

The computational refined Humbert invariant problem is equivalent to the computational isogeny problem

Eda Kirimli^{1,2,3} and Chloe Martindale¹

¹ University of Bristol, UK

² Université de Neuchâtel, Switzerland

³ University of Birmingham, UK

eda.kirimli@bristol.ac.uk

chloe.martindale@bristol.ac.uk

Abstract. In this paper, we discuss *refined Humbert invariants*, introduced by Kani in [26]. We show that in the contexts of SQISign and CSIDH, under GRH, the computational isogeny problem is polynomially equivalent to the computational refined Humbert invariant problem. This includes an algorithm to compute the basis of a maximal order of a quaternion algebra given its norm form. Finally, we also review what is known in the literature about computing refined Humbert invariants.

Keywords: Isogenies · Abelian surfaces · Refined Humbert invariants

Introduction

Every primitive in isogeny-based cryptography depends on a variant of *the computational isogeny problem*: given two elliptic curves E and E' defined over a finite field, find and compute an isogeny from E to E' (if it exists). The properties of the elliptic curves determine the relative difficulty of this problem. Two particular cases of interest are an isogeny problem underlying SQISign [12], in which E and E' are supersingular elliptic curves defined over \mathbb{F}_{p^2} , and an isogeny problem underlying CSIDH [7], in which E and E' are supersingular elliptic curves defined over \mathbb{F}_p .

In this paper, we study arithmetic invariants that are closely related to the isogeny problem, namely *refined Humbert invariants*, introduced by Kani [26] in 1994. These are (isomorphism) invariants of the ‘polarized Néron-Severi group’ of principally polarized abelian surfaces, the computation of which is also a difficult problem that has been studied extensively, especially in the work of Kani [26,29,30,31], and are described simply as equivalence classes of certain integral quadratic forms. We will show in Theorem 2 that, under GRH, computing the quintic (5-variable) refined Humbert invariant of a principally polarized superspecial surface defined over \mathbb{F}_{p^2} is polynomially equivalent to the isogeny problem in this context. Similarly, we will show in Theorem 3 that, under GRH, computing the ternary (3-variable) refined Humbert invariant of a principally

polarized superspecial surface defined over \mathbb{F}_p , in the appropriate context, is polynomially equivalent to the CSIDH isogeny problem.

Our work provides a different approach to computational isogeny problems by the use of arithmetically rich refined Humbert invariants of principally polarized abelian surfaces. On the surface, Theorems 2 and 3 are not surprising: a refined Humbert invariant of a principally polarized abelian surface has close connections to its symmetric endomorphism ring. Our work does, however, place the isogeny problem in a new light that highlights the geometric context and it may lead to new insights. To this end, we also provide a summary of the existing known algorithms for refined Humbert invariants.

The outline of the paper is as follows. In Section 1, we give preliminaries on arithmetic tools, geometric tools and refined Humbert invariants (which are equivalence classes of certain quadratic forms). In Section 2, we prove Theorem 2 and Theorem 3: that, under GRH, the computational refined Humbert invariant problem is polynomially equivalent to (certain instantiations of) the computational isogeny problem for supersingular elliptic curves over \mathbb{F}_{p^2} and \mathbb{F}_p respectively. In Section 3, we place the computational refined Humbert invariant problems of Section 2 in their more general context and give an overview of the existing literature on the topic. Finally, we briefly mention some applications that are already within reach.

Acknowledgments. The authors would like to thank John Voight for suggesting an improvement especially regarding Algorithm 1, Harun Kir for proofreading the document, and Péter Kutas, Jonathan Love, and Julian Lyczak for the fruitful discussions. The first author was partially funded by EPSRC (8459-DTP-IILF).

1 Preliminaries

In this section, we summarize the relevant aspects of quadratic forms, quaternion algebras, abelian varieties, and the theory of refined Humbert invariants. We refer to [19] for a more extensive survey discussing the relationship with isogeny-based cryptography.

1.1 Integral Quadratic forms

Firstly, we summarize basic concepts and facts regarding quadratic forms. The main references are [6,13,24,66].

Definition 1. Let R be a commutative ring. A quadratic form over R is a polynomial $f(x_1, \dots, x_n)$ of the form

$$f = f(x_1, \dots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j,$$

where $a_{ij} \in R$. If $R = \mathbb{Z}$, we say that f is an integral quadratic form.

Consider an integral quadratic form with $n = 2$ variables

$$f(x_1, x_2) = a_{11}x_1^2 + a_{12}x_1x_2 + a_{22}x_2^2.$$

When $n = 2$, we say that f is an *integral binary quadratic form*, which we also denote by

$$[a_{11}, a_{12}, a_{22}].$$

Consider an integral quadratic form with $n = 3$ variables

$$f(x_1, x_2, x_3) = a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + a_{23}x_2x_3 + a_{13}x_1x_3 + a_{12}x_1x_2.$$

When $n = 3$, we say that f is an *integral ternary quadratic form*, which we also denote by

$$[a_{11}, a_{22}, a_{33}, a_{23}, a_{13}, a_{12}].$$

Quadratic forms with 1, 2, 3, 4, 5, and n variables are referred to as unary, binary, ternary, quaternary, quintic⁴, and n -ary respectively.

The variables x_1, x_2, \dots, x_n of an n -ary quadratic form can be viewed as the elements of the column vector, i.e., $n \times 1$ matrix, $x = (x_1, \dots, x_n)^t$. There is a unique symmetric matrix M_f such that the quadratic form f can be expressed as $f(x) = \frac{1}{2}x^t M_f x$. We will refer to the matrix M_f as the *coefficient matrix* of f (this is consistent with Kani's notation [26]). We will refer to $\frac{1}{2}M_f$ as the *Gram matrix* of f (this is consistent with SageMath [59] and Magma [4]). For simplicity, the notation $\det(f)$ is used instead of $\det(M_f)$. The *discriminant* of f is defined as

$$\Delta(f) = \begin{cases} (-1)^{\frac{n}{2}} \det(f) & \text{if } n \text{ is even,} \\ \frac{1}{2}(-1)^{\frac{n-1}{2}} \det(f) & \text{if } n \text{ is odd.} \end{cases} \quad (1)$$

In what follows, the discriminant will always be nonzero. The discriminant of an integral binary quadratic form for $f = [a_{11}, a_{12}, a_{22}]$ is $\Delta(f) = a_{12}^2 - 4a_{11}a_{22}$. A discriminant $\Delta = \Delta(f)$ of an integral binary quadratic form is a *fundamental discriminant* if either Δ is a square-free or $\frac{\Delta}{4}$ is a square-free and $\frac{\Delta}{4} \not\equiv 1 \pmod{4}$. The discriminant of an integral ternary quadratic form $f = [a, b, c, r, s, t]$ is

$$\Delta(f) = -4abc - rst + ar^2 + bs^2 + ct^2. \quad (2)$$

An integral quadratic form f represents a number m if there is an integral solution $x = (x_1, \dots, x_n) \neq 0$ such that $f(x) = m$. The integral quadratic form f primitively represents m if there is a primitive solution (x_1, \dots, x_n) , i.e., if $\gcd(x_1, \dots, x_n) = 1$.

An integral quadratic form f is called *positive definite* if, for $x \neq 0$, it only represents positive integers. If it represents both positive and negative integers, we say that the integral quadratic form f is *indefinite*. The *content* of an integral quadratic form f is the greatest common divisor of its coefficients, denoted by $\text{cont}(f)$. If $\text{cont}(f) = 1$, we say that it is a *primitive* form, otherwise, it is called *imprimitive*.

⁴ We use ‘quintic’ rather than ‘quinary’ in order to be consistent with [32]. A ‘quintic quadratic form’ therefore refers to a form in 5 variables of degree 2.

Definition 2. Let R be a commutative ring and let S be an R -module. A map

$$q : S \rightarrow R$$

is called a quadratic form if

- for all $\alpha \in R$ and $x \in S$, we have $q(\alpha x) = \alpha^2 q(x)$, and
- $\beta_q : (x, y) \mapsto q(x + y) - q(x) - q(y)$ from $S \times S$ to R is bilinear.

