scalar endomorphisms is equivalent to solving the endomorphism ring problem [53].

In certain applications, specialization of isogeny problems with extra information is utilized, such as fixing the degree of the isogeny. We aim to understand the so-called *fixed degree isogeny problem* in detail. The problem says that 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. In [18], it was mentioned that finding a fixed-degree isogeny is only known to be equivalent to endomorphism ring computations if the isogeny degree is smaller than $\sqrt{p}$, where p is the characteristic of the finite field.

We address the problem of identifying isogenies of fixed degree between two random supersingular elliptic curves, which is a significant problem in isogeny-based cryptography. For isogenies of large degree, this can be efficiently solved by the KLPT algorithm [44] or the generalized KLPT algorithm [13]. For small isogeny degrees, usual lattice reduction techniques are sufficient. The intermediate range of isogeny degrees was recently investigated in [2]; the improved algorithms for the fixed degree isogeny problem with the given endomorphism rings were worked out in detail. Furthermore, a heuristic algorithm is provided in [12] that operates in polynomial time for any degree d, under the condition that both orders are oriented and possess a small class number.

Heuristically, it is believed that an isogeny of smooth degree $\approx p$ exists, yet no efficient algorithm is currently known for finding such an isogeny. The best-known classical methods, including exhaustive search and meet-in-the-middle strategies, all remain exponential in cost. The improved algorithms using techniques such as Cornacchia's algorithm and multivariate Coppersmith methods were introduced in [2], which offer better performance for certain ranges of degrees; especially when the degree is sufficiently smooth, they focus on the "middle" isogeny degree cases, i.e, isogenies of degrees between $p^{1/2}$ and p^3, see the discussion in [2, §3]. Nonetheless, these approaches still rely on heuristics or partial guessing of variables and do not yield a general polynomial-time solution.

The difference of our technique is no assumption on the endomorphism rings. We compute all the degree maps that can appear over a fixed field; this is done by the intersection theory of abelian surfaces. We first calculate quintic refined Humbert invariants of principally polarized superspecial abelian surfaces and then the degree maps (quaternary integral quadratic forms). Then, we can

use known methods to work out the existence of a solution of the degree map q_{E_1,E_2}, like p-adic methods. Different from [2], here we do not compute an isogeny between two given supersingular elliptic curves by using a variant of KLPT or any endomorphism ring of elliptic curves.

We just compute a random (candidate) refined Humbert invariant corresponding to a principally polarized superspecial surface $(\mathcal{A}, \theta)$ where $\mathcal{A} = E \times E'$ with a product polarization θ. Then calculate the degree map on $\mathrm{Hom}(E_1, E_2)$. As we find a random degree map, we just need the existence of a solution rather than finding a solution. The isogeny degrees between $p^{1/2}$ and p^3 can be worked out easily with our method.

The minimum isogeny degree complexity. The minimum isogeny complexity is around $\simeq p^{1/2}$, and this was proved by different methods as follows. Galbraith, Petit, Shani, and Ti demonstrated that if the degree of an isogeny $\simeq p^{1/2}$ or shorter, the isogeny is mostly the shortest isogeny between the two supersingular curves [18, §4.2]. Therein, they use the property of Ramanujan graphs and give a counting argument to achieve this bound; however, the collisions are not considered in their approach; but, it is known that there are very few collisions for degrees $\leq \sqrt{p}$ as worked out in [47].

Another proven bound is established in [6, Lemma 12]; the minimum degree of isogenies between two supersingular elliptic curves is bounded above by $2\sqrt{2p}/\pi$. Here, this was achieved by lattice reduction and successive minima, and given the endomorphism ring. It was also mentioned with a different perspective in [47, Theorem 1.3(a)] by using non-scalar endomorphisms.

However, there is currently no proof about the sharpness of these proven bounds. This is precisely where our experiments, based on degree maps derived from refined Humbert invariants, become relevant. We provide strong evidence supporting the validity of the above bounds, while also highlighting the need for further work to sharpen the established bounds. We demonstrate evidence on this complexity by calculating the refined Humbert invariant $q_{(\mathcal{A},\theta)}$ and then extracting degree maps q_{E_1,E_2}, and we compute this invariant without using any information related to endomorphism rings.