The (symmetric) bilinear form β_q is the bilinear form associated to q . A quadratic R -module is a pair of an R -module S with a quadratic form q on S .

Definition 3. A homomorphism of quadratic R -modules $(S, q) \rightarrow (S', q')$ is an R -linear map $\alpha : S \rightarrow S'$ such that $q = q' \circ \alpha$. If α is an R -linear isomorphism such that $q = q' \circ \alpha$, then α is called an isometry. The automorphism group of (S, q) is

$$\text{Aut}(S, q) = \{\alpha \in \text{Aut}_R(S) : q \circ \alpha = q\}.$$

A quadratic form f in n variables induces a map from R^n into R , i.e., $q(x) = f(x)$ where $x = (x_1, \dots, x_n)^t \in R^n$. Clearly, it satisfies $q(\alpha x) = \alpha^2 q(x)$ for all $\alpha \in R$ and $x \in R^n$. Thus (R^n, q) is a quadratic R -module.

We define a linear transformation for a quadratic form f in n variables in R as: if $T \in \text{GL}_n(R)$, the linear transformation fT of the form f by T is

$$(fT)(x) = f(Tx).$$

In terms of the coefficient matrices, it translates as

$$M_{fT} = T^t M_f T.$$

Definition 4. Let f_1, f_2 be n -ary quadratic forms in R . We say that two forms f_1 and f_2 are $\text{GL}_n(R)$ -equivalent (or R -equivalent) if there exists $T \in \text{GL}_n(R)$ such that $f_2 = f_1 T$.

Two n -ary quadratic forms f_1 and f_2 are R -equivalent if and only if the quadratic R -modules (R^n, f_1) and (R^n, f_2) are isomorphic. If f_1 and f_2 are \mathbb{Z} -equivalent integral quadratic forms, then we say that they are *equivalent*, and we use the symbol $f_1 \sim f_2$. If there exists $T \in \text{SL}_n(\mathbb{Z})$ such that $f_2 = f_1 T$, we say that they are *properly equivalent*, or $\text{SL}_n(\mathbb{Z})$ -equivalent, denoted by $f_1 \approx f_2$. Let \mathbb{Z}_p be the ring of p -adic integers. If f_1 and f_2 are quadratic forms in \mathbb{Z}_p for any prime p and they are \mathbb{Z}_p -equivalent, then we say that they are p -adically equivalent, denoted by $f_1 \sim_p f_2$. Finally, if f_1 and f_2 are quadratic forms in \mathbb{R} , and they are \mathbb{R} -equivalent, we use the symbol $f_1 \sim_\infty f_2$. Notice that two equivalent integral quadratic forms have the same discriminant, represent the same integers, and represent the same integers [66, p.6].

Definition 5. Let f be an n -ary integral quadratic form. An automorphism of the form f is a matrix $M \in \text{GL}_n(\mathbb{Z})$ such that $fM = f$. The automorphism group of f is

$$\text{Aut}(f) = \{M \in \text{GL}_n(\mathbb{Z}) : fM = f\}.$$

The positive automorphism group of f is $\text{Aut}^+(f) := \text{Aut}(f) \cap \text{SL}_n(\mathbb{Z})$.

Let f be an n -ary integral quadratic form. One can see that if $fM = f$, then the associated linear map $\alpha_M : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ defined by $\alpha_M(x) = Mx$ gives an automorphism of the quadratic module (\mathbb{Z}^n, f) and conversely. Thereby, it follows that $M \in \text{Aut}(f)$ if and only if $\alpha_M \in \text{Aut}(\mathbb{Z}^n, f)$.

Definition 6. Let f_1 and f_2 be integral quadratic forms. If, for all primes p including $p = \infty$, we have that $f_1 \sim_p f_2$, then f_1 and f_2 are genus-equivalent, denoted by $f_1 \simeq f_2$.

Two integral quadratic forms q_1 and q_2 with nonzero discriminant are genus equivalent if and only if $(xy - q_1) \sim (xy - q_2)$ [8, p. 378].

Definition 7. A ternary quadratic form $q = [a_1, a_2, a_3, a_4, a_5, a_6]$ is improperly primitive if $\text{cont}(q) = 2$ and at least one of the integers $\frac{a_4}{2}, \frac{a_5}{2}, \frac{a_6}{2}$ is odd.

Throughout this document, we call an element $s \in S$ of a finitely generated free \mathbb{Z} -module S primitive if the quotient module $S/\mathbb{Z}s$ is torsion-free. From now on, a quadratic form means an integral quadratic form unless otherwise stated.

1.2 Quaternion algebras

In this section, we summarize the necessary basics of quaternion algebras. We refer the reader to [63,64] for further details.

Definition 8. An algebra \mathcal{B} over a field K with $\text{char}(K) \neq 2$ is a quaternion algebra if there exist $1, \mathbf{i}, \mathbf{j} \in \mathcal{B}$ such that the set $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ is a K -basis for \mathcal{B} and there exist $a, b \in K^\times$ such that

$$\mathbf{i}\mathbf{i} = a, \quad \mathbf{j}\mathbf{j} = b, \quad \mathbf{i}\mathbf{j} = -\mathbf{j}\mathbf{i} = \mathbf{k}.$$

We denote \mathcal{B} by $(a, b|K)$.

Definition 9. Let $\mathcal{B} = (a, b|K)$ be a quaternion algebra with K -basis $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$. Let $\alpha = \alpha_0 + \alpha_1\mathbf{i} + \alpha_2\mathbf{j} + \alpha_3\mathbf{k} \in \mathcal{B}$. We define the conjugate of α to be

$$\bar{\alpha} = \alpha_0 - \alpha_1\mathbf{i} - \alpha_2\mathbf{j} - \alpha_3\mathbf{k},$$

the reduced norm of α to be

$$\text{nrd}(\alpha) = \alpha\bar{\alpha} \in K,$$

and the reduced trace of α to be

$$\text{trd}(\alpha) = \alpha + \bar{\alpha} \in K.$$

Definition 10. The reduced norm defines a quadratic form in 4 variables on \mathcal{B} , the norm form, given by

$$\text{nrd}(w + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}) = w^2 - ax^2 - by^2 + abz^2.$$

Example 1. Let p be a prime number. We denote by $\mathcal{B}_{p,\infty}$ a quaternion algebra over \mathbb{Q} ramifying only at p and ∞ . The quaternion algebra $\mathcal{B}_{p,\infty}$ has dimension 4 over \mathbb{Q} , and it is non-commutative. If $p \equiv 3 \pmod{4}$, the $\mathcal{B}_{p,\infty}$ has a \mathbb{Q} -basis given by $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ for which $\mathbf{i}^2 = -1, \mathbf{j}^2 = -p$ and $\mathbf{k} = \mathbf{i}\mathbf{j} = -\mathbf{j}\mathbf{i}$. Then

$$\bar{\alpha} = \alpha_0 - \alpha_1 \mathbf{i} - \alpha_2 \mathbf{j} - \alpha_3 \mathbf{k},$$

the reduced trace

$$\text{tr}(\alpha) = \alpha + \bar{\alpha} = 2\alpha_0,$$

and the *reduced norm*

$$\text{nrd}(\alpha) = \alpha \cdot \bar{\alpha} = \alpha_0^2 + \alpha_1^2 + p(\alpha_2^2 + \alpha_3^2) \in \mathbb{Q}.$$

Every non-zero element α of $\mathcal{B}_{p,\infty}$ is invertible, i.e., there is a unique $\alpha' \in \mathcal{B}_{p,\infty}$ satisfying $\alpha\alpha' = \alpha'\alpha = 1$.

Lemma 1 ([53]). *Let $p > 2$. The explicit presentations of definite quaternion algebras $\mathcal{B}_{p,\infty}$ over \mathbb{Q} ramified at p and ∞ with $\text{disc}(\mathcal{B}_{p,\infty}) = p$ are given by*

1. if $p = 2$ then $\mathcal{B}_{p,\infty} = (-1, -1 | \mathbb{Q})$;
2. if $p \equiv 3 \pmod{4}$ then $\mathcal{B}_{p,\infty} = (-1, -p | \mathbb{Q})$; and
3. if $p \equiv 5 \pmod{8}$ then $\mathcal{B}_{p,\infty} = (-2, -p | \mathbb{Q})$; and
4. if $p \equiv 1 \pmod{8}$ then $\mathcal{B}_{p,\infty} = (-s, -p | \mathbb{Q})$, where $s \equiv 3 \pmod{4}$ is a prime such that $\left(\frac{s}{p}\right) = -1$.

Definition 11. A quaternion order in $\mathcal{B}_{p,\infty}$ is a subring $\mathcal{O} \subset \mathcal{B}_{p,\infty}$ that is also a lattice, i.e., it has rank 4 as a \mathbb{Z} -module. An order is maximal when it is not contained in any other order.

Definition 12. Let I be a \mathbb{Z} -module rank of 4 in $\mathcal{B}_{p,\infty}$. The left order of I is defined as $\mathcal{O}_L(I) = \{\sigma \in \mathcal{B}_{p,\infty} : \sigma I \subset I\}$. Similarly, the right order of I is defined as $\mathcal{O}_R(I) = \{\sigma \in \mathcal{B}_{p,\infty} : I\sigma \subset I\}$. If $I \subset \mathcal{O}_L(I)$ (resp. $I \subset \mathcal{O}_R(I)$), the ideal I is called an integral ideal. An integral ideal I is a left- $\mathcal{O}_L(I)$ ideal and a right- $\mathcal{O}_R(I)$ ideal.

Definition 13. When $\mathcal{O}_L(I)$ is maximal, then I is said to be a connecting ideal between $\mathcal{O}_L(I)$ and $\mathcal{O}_R(I)$; similarly for $\mathcal{O}_R(I)$. If $\mathcal{O}_1, \mathcal{O}_2 \subset \mathcal{B}_{p,\infty}$ are two maximal orders, we denote the set of connecting ideals by $\mathcal{I}(\mathcal{O}_1, \mathcal{O}_2)$.

Definition 14. [64, Theorem 16.1.3] Let $I \subset \mathcal{B}_{p,\infty}$ be an ideal. The reduced norm of I is $\mathcal{N}(I) = \gcd(\{\text{nrd}(\gamma) : \gamma \in I\})$. Furthermore, we have $\mathcal{N}(I)^2 = [\mathcal{O}_L(I) : I] = [\mathcal{O}_R(I) : I]$.

1.3 Elliptic curves

An *elliptic curve* is an abelian variety of dimension 1. An *isogeny* is a non-trivial morphism between two elliptic curves. If there is an isogeny $E \rightarrow E'$ then we say that E and E' are *isogenous*, denoted by $E \sim E'$. An *endomorphism* of elliptic curves is either an isogeny from an elliptic curve to itself or the zero map. The set of all endomorphisms of an elliptic curve E forms the *endomorphism ring* $\text{End}(E)$. For any integer n , we denote by $[n]$ the *multiplication by- n* map over E , and its kernel, denoted by $E[n]$, is called the *n -torsion subgroup* of E . An isogeny $\varphi : E \rightarrow E'$ induces a map of function fields $\varphi^* : K(E') \rightarrow K(E)$ and its *degree* is the degree of the field extension $\deg(\varphi) = [K(E) : \varphi^* K(E')]$. If this field extension is separable, or equivalently if the characteristic of the field over which E and E' are defined is coprime to the degree, then $\deg(\varphi) = \#\ker(\varphi)$. Every isogeny $\varphi : E \rightarrow E'$ has a *dual isogeny* $\widehat{\varphi}$ satisfying $\varphi \circ \widehat{\varphi} = \widehat{\varphi} \circ \varphi = [\deg(\varphi)]$. An elliptic curve E defined over a field K of characteristic p is said to be *supersingular* if $E[p] \cong \{0_E\}$. The endomorphism ring of a supersingular elliptic curve defined over \mathbb{F}_{p^2} is a maximal order in $\mathcal{B}_{p,\infty}$, where $\mathcal{B}_{p,\infty}$ is the quaternion algebra described in Lemma 1. The following definition gives examples of such curves:

Definition 15. Let $p > 2$ be a prime and s be as in Lemma 1. Let c be an integer such that $s|c^2p + 1$. We define E_0/\mathbb{F}_p to be the supersingular elliptic curve computed by [17, Proposition 3] such that

$$\text{End}(E_0) \cong \begin{cases} \left\langle 1, i, \frac{i+ij}{2}, \frac{1+j}{2} \right\rangle & \text{if } p \equiv 3 \pmod{4} \\ \left\langle 1, i, \frac{2-i+ij}{4}, \frac{-1+i+j}{2} \right\rangle & \text{if } p \equiv 5 \pmod{8} \\ \left\langle \frac{1+i}{2}, \frac{j+ij}{2}, \frac{i+cij}{s}, ij \right\rangle & \text{if } p \equiv 1 \pmod{8}. \end{cases}$$

1.4 Abelian varieties

An *isogeny* of abelian varieties is a surjective morphism with finite kernel. If there is an isogeny φ between abelian varieties A and A' then we say that they are *isogenous*, denoted by $A \sim A'$. An isogeny $A \rightarrow A'$ induces a map of function fields $\varphi^* : K(A') \rightarrow K(A)$ and its *degree* is the degree of the field extension $\deg(\varphi) = [K(A) : \varphi^* K(A')]$. If this field extension is separable, then $\deg(\varphi) = \#\ker(\varphi)$. An abelian variety of dimension two is an *abelian surface*.

A *prime divisor* on A is a closed subvariety of dimension $n - 1$, where $n = \dim(A)$. The divisor group $\text{Div}(A)$ is the set of all divisors on A ; it is the free abelian group generated by the prime divisors. A *divisor* $D \in \text{Div}(A)$ (Weil divisor) is a formal linear combination of prime divisors. Any divisor D is called a *principal divisor* if it is equal to the divisor of a (nonzero) rational function on A . Two divisors D_1 and D_2 are linearly equivalent if $D_1 - D_2$ is a principal divisor. For $D \in \text{Div}(A)$, the map $\phi_D : A(K) \rightarrow \text{Pic}(A)$ defined by $\phi_D(a) = [\mathcal{L}(D_{-a} - D)]$ is a morphism. A divisor D is ample if and only if the morphism ϕ_D has finite kernel by [48, p.60].

A *polarization* λ on an abelian variety A is an isogeny $\lambda : A \rightarrow \hat{A}$ such that $\lambda = \varphi_{\mathcal{L}}$ (see [46, Theorem 6.7] for the definition of $\varphi_{\mathcal{L}}$) for some ample invertible

sheaf \mathcal{L} on A . The *degree of a polarization* is its degree as an isogeny. If the polarization has degree 1, it is called a *principal polarization*. An abelian variety A with a principal polarization λ is called a *principally polarized abelian variety*, denoted by (A, λ) .

The *Picard group* $\text{Pic}(A)$ of A is defined as the group of isomorphism classes of invertible sheaves on A with operation \otimes , see [22, p. 143]. Let $\text{Pic}^0(A)$ be the set of isomorphism classes of invertible sheaves \mathcal{L} where $t_Q^*\mathcal{L} \simeq \mathcal{L}$ for any $Q \in A(K)$. The $\text{Pic}^0(A)$ is naturally isomorphic to the set of K -rational points of an abelian variety \widehat{A} , called the *dual abelian variety* of A by [48, p.74]. An *isogeny of polarized abelian varieties* $(A, \lambda) \rightarrow (A', \lambda')$ is an isogeny morphism $\alpha : A \rightarrow A'$ such that $\alpha^*\lambda' = \lambda$ where $\alpha^*\lambda' := \widehat{\alpha}\lambda'\alpha : A \rightarrow \widehat{A}$.