Our data list all the possible degree maps q_{E_1,E_2} over a finite field of characteristic p. For a fixed finite field, we listed all possible refined Humbert invariants of a principally polarized superspecial abelian surface $(\mathcal{A}, \theta) = (E_1 \times E_2, \theta_{E_1 \times E_2})$, then we list all the possible degree maps q_{E_1,E_2} which can appear over the prescribed field. We reduce all the degree maps obtained using LLLreduction[15], and their first coefficient is the smallest integer represented by this form, namely the minimum isogeny degree between E_1 and E_2. We apply the same procedure for all the degree maps for each prime in our data. The data of all the degree maps can be used to understand the frequency of the minimum isogeny, and there are mostly repetitions. For instance, the distribution for $p = 647$ and $\ell = 1$ is demonstrated in Figure 3. For every prime up to $p = 727$, we computed all the degree

[15] This is equivalent to Minkowski reduced form, see [50, Theorem 2.2.2], as the degree map has 4 variables in our computations.

maps, and we can verify these bounds with a distribution of minimum isogenies, similar to the case of $p = 647$ as in Figure 3. To the best of our knowledge, this is the first time that experimental data has been used to support these bounds.

Acknowledgments. Thanks to Harun Kır and Chloe Martindale for proofreading the paper, and to Craig Costello, Tommy Hofmann, William C. Jagy, Aurel Page, Christophe Petit, and John Voight for useful discussions.
The first author was partially funded by the grant EPSRC 8459-DTP-IILF.
This work was carried out using the computational facilities of the Advanced Computing Research Centre, University of Bristol - http://www.bristol.ac.uk/acrc/.
Author list in alphabetical order; see https://ams.org/profession/leaders/CultureStatement04.pdf.

References

1. Basso, A., Dartois, P., Feo, L.D., Leroux, A., Maino, L., Pope, G., Robert, D., Wesolowski, B.: SQIsign2D-West - The Fast, the Small, and the Safer. In: Advances in Cryptology - ASIACRYPT 2024. LNCS, vol. 15486, pp. 339–370. Springer (2024)
2. Bencina, B., Kutas, P., Merz, S., Petit, C., Stopar, M., Weitkämper, C.: Improved algorithms for finding fixed-degree isogenies between supersingular elliptic curves. In: Advances in Cryptology - CRYPTO 2024. LNCS, vol. 14924, pp. 183–217. Springer (2024)
3. Beullens, W., De Feo, L., Galbraith, S.D., Petit, C.: Proving knowledge of isogenies: a survey. Des. Codes Cryptogr. **91**(11), 3425–3456 (2023)
4. Chávez-Saab, J., Corte-Real Santos, M., De Feo, L., Eriksen, J.K., Hess, B., Kohel, D., Leroux, A., Longa, P., Meyer, M., Panny, L., Patranabis, S., Petit, C., Rodríguez-Henríquez, F., Schaeffler, S., Wesolowski, B.: SQIsign version 1.0. Tech. rep., National Institute of Standards and Technology (2023), https://sqisign.org/spec/sqisign-20230601.pdf
5. Cohen, H.: A course in computational algebraic number theory, Graduate Texts in Mathematics, vol. 138. Springer-Verlag, Berlin (1993)
6. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQIsignHD: New Dimensions in Cryptography. In: Advances in Cryptology - EUROCRYPT 2024. LNCS, vol. 14651, pp. 3–32. Springer (2024)
7. 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)
8. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hansischen Univ. **14**, 197–272 (1941)
9. Duparc, M., Fouotsa, T.B.: SQIPrime: A Dimension 2 Variant of SQISignHD with Non-smooth Challenge Isogenies. In: Advances in Cryptology - ASIACRYPT 2024. LNCS, vol. 15486, pp. 396–429. Springer (2024)
10. Eichler, M.: Über die idealklassenzahl total definiter quaternionenalgebren. Mathematische Zeitschrift **43**, 102–109 (1938)
11. 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)