Jacobians of curves are important examples of principally polarized abelian varieties. If C/K is a non-singular algebraic curve and g_C is its genus (see [22, p. 181]), its Jacobian $\mathcal{J}(C)$ is a principally polarized abelian variety of dimension g_C such that $\mathcal{J}(C)(K) \simeq \text{Pic}^0(C)$ [47, Theorem 1.1].

Definition 16. Let C/K be a nonsingular algebraic curve of genus 2, let $P \in C(K)$ be a point, and let $f_P : C(K) \rightarrow \mathcal{J}(C)$ be the map $f_P(Q) = \mathcal{L}(Q) \otimes \mathcal{L}(P)^{-1}$ (see [22, Corollary II.6.14] for the definition of $\mathcal{L}(D)$). The map f_P gives an isomorphism from C onto $f_P(C)$ by [47, Proposition 2.3], and $f_P(C)$ is nonsingular. A divisor $\theta_C := f_P(C)$ on $\mathcal{J}(C)$ is called a theta divisor.

As a consequence, every irreducible principally polarized abelian surface is isomorphic to $(\mathcal{J}(C), \theta_C)$ for some hyperelliptic curve C of genus 2 [67,62].

Definition 17. The Neron-Severi group of an abelian variety A is defined as the quotient group

$$\text{NS}(A) = \text{Pic}(A)/\text{Pic}^0(A).$$

It is a free \mathbb{Z} -module of finite rank.

We will give another, equivalent, definition of the Neron-Severi group of an abelian surface in Definition 19.

1.5 Supersingular and superspecial abelian varieties

Let \mathbb{F}_q be a field of characteristic $p > 0$ and $\overline{\mathbb{F}}_q$ be its algebraic closure. An abelian variety over a field K is said to be *supersingular* if it is isogenous to a product of supersingular elliptic curves over \overline{K} [52] and it is said to be *superspecial* if it is $\overline{\mathbb{F}}_q$ -isomorphic to a product of supersingular elliptic curves. A curve C is called *supersingular* (respectively, *superspecial*) if its Jacobian $A = \mathcal{J}(C)$ is supersingular (respectively, *superspecial*). If A is superspecial, then it is supersingular, but the converse is not true for $\dim(A) \geq 2$. Deligne, Ogus and Shioda proved that all g -dimensional superspecial abelian varieties over \mathbb{F}_q are $\overline{\mathbb{F}}_q$ -isomorphic as unpolarized abelian varieties, see [51, Theorem 6],[57, Theorem 3.5], and [44, Section 1.6]. Let $\mathcal{B}_{p,\infty}$ be as in Definition 1 and let \mathcal{O} be any maximal order of $\mathcal{B}_{p,\infty}$. By [61, Corollary 2.9], we can identify principal polarizations with the

quaternion Hermitian matrices $\mathfrak{G}^* = \mathfrak{G} \in M_n(\mathcal{O})$ with $\det \mathfrak{G} = 1$. Therefore, for any superspecial abelian surface, the set of polarizations is given by

$$\theta \in \left\{ \begin{pmatrix} u & \alpha \\ \bar{\alpha} & v \end{pmatrix} : u, v \in \mathbb{Z}_{>0}, \alpha \in \mathcal{O}, uv - \alpha\bar{\alpha} = 1 \right\}.$$

1.6 Refined Humbert invariants

In this section, we introduce *refined Humbert invariants*, as defined by Kani [26,29]. A refined Humbert invariant $q_{(A,\theta)}$ of a principally polarized abelian surface (A, θ) , see Definition 23, is the main ingredient of this paper. These are isomorphism invariants of the polarized Néron-Severi group of a principally polarized abelian surface (A, θ) , see Definition 21, and they can be used to translate geometric problems into arithmetic problems. It encodes many special properties of (A, θ) , and this makes them worth studying for various reasons. The various usage of such invariants can be found in [28,29]. This section mainly follows from Kani [30,31].

Definition 18. [22, p.357] Let A be an abelian surface over a field K . Let $\text{Div}(A)$ be the set of divisors on A defined over K . Let $D_1, D_2 \in \text{Div}(A)$. We say that D_1 is numerically equivalent to D_2 , denoted by $D_1 \equiv D_2$, if for all $D \in \text{Div}(A)$ we have that

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

where (\cdot) denotes the intersection number.

Definition 19. [42, Corollary of Theorem V.1] Let A/K be an abelian surface. We define the Néron-Severi group $\text{NS}(A)$ of A to be

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

where \equiv is the equivalence defined in Definition 18.

This definition agrees with the one defined in [42, p.101], so the $\text{Pic}^0(A)$ -equivalence and the numerical equivalence coincide [42, Corollary of Theorem V.1].

Theorem 1 (Nakai-Moishezon Criterion). [22, Theorem V.1.10] A divisor D on a surface A is ample if and only if $D^2 = (D \cdot D) > 0$ and, for all irreducible curves C in A , we have that $(D \cdot C) > 0$.

If D is an ample divisor on A , then there is an effective divisor $D' \sim D$ with $D' \geq 0$. When A is an abelian surface, the set $\text{cl}(D)$ can be identified with the numerical equivalence class of D for a divisor $D \in \text{Div}(A)$.

Remark 1. We refer the reader to Chapter 4.1 of [55] and Chapter V.1 of [22] for technical details on the intersection theory of abelian surfaces. In the case of $A = E_1 \times E_2$ given by Theorem 4 below, there is a simple formula for the intersection formula which is sufficient for our computations.

Definition 20. Let A/K be an abelian surface. We define

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

to be the set of principal polarizations of A .

Definition 21. Let A/K be an abelian surface and let $\theta \in \mathcal{P}(A)$ be a principal polarization of A . We define the polarized Néron-Severi group of (A, θ) to be

$$\text{NS}(A, \theta) := \text{NS}(A)/\mathbb{Z}\theta.$$

Definition 22. Suppose that (A, θ) is a principally polarized abelian surface. Then the Humbert invariant of a divisor $D \in \text{Div}(A)$ is given by

$$\text{HI}(D) := (D \cdot \theta)^2 - 2(D \cdot D).$$

Kani argues in [26, Section 3] that HI induces a well-defined map on $\text{NS}(A, \theta)$ via $\text{HI}(\text{cl}(D)) = \text{HI}(D)$ and furthermore that this defines a positive-definite quadratic form on $\text{Div}(A)$ and $\text{NS}(A, \theta)$.⁵

Definition 23. Let (A, θ) be a principally polarized abelian surface. A refined Humbert invariant $q_{(A, \theta)}$ of (A, θ) is a positive-definite quadratic form on $\text{NS}(A, \theta)$ satisfying, for all $[D] \in \text{NS}(A, \theta)$, the rule

$$q_{(A, \theta)}([D]) = \text{HI}(D) = (D \cdot \theta)^2 - 2(D \cdot D).$$

A refined Humbert invariant should be thought of as an isomorphism invariant of the polarized Néron-Severi group. This already gives us an insight into why we can expect a connection with the isogeny problem. Let E_1 and E_2 be elliptic curves over a field K . We recall below in Theorem 4 the classical isomorphism

$$\text{NS}(E_1 \times E_2) \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \text{Hom}(E_1, E_2),$$

so in this particular case of interest, the refined Humbert invariant of $E_1 \times E_2$ equipped with the canonical product polarization is closely related to $\text{Hom}(E_1, E_2)$.

Remark 2. Recently, a new equivalent isogeny problem HOMMODULE appeared in [45]. It reformulates another problem to find the set of all isogenies between E_1 to E_2 rather than finding one isogeny. The [HOMMODULE] problem is: given two supersingular elliptic curves E_1 and E_2 over \mathbb{F}_{p^2} , find four isogenies generating $\text{Hom}(E_1, E_2)$ as a \mathbb{Z} -module. It is obvious that ISOGENYPATH, see Problem 1, reduces to HOMMODULE. The inverse security reduction was proved in [45, Section 4]. We would like to emphasize that HOMMODULE is naturally related to Problem 2 and Problem 4.

⁵ We usually use $\text{cl}(D)$ for divisors in $\text{NS}(A)$ and $[D]$ in $\text{NS}(A, \theta)$. We sometimes drop the class representation when it is clear from the context.

Remark 3. We have $\text{NS}(A) \cong \mathbb{Z}^\rho$ where $\rho = \rho(A)$ is the Picard number of A by [48, p.60], and henceforth $\text{NS}(A, \theta) \cong \mathbb{Z}^{\rho-1}$. If the K -rational endomorphism ring $\text{End}_K(A)$ is rank 2, and Picard number of A is $\rho = 4$, then $q_{(A, \theta)}$ is a *ternary* quadratic form. If the K -rational endomorphism ring $\text{End}_K(A)$ is rank 4, and its Picard number of A is $\rho = 6$, then $q_{(A, \theta)}$ is a *quintic* quadratic form [26, p.200].

Lemma 2 on the special case of a product surface is central to our two main theorems relating the problem of computing refined Humbert invariants and the computational isogeny problem.

Definition 24. [58, Corollary III.6.3] *Let E_1 and E_2 be isogenous elliptic curves $E_1 \sim E_2$ via $\varphi : E_1 \rightarrow E_2$. For $i = 1, 2$ we define*

$$r = \text{rank}(\text{Hom}(E_1, E_2)) = \dim_{\mathbb{Q}}(\text{End}^0(E_i)).$$

We define the degree map \deg_{E_1, E_2} to be a positive definite quadratic form on $\text{Hom}(E_1, E_2)$ in r variables.

The degree map \deg_{E_1, E_2} is defined only up to \mathbb{Z} -equivalence. Moreover, $\text{Hom}(E_1, E_2)$ is isomorphic to an $\text{End}(E_1)$ -ideal via φ (see [64, Lemma 42.2.7]).

Lemma 2. *Let E_1 and E_2 be isogenous elliptic curves. Write $\theta_{E_1} \times \theta_{E_2}$ for the canonical product polarization on $E_1 \times E_2$. Then the refined Humbert invariant $q_{(E_1 \times E_2, \theta_{E_1} \times \theta_{E_2})}$ is \mathbb{Z} -equivalent to*

$$x^2 + 4\deg_{E_1, E_2},$$

where $\deg_{E_1, E_2} \in \mathbb{Z}[y_1, \dots, y_n]$ is the degree map of Definition 24.⁶

Proof. See [30, Lemma 21].

The majority of the literature on computing refined Humbert invariants suitable for cryptographic applications to date focuses on the case that A is a complex multiplication (CM) product surface $E_1 \times E_2$. All known methods to compute refined Humbert invariants in this case make use of information about $\text{Hom}(E_1, E_2)$ (in some cases this information can be just the degree of an isogeny from E_1 to E_2). In Section 3.3, we give an overview of the best known methods to compute refined Humbert invariants in different cases of interest.

Relationship with endomorphism rings

In Proposition 1 below, we see that we can also characterize the refined Humbert invariant directly in terms of the symmetric endomorphism ring. This can be thought of as an equivalent definition of the refined Humbert invariant; Kani extends the definition of refined Humbert invariants to any abelian variety as follows.

⁶ Here $n = \rho - 1 = r + 1$ where ρ is the Picard number of A and r is the rank of $\text{Hom}(E_1, E_2)$.

Definition 25. Let A be an abelian surface over a field K . If A has a principal polarization $\theta : A \rightarrow \hat{A}$ defined over K , then we define the symmetric endomorphism ring $\text{End}_\theta(A)$ to be the additive subgroup of the ring $\text{End}_K(A)$ of K -endomorphisms of A given by

$$\text{End}_\theta(A) = \{\alpha \in \text{End}_K(A) : \hat{\alpha} \circ \theta = \theta \circ \alpha\} = \{\alpha \in \text{End}_K(A) : \alpha = \alpha'\}, \quad (3)$$

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

Proposition 1. Let (A, θ) be a principally polarized abelian surface over a field K and let $q_{(A, \theta)}$ be a refined Humbert invariant of (A, θ) . Then for every $\alpha \in \text{End}_\theta(A)$, we have that

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

where tr is the usual (rational) trace of an endomorphism (c.f. [48, p.182]).⁷

Proof. See [31, Proposition 14, Remark 16].

Three different types of integral quadratic forms: q_A , $q_{(A, \theta)}$, and \deg_{E_1, E_2} are being used in this paper. In the table below we give a dictionary to make the notation clearer for the reader. In this table $A = E_1 \times E_2$ denotes a product surface and θ a principal polarization (not necessarily a product polarization). We always work in the case that E_1 and E_2 are isogenous, so that in particular they have the same endomorphism algebra. We consider two cases: either the endomorphism rings of E_1 and E_2 are quaternion orders or they are quadratic orders in an imaginary quadratic number field. The second case is either the case in which E_1 and E_2 are ordinary or the case in which E_1 and E_2 are defined over \mathbb{F}_p and we consider only the endomorphisms defined over \mathbb{F}_p . We refer to $q_{(A, \theta)}$ as a *ternary refined Humbert invariant* in the first case and a *quintic refined Humbert invariant* in the second case, respectively.

Table 1. Dictionary of the notation

	$\text{NS}(A)$	$\text{NS}(A, \theta)$	$\text{Hom}(E_1, E_2)$
Quadratic form notation	q_A	$q_{(A, \theta)}$	\deg_{E_1, E_2}
# variables	6	5	4
# variables	4	3	2

⁷ Note that $\text{tr}(\alpha)$ is the trace of the characteristic polynomial of α acting on the ℓ -adic representation $T_\ell(A) \otimes \mathbb{Q}$, and it is always integer.

Higher dimensions

Auffarth [1] introduced a form of a higher degree to generalize the refined Humbert invariant to a principally polarized abelian varieties. Also, Kani mentioned in [31] that refined Humbert invariants (Proposition 1) can be generalized to a principal polarized abelian varieties of arbitrary dimension.

2 The supersingular isogeny path and the computational refined Humbert invariant problem are equivalent

In this section, we prove that computing certain refined Humbert invariants is polynomially equivalent to computing supersingular isogeny paths both in the context of supersingular elliptic curves defined over \mathbb{F}_p and over \mathbb{F}_{p^2} . We start with the case of \mathbb{F}_{p^2} .

2.1 The supersingular isogeny path problem over \mathbb{F}_{p^2}

Following [68], we consider the supersingular isogeny path problem in the context of elliptic curves over \mathbb{F}_{p^2} to be the following:

Problem 1. [ℓ -ISOGENYPATH] Given a prime p , a prime $\ell \neq p$, and supersingular elliptic curves E and E'/\mathbb{F}_{p^2} , find a path from E to E' in the ℓ -isogeny graph of supersingular elliptic curves over \mathbb{F}_{p^2} .

We will show in Theorem 2 that this is polynomially equivalent to the following problem:

Problem 2. [RHI-QUINTIC] Given a prime p and supersingular elliptic curves E and E'/\mathbb{F}_{p^2} , compute the coefficients of a (quintic) refined Humbert invariant $q_{(E \times E', \theta_E \otimes \theta_{E'})}$ as in Definition 23.

A crucial step in this is computing a basis of a maximal quaternion order \mathcal{O} from its norm form, so we first provide an algorithm, Algorithm 1, for this step. The authors thank John Voight for suggesting this algorithm and for the base of the accompanying Magma code <https://github.com/NSinvariant/RHI/>.

Remark 4. A Magma [4] implementation for Algorithm 1 can be found at <https://github.com/NSinvariant/RHI/>. The implementation is fairly minimal as it builds on existing Magma subroutines for Steps (1) and (3). An implementation of (1) also exists in Pari/GP [60], which can also be called in SageMath [59], but to the best knowledge of the authors there is not yet an implementation of the Clifford functor in SageMath or Pari/GP.

Lemma 3. *Algorithm 1 is correct and runs in time polynomial in the size of the input.*

Algorithm 1: Given a quaternary integral quadratic form that is known to be the norm form of a maximal quaternion order in $\mathcal{B}_{p,\infty}$, compute a basis of a maximal quaternion order with this norm form

Input: A quaternary integral quadratic form $Q \in \mathbb{Z}[w, x, y, z]$ that is known to be the norm form of a maximal quaternion order \mathcal{O} in $\mathcal{B}_{p,\infty}$.