12. Eriksen, J.K., Leroux, A.: Computing orientations from the endomorphism ring of supersingular curves and applications. IACR Communications in Cryptology **1**(3) (2024). https://doi.org/10.62056/ae0fhbmo
13. Feo, L.D., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: Compact post-quantum signatures from quaternions and isogenies. In: Advances in Cryptology - ASIACRYPT 2020. LNCS, vol. 12491, pp. 64–93. Springer (2020)
14. Feo, L.D., Leroux, A., Longa, P., Wesolowski, B.: New Algorithms for the Deuring Correspondence - Towards Practical and Secure SQISign Signatures. In: Advances in Cryptology - EUROCRYPT 2023. LNCS, vol. 14008, pp. 659–690. Springer (2023)
15. 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)
16. Fincke, U., Pohst, M.: Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. Math. Comp. **44**(170), 463–471 (1985)
17. Fulton, W.: 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
18. Galbraith, S.D., Petit, C., Shani, B., Ti, Y.B.: On the security of supersingular isogeny cryptosystems. In: Advances in cryptology—ASIACRYPT 2016. Part I, Lecture Notes in Comput. Sci., vol. 10031, pp. 63–91. Springer, Berlin (2016)
19. Grieve, N.: Reduced norms and the Riemann-Roch theorem for Abelian varieties. New York J. Math. **23**, 1087–1110 (2017)
20. Hartshorne, R.: Algebraic geometry, Graduate Texts in Mathematics, vol. 52. Springer-Verlag, New York-Heidelberg (1977)
21. Hashimoto, K., Ibukiyama, T.: On class numbers of positive definite binary quaternion Hermitian forms. J. Fac. Sci. Univ. Tokyo Sect. IA Math. **27**(3), 549–601 (1980)
22. Ibukiyama, T.: Supersingular abelian varieties and quaternion hermitian lattices. In: Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties, RIMS Kôkyûroku Bessatsu, vol. B90, pp. 17–37. Res. Inst. Math. Sci. (RIMS), Kyoto (2022), http://hdl.handle.net/2433/276271
23. Ibukiyama, T., Katsura, T.: On the field of definition of superspecial polarized abelian varieties and type numbers. Compositio Mathematica **91**(1), 37–46 (1994)
24. Ibukiyama, T., Katsura, T., Oort, F.: Supersingular curves of genus two and class numbers. Compositio Math. **57**(2), 127–152 (1986)
25. Igusa, J.i.: Class number of a definite quaternion with prime discriminant. Proc. Nat. Acad. Sci. U.S.A. **44**, 312–314 (1958)
26. Kani, E.: Elliptic curves on abelian surfaces. Manuscripta mathematica **84**, 199–223 (1994)
27. Kani, E.: The number of curves of genus two with elliptic differentials. JJournal für die reine und angewandte Mathematik 485 p. 93–122 (1997), http://www.mathjournals.org/jrms/2014-029-001/2014-029-001-003.html
28. Kani, E.: Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms. Journal of Number Theory p. 139:138–174 (2014)
29. Kani, E.: The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. Collect. Math. **67**, 21–54 (2016)
30. Kani, E.: Elliptic subcovers of a curve of genus 2. II. The refined Humbert invariant. Journal of Number Theory **193**, 302–335 (2018)

31. Kani, E.: Elliptic subcovers of a curve of genus 2. I. The isogeny defect. Annales mathématiques du Québec **43**, 281–303 (2019)
32. Kani, E.: Subcovers of curves and moduli spaces. In: Geometry at the frontier—symmetries and moduli spaces of algebraic varieties, Contemp. Math., vol. 766, pp. 229–250. Amer. Math. Soc. (2021)
33. Kani, E.: Principal polarizations on abelian product surfaces. Preprint (2024), https://mast.queensu.ca/~kani/papers/prinpol5.pdf
34. Kani, E., Kır, H.: The number of curves of genus 2 with a given refined Humbert invariant. Preprint (2023), https://mast.queensu.ca/~kani/papers/cardHq13.pdf
35. 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)
36. 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)
37. Kır, 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
38. Kır, H.: The classification of the refined humbert invariant for curves of genus 2. International Journal of Number Theory **21**(06), 1247–12791–33 (2025)
39. Kır, H.: The refined Humbert invariant for an automorphism group of a genus 2 curve. To appear on Contemporary Mathematics (2025), https://arxiv.org/abs/2310.19076
40. Kırımlı, E., Korpal, G.: Testing the folklore, detecting split surfaces, and minimum walks on isogeny graphs of abelian surfaces. Preprint (2025)
41. Kırımlı, E., Martindale, C.: The computational refined Humbert invariant problem is equivalent to the computational isogeny problem. Preprint (2024), https://eprint.iacr.org/2025/1295, https://eprint.iacr.org/2025/1295
42. Kneser, M.: Klassenzahlen definiter quadratischer Formen. Arch. Math. **8**, 241–250 (1957)
43. Kohel, D.: Endomorphism rings of elliptic curves over finite fields (1996)
44. Kohel, D., Lauter, K., Petit, C., Tignol, J.P.: On the quaternion ℓ-isogeny path problem. LMS J. Comput. Math. **17**, 418–432 (2014)
45. Lang, S.: Abelian varieties. Springer-Verlag New York (1983)
46. Li, K.Z., Oort, F.: Moduli of Supersingular Abelian Varieties, Lecture Notes in Mathematics, vol. 1680. Springer, Berlin (1998)
47. Love, J., Boneh, D.: Supersingular curves with small noninteger endomorphisms. In: ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium. Open Book Ser., vol. 4, pp. 7–22. Math. Sci. Publ., Berkeley, CA (2020)
48. Mumford, D.: Abelian Varieties. Oxford University Press, Oxford (1970)
49. Nakagawa, K., Onuki, H., Castryck, W., Chen, M., Invernizzi, R., Lorenzon, G., Vercauteren, F.: SQIsign2D-East: A New Signature Scheme Using 2-Dimensional Isogenies. In: Advances in Cryptology - ASIACRYPT 2024. LNCS, vol. 15486, pp. 272–303. Springer (2024)
50. Nguyen, P.Q., Stehlé, D.: Low-dimensional lattice basis reduction revisited. ACM Trans. Algorithms **5**(4), Art. 46, 48 (2009)
51. 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)
52. Oort, F.: Subvarieties of moduli spaces. Inventiones mathematicae **24**, 95–120 (1974)

53. Page, A., Wesolowski, B.: The supersingular endomorphism ring and one endomorphism problems are equivalent. In: Advances in Cryptology - EUROCRYPT 2024. LNCS, vol. 14656, pp. 388–417. Springer (2024)
54. Petit, C., Smith, S.: An improvement to the quaternion analogue of the l-isogeny path problem. MathCrypt (2018)
55. Plesken, W., Souvignier, B.: Computing isometries of lattices. J. Symbolic Comput. **24**(3-4), 327–334 (1997), computational algebra and number theory (London, 1993)
56. Pujol, X., Stehlé, D.: Rigorous and efficient short lattice vectors enumeration. In: Advances in cryptology—ASIACRYPT 2008, Lecture Notes in Comput. Sci., vol. 5350, pp. 390–405. Springer, Berlin (2008)
57. Schulze-Pillot, R.: Lecture notes on quadratic forms and their arithmetic (2021), https://arxiv.org/abs/2008.12847
58. Shafarevich, I.R.: Basic algebraic geometry. 1. Springer, Heidelberg, third edn. (2013), varieties in projective space
59. Shioda, T.: Supersingular $K3$ surfaces. In: Algebraic Geometry. Lecture Notes in Math., vol. 732, pp. 564–591. Springer Berlin (1979)
60. Silverman, J.H.: The arithmetic of elliptic curves. Graduate Texts in Mathematics, vol. 106. Springer, New York (2009)
61. Simon, D.: Solving quadratic equations using reduced unimodular quadratic forms. Math. Comp. **74**(251), 1531–1543 (2005)
62. The OSCAR Team: OSCAR – Open Source Computer Algebra Research system, Version 1.2.2 (2024), https://www.oscar-system.org
63. Voight, J.: Quaternion Algebras, Graduate Texts in Mathematics, vol. 288. Springer International Publishing (2021), errata and addenda: http://quatalg.org
64. Voight, J.: Kneser's method of neighbors. Arch. Math. (Basel) **121**(5-6), 537–557 (2023)
65. 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)
66. Weil, A.: Zum beweis des torellischen satzes. In: Nachr. Akad. Wiss. Gottingen. Math.-Phys. Kl. IIa. pp. 33–55 (1957)
67. Wesolowski, B.: The supersingular isogeny path and endomorphism ring problems are equivalent. In: 62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS. pp. 1100–1111. IEEE (2021)
68. Woerden, W.v.: Lattice cryptography: from cryptanalysis to New Foundations. Ph.D. thesis, Leiden University (2023), https://hdl.handle.net/1887/3564770