Output: A basis $\{b_0, b_1, b_2, b_3\}$ of a maximal quaternion order in $\mathcal{B}_{p,\infty}$ such that $Q = \text{nrd}(wb_0 + xb_1 + yb_2 + zb_3)$.

- 1 Compute the LLL reduction \bar{Q} of the Gram matrix of Q .
- 2 Define the matrix \mathbf{Z} to be the following 3×3 submatrix:

$$(2\bar{Q})^{-1} = \begin{pmatrix} * & * & * & * \\ * & * & & \\ * & & \mathbf{Z} & \\ * & & & \end{pmatrix}.$$

- 3 Compute a basis $\{b_0, b_1, b_2, b_3\}$ of a quaternion order \mathcal{O}' given by the image of the ternary quadratic form

$$2^4 \cdot p \cdot (x_1, x_2, x_3) \cdot \mathbf{Z} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

under the inverse of the Clifford functor (see e.g. [64, 22.1.2], which is implemented in Magma [4]).

- 4 **Return** $\{b_0, b_1, b_2, b_3\}$
-

Proof. We first justify that the first element of the LLL-reduced basis is a unit:⁸ As $1 \in \mathcal{O}$, the lattice contains an element of norm 1. Nguyen and Stehlé's algorithm [50, L³ algorithm] runs in polynomial-time and returns (the Gram matrix of) a basis for which the norm of the first vector is arbitrarily close to the Hermite constant $(4/3)^{\frac{4-1}{4}} < 2$.

As norms are integral, in this case the first entry of the LLL-reduced basis must be a unit, call this e_0 . Then \bar{Q} is the Gram matrix⁹

$$\bar{Q} = \left(\frac{1}{2} \text{trd}(e_i \bar{e}_j) \right)_{i,j=0,\dots,3}$$

for the quadratic norm form $\text{nrd}(we_0 + xe_1 + ye_2 + ze_3)$ coming from some basis $\{e_0, e_1, e_2, e_3\}$ of \mathcal{O} .

Voight [65] gave an explicit bijection between quaternion orders and ternary integral quadratic forms using Clifford's functor; we follow Voight's textbook [64, 22.1.2] for the below. The ternary integral quadratic form related to a given \mathcal{O} comes from the trace-zero part of the trace dual $(\mathcal{O}^\#)^0$. We now show how to compute this ternary integral quadratic form from \bar{Q} . Define an isomorphism of \mathbb{Z} -modules

$$\begin{aligned} \vartheta : \mathcal{O} &\rightarrow \mathbb{Z}^4 \\ \sum x_i e_i &\mapsto (x_0, x_1, x_2, x_3) \end{aligned}$$

and a pairing

$$\begin{aligned} \mathcal{T} : \mathbb{Z}^4 \times \mathbb{Z}^4 &\rightarrow \mathbb{Z} \\ \mathbf{x}, \mathbf{y} &\mapsto \mathbf{x}^t \cdot 2\bar{Q} \cdot \mathbf{y}. \end{aligned}$$

Let $\{e_0^\#, e_1^\#, e_2^\#, e_3^\#\}$ be the dual basis in the sense of [64, 15.6.3], that is, this is defined by

$$\text{trd}(e_i^\# e_j) = \begin{cases} 1 & \text{when } i = j \\ 0 & \text{when } i \neq j. \end{cases}$$

As multiplying the basis choice by a unit does not change the norm form Definition 10, we can let $e_0 = 1$. Therefore $\{e_1^\#, e_2^\#, e_3^\#\}$ gives us a basis of $(\mathcal{O}^\#)^0$ in the sense of [64, 15.6].

Then we claim that

$$\vartheta(e_i^\#) = (2\bar{Q})^{-1} \vartheta(e_i),$$

as if so

$$\begin{aligned} \mathcal{T}(\vartheta(e_i^\#), \vartheta(e_j)) &= \vartheta(e_i^\#)^t (2\bar{Q}) \vartheta(e_j) \\ &= \vartheta(e_i)^t (2\bar{Q})^{-1} (2\bar{Q}) \vartheta(e_j) \\ &= \vartheta(e_i)^t \vartheta(e_j) \\ &= \begin{cases} 1 & \text{when } i = j \\ 0 & \text{when } i \neq j; \end{cases} \end{aligned}$$

⁸ LLL for Gram matrices is implemented in PARI/GP [60] and integrated into Sage-Math [59]; the algorithm is based on Nguyen and Stehlé [50, Fig. 4-6].

⁹ Note that $\text{nrd}(e_i \bar{e}_i) = \frac{1}{2} \text{trd}(e_i \bar{e}_i)$.

Given that the reduced discriminant of $2\bar{Q}$ is $2^4 \cdot p$, the ternary integral quadratic form itself is as defined in [64, Equation 22.1.3], the norm form of $(\mathcal{O}^\#)^0$ scaled by $2^4 \cdot p$, which is given by

$$2^4 \cdot p \cdot (x_1, x_2, x_3) \cdot \mathbf{Z} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

The basis elements e_1 , e_2 , and e_3 can then be computed via the Clifford functor using [64, 22.1.2], which is implemented in Magma [4], and which is also polynomial-time. \square

Theorem 2. *Under GRH, Problems 1 and 2 are equivalent up to algorithms that:*

- are expected polynomial-time in $\log(p)$,
- are expected polynomial-time in the size of the output of [68, Algorithm 3],
- are polynomial-time in the size of the inputs of problems 1 and 2,

requiring two calls to the oracle solving the respective problem.

We first prove two lemmas.

Lemma 4. *Under GRH, given an oracle O_1 for Problem 1 which outputs paths that can be represented in a number of bits polynomial in $\log(p)$, Algorithm 2 is correct and runs in expected polynomial time in $\log(p)$ and the length of the basis for the quaternion order $\mathcal{O} \cong \text{End}(E_1)$ output by [68, Algorithm 3], plus two calls to the oracle O_1 .*

Proof. By [68, Theorem 7.2], under GRH, step 1 is correct and runs in expected polynomial time in $\log(p)$ and the size of the output of the oracle O_1 , plus one call to O_1 . By [68, Theorem 8.1], under GRH, step 2 is correct and runs in expected polynomial time in $\log(p)$ and the length of the b_i . Step 3 is a simple multiplication and can be trivially computed in time polynomial in the length of the b_i and $\log(p)$. For step 6.1, as the endomorphisms θ_i output by [68, Algorithm 6] are compositions of $(\log p)^c$ -powersmooth isogenies and small endomorphisms, they can be evaluated on points in $E_1[D]$ in time polynomial in $\log(p)$. Checking which i, j gives a basis is a pairing calculation, which is polynomial in $\log p$ and $\log D$. For step 7.2, we use the BiDLP function exactly as in [43], which has complexity $O(d\sqrt{l})$, where $D = \ell^d$. Step 7.3, using step 2, is a simple multiplication and is polynomial in a and b , which are polynomial in $\log(p)$ and in the length of the b_i . Step 8 uses elementary row operations and is polynomial in the length of the input elements. The degree D has polynomial length by assumption on the oracle, the output a and b of step 7.2 are polynomial in $\log(p)$, so this step is polynomial in $\log(p)$ and the length of the b_i . Step 9 is a simple multiplication so is polynomial in the length of the β_i , which similarly to step 8 is polynomial in $\log(p)$ and the length of the b_i . The output is then correct by Lemma 2. \square

Algorithm 2: Solve Problem 2 given an oracle that solves Problem 1

Input: A prime p , supersingular elliptic curves E_1 and E_2/\mathbb{F}_{p^2} , an oracle O_1 for Problem 1.

Output: A quintic refined Humbert invariant $q_{(E_1 \times E_2, \theta_{E_1 \times E_2})}$ as in Definition 23.

- 1 Use [68, Algorithm 3] (which makes a call to O_1) to compute a basis $\{b_1, b_2, b_3, b_4\}$ of a maximal order $\mathcal{O}_1 \in \mathcal{B}_{p,\infty}$ that is isomorphic to $\text{End}(E_1)$.
- 2 Use [68, Algorithm 6] to compute endomorphisms $\theta_1, \theta_2, \theta_3, \theta_4$ generating $\text{End}(E_1)$. Define the isomorphism κ by

3

$$\begin{aligned}\kappa : \text{End}(E_1) &\rightarrow \mathcal{O}_1 \\ \theta_i &\mapsto b_i.\end{aligned}$$

- 4 Compute $N_i = \text{nrd}(b_i)$ and choose a small ℓ such that, for all i , we have that $\gcd(\ell, N_i) = 1$.
- 5 Compute an ℓ -isogeny path $\varphi : E_1 \rightarrow E_2$ by making a call to oracle O_1 . Let $D = \deg(\varphi)$ and choose $P \in E_1[D]$ such that $\langle P \rangle = \ker(\varphi)$.
- 6 Compute the ideal corresponding to φ following steps 3-6 of KernelToIdeal [43, Algorithm 20]:
 - 7.1 Find i, j such that $\theta_i(P), \theta_j(P)$ is a basis of $E_1[D]$.
 - 7.2 Choose $k \neq i, j$ and compute a, b such that $\theta_k(P) = a\theta_i(P) + b\theta_j(P)$.
 - 7.3 Compute $\alpha = \kappa(\theta_k - a\theta_i - b\theta_j)$.
 - 7.4 Define $I_\varphi := \mathcal{O}_1\langle \alpha, D \rangle$.
- 8 Using linear algebra, reduce the generating set $\{\alpha b_i, D b_i\}_{i=1\dots 4}$ to an integral basis $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ for I_φ .
- 9 Compute \deg_{E_1, E_2} as

$$\deg_{E_1, E_2} = \text{nrd}(w\beta_1 + x\beta_2 + y\beta_3 + z\beta_4).$$

-
- 10 **Return** $u^2 + 4 \deg_{E_1, E_2}$
-

Algorithm 3: Solve Problem 1 given an oracle that solves Problem 2

Input: A prime p , a prime $\ell \neq p$, supersingular elliptic curves E_1 and E_2/\mathbb{F}_{p^2} , an oracle O_2 for Problem 2.

Output: A path from E_1 to E_2 in the ℓ -isogeny graph.

- 1 Invoke oracle O_2 to compute a refined Humbert invariant $q = q_{(E_1 \times E_1, \theta_{E_1} \times \theta_{E_1})}$ of $(E_1 \times E_1, \theta_{E_1} \times \theta_{E_1})$ as defined in Definition 23.
- 2 Compute the Gram matrix G of q and reduce this with LLL to get a Gram matrix

$$G' = \begin{pmatrix} 1 & \mathbf{v} \\ \mathbf{v} & * \end{pmatrix} = (\langle \mathbf{b}'_i, \mathbf{b}'_j \rangle)_{i,j=0,\dots,4}$$

of a basis $\{\mathbf{b}'_0, \dots, \mathbf{b}'_4\}$.

- 3 **If** $v = 0$ **then**
- 4 | continue to Step 15
- 5
- 6 **else**
- 7 | **For** $i = 1, \dots, 4$ **do**
- 8 | | $n \leftarrow G'_{0i}$
- 9 | | **For** $j = 1, \dots, 4$ **do**
- 10 | | | If $i \neq j$ then $G'_{ji} \leftarrow G'_{ji} - nG'_{j0}$
- 11 | | | $G'_{ij} \leftarrow G'_{ji} - nG'_{j0}$
- 12 | | | $G'_{ii} \leftarrow G'_{ii} - nG'_{i0}$
- 13 | | | $G'_{i0} \leftarrow 0$
- 14 | | | $G'_{0i} \leftarrow 0$

- 15 We now have

$$G' = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & M \end{pmatrix};$$

define

$$f_1 = \frac{1}{4} \begin{pmatrix} w & x & y & z \end{pmatrix} M \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} \in \mathbb{Z}[w, x, y, z].$$

Using Algorithm 1, compute a basis of a maximal order \mathcal{O}_1 in $\mathcal{B}_{p,\infty}$ with norm form $f_1(w, x, y, z)$; then $\text{End}(E_1) \cong \mathcal{O}_1$.

- 16 Repeat for E_2 .
 - 17 Using [68, Algorithm 5], compute a path from E_1 to E_2 in the ℓ -isogeny graph.
-

Lemma 5. *Under GRH, given an oracle O_2 for Problem 2 (when $E \cong E'$) which outputs a refined Humbert invariant q , Algorithm 3 is correct and runs in time that is probabilistic polynomial in $\log(p)$ and in the size of the coefficients of q , plus two calls to the oracle O_2 .*

Proof. By Lemma 2 we know that there exists $f_1 \in \mathbb{Z}[w, x, y, z]$ such that $q \sim x^2 + 4f_1$. Let q be the q of Step 1 and $q' = x^2 + 4f_1$; the matrix G' will be the Gram matrix of q' . For Step 2, we need only argue that the integral lattice of G contains a vector of norm 1 and that LLL indeed finds the shortest vector in polynomial time.¹⁰ As q is known to be equivalent to q' , the lattice contains an element of norm 1. Nguyen and Stehlé's L^3 algorithm [50] runs in polynomial-time and returns (the Gram matrix of) a basis $\{\mathbf{b}'_0, \dots, \mathbf{b}'_4\}$ for which the norm of \mathbf{b}'_0 is arbitrarily close to the Hermite constant $(4/3)^{5/4} < 2$, so \mathbf{b}'_0 is a unit.

LLL only returns a basis that is *almost* orthogonal, so we cannot guarantee that $\mathbf{v} = 0$. However, as we don't care about the norms of \mathbf{b}'_i for $i = 0$, this is easy to adjust using steps 7-14. These steps correspond to systematically replacing, for $i > 0$, each \mathbf{b}'_i with $(\mathbf{b}'_i)_{\text{new}} = \mathbf{b}'_i - \langle \mathbf{b}'_i, \mathbf{b}'_0 \rangle \mathbf{b}'_0$ as this then ensures that

$$\begin{aligned} \langle (\mathbf{b}'_i)_{\text{new}}, \mathbf{b}'_0 \rangle &= \langle \mathbf{b}'_i - \langle \mathbf{b}'_i, \mathbf{b}'_0 \rangle \mathbf{b}'_0, \mathbf{b}'_0 \rangle \\ &= \langle \mathbf{b}'_i, \mathbf{b}'_0 \rangle (1 - \langle \mathbf{b}'_0, \mathbf{b}'_0 \rangle) \\ &= 0, \end{aligned}$$

as required. This is clearly polynomial-time in the size of the inner products of the basis elements.

Now our matrix G' is in the right form to be the Gram matrix of q' above, and as the degree map is also only defined up to equivalence, we can take f_1 to be the one defined in Step 15. As, again by Lemma 2, our f_1 is the norm form of E_1 (recall that the factor of 4 comes from Lemma 2), we can use Algorithm 1 as stated which is polynomial time in the size of the input.

Finally, for Step 17, a path in the ℓ -isogeny graph, for ℓ polynomial in $\log(p)$, can be computed (under GRH) in probabilistic polynomial time using [68]. \square

Proof (Proof of Theorem 2). This follows immediately from Lemmas 4 and 5. \square

2.2 The CSIDH isogeny path problem

In this section, we study the relationship between breaking CSIDH and computing ternary refined Humbert invariants. This section concerns ternary refined Humbert invariants rather than quintic as we are studying morphisms and elliptic curves over \mathbb{F}_p . For this section, we make use of the recent work of Kani [32, p.32] and [25, Theorem 2] applied to the results of [38] for extending the theory of refined Humbert invariants to arbitrary base fields.

In order to simplify our reductions, we make an assumption in our problem statements that the CSIDH isogeny secret key is the *shortest* isogeny between

¹⁰ LLL for Gram matrices is implemented in PARI/GP [60] and integrated into Sage-Math [59]; the algorithm is based on Nguyen and Stehlé [50, Fig. 4-6].

the two elliptic curves and that the instantiation of the class-group action uses only positive exponents. We leave the removal of this assumption for future work. Also, while the CSIDH setup is a special case of than the general supersingular isogeny path problem over \mathbb{F}_p , it is the most cryptographically relevant case, so we leave a general equivalence (if it exists) to future work.

Definition 26. Let p be a prime, let E_0/\mathbb{F}_p be the supersingular elliptic curve of Definition 15, and let \mathfrak{R} be its \mathbb{F}_p -rational endomorphism ring. Let $\ell_1 < \dots < \ell_n$ be primes dividing $p+1$ with $\ell_n \approx \log(p)$ that are split in \mathfrak{R} ; let $\mathfrak{l}_1, \dots, \mathfrak{l}_n$ denote ideals in \mathfrak{R} of norm ℓ_1, \dots, ℓ_n respectively. For fixed small integers k_1, \dots, k_n , define the CSIDH subset for $(\mathfrak{R}, \mathfrak{l}_1, \dots, \mathfrak{l}_n, k_1, \dots, k_n)$ to be the set

$$\left\{ \left[\prod \mathfrak{l}_i^{e_i} \right] * E_0 : 0 \leq e_i \leq k_i \right\},$$

where $*$ denotes the standard class-group action. For $E = [\prod \mathfrak{l}_i^{e_i}] * E_0$ in this CSIDH subset, we say that $I = \prod \mathfrak{l}_i^{e_i}$ is a CSIDH subset ideal representative of E .

Problem 3. [CSIDH-ISOGENYPATH] Let p be a prime and let E_0/\mathbb{F}_p be as in Definition 15, and denote by \mathfrak{R} its \mathbb{F}_p -rational endomorphism ring. Let $\ell_1 < \dots < \ell_n$ be primes dividing $p+1$ with $\ell_n \approx \log(p)$ that are split in \mathfrak{R} ; let $\mathfrak{l}_1, \dots, \mathfrak{l}_n$ denote ideals in \mathfrak{R} of norm ℓ_1, \dots, ℓ_n respectively. Given supersingular elliptic curves E and E'/\mathbb{F}_p in the CSIDH subset for $(\mathfrak{R}, \mathfrak{l}_1, \dots, \mathfrak{l}_n, k_1, \dots, k_n)$ such that the shortest isogeny $E_0 \rightarrow E$ (resp. $E_0 \rightarrow E'$) corresponds to a CSIDH subset ideal representative of E (resp. E'), compute an isogeny from E to E' .

Remark 5. For the right choices of p, ℓ_i , and k_i , Problem 3 reduces to the more intuitive ‘Given supersingular elliptic curves E and E'/\mathbb{F}_p with the same \mathbb{F}_p -rational endomorphism ring, compute an isogeny from $E \rightarrow E'$ ’. However, in a typical cryptographic scenario, we will have only heuristic guarantees that this is the case: making sure that the choices made are the ‘right’ ones involves, among other things, computing the structure of the class group, which is a subexponential computation on a classical computer.

Problem 4. [RHI-TERNARY] Let p be a prime and let E_0/\mathbb{F}_p be as in Definition 15, and denote by \mathfrak{R} its \mathbb{F}_p -rational endomorphism ring. Let $\ell_1 < \dots < \ell_n$ be primes dividing $p+1$ with $\ell_n \approx \log(p)$ that are split in \mathfrak{R} ; let $\mathfrak{l}_1, \dots, \mathfrak{l}_n$ denote ideals in \mathfrak{R} of norm ℓ_1, \dots, ℓ_n respectively. Given supersingular elliptic curves E and E'/\mathbb{F}_p in the CSIDH subset for $(\mathfrak{R}, \mathfrak{l}_1, \dots, \mathfrak{l}_n, k_1, \dots, k_n)$ such that the shortest isogeny $E_0 \rightarrow E$ (resp. $E_0 \rightarrow E'$) corresponds to a CSIDH subset ideal representative of E (resp. E'), compute the coefficients of a (ternary) refined Humbert invariant $q_{(E \times E', \theta_E \times \theta_{E'})}$ of Definition 23.

Theorem 3. Under GRH, Problems 3 and 4 are equivalent up to algorithms that:

- are expected polynomial-time in $\log(p)$,
- are expected polynomial-time in the size of the output of [68, Algorithm 3],
- are expected polynomial-time in the size of the output of an oracle solving Problem 4,

requiring two calls to the oracle solving the respective problems.

We first prove two lemmas.

Algorithm 4: Solve Problem 4 given an oracle that solves Problem 3

Input:

- A prime p ,
- the elliptic curve E_0/\mathbb{F}_p of Definition 15 with \mathbb{F}_p -rational endomorphism ring \mathfrak{R} ,
- primes $\ell_1 < \dots < \ell_n$ dividing $p+1$ with $\ell_n \approx \log(p)$ that are split in \mathfrak{R} ,
- prime ideals $\mathfrak{l}_1, \dots, \mathfrak{l}_n$ in \mathfrak{R} of norm ℓ_1, \dots, ℓ_n respectively,
- small integers k_1, \dots, k_n ,
- supersingular elliptic curves E and E'/\mathbb{F}_p in the CSIDH subset for $(\mathfrak{R}, \mathfrak{l}_1, \dots, \mathfrak{l}_n, k_1, \dots, k_n)$ such that the shortest isogeny $E_0 \rightarrow E$ (resp. $E_0 \rightarrow E'$) corresponds to a CSIDH subset ideal representative of E (resp. E'),
- an oracle O_3 that solves Problem 3.

Output: A ternary refined Humbert invariant of $E \times E'$ equipped with the natural product polarization.

- 1 Compute a basis $\{w_0, w_1, w_2, w_3\}$ of a maximal order $\mathcal{O} \in B_{p,\infty}$ that is isomorphic to $\text{End}(E)$ using [68, Algorithm 3] (making a call to oracle O_3); compute an equivalent basis with $w_0 = 1$ and $w_1 = \pi$ or $(\pi + 1)/2$ so that $\mathfrak{R} = \mathbb{Z}[w_1]$.
- 2 Similarly, compute a basis $\{1, w'_1, w'_2, w'_3\}$ of a maximal order $\mathcal{O}' \in B_{p,\infty}$ that is isomorphic to $\text{End}(E')$.
- 3 Follow steps 2-7 of Algorithm 2 to compute an integral basis $\{b_0, b_1, b_2, b_3\}$ of the ideal I connecting \mathcal{O} and \mathcal{O}' .
- 4 Define B to be the matrix such that

$$(b_0 \ b_1 \ b_2 \ b_3) = (1 \ w_1 \ w_2 \ w_3) B.$$

- 5 Compute the reduced row echelon form $U = B \cdot E$ of B .
- 6 Let $(\mathbf{e}_0 \ \mathbf{e}_1)$ denote the first two columns of E so that

$$(\beta_0 \ \beta_1) := (b_0 \ b_1 \ b_2 \ b_3) (\mathbf{e}_0 \ \mathbf{e}_1).$$

Then $\beta_i \in \mathbb{Z}[w_1]$; let σ generate $\text{Gal}(\mathbb{Q}(w_1)/\mathbb{Q})$.

- 7 **Return** $x^2 + 4(y\beta_0 + z\beta_1)(y\sigma(\beta_0) + z\sigma(\beta_1))$.
-

Lemma 6. *Under GRH, Algorithm 4 is correct and runs in time probabilistic polynomial in $\log(p)$ and the length of the bases for the quaternion orders $\mathcal{O} \cong \text{End}(E)$ and $\mathcal{O}' \cong \text{End}(E')$ output by [68, Algorithm 3], plus two calls to the oracle O_3 .*

Proof. For step 1 (equivalently step 2), under GRH [68, Algorithm 3] runs in probabilistic polynomial-time in $\log(p)$ and $\ell_n \approx \log(p)$.

For step 3: Algorithm 2 can be applied here but calls to O_3 instead of O_1 . We can call to O_3 also to get an isogeny to the E_0 of Definition 15 as by assumption E is in the CSIDH subset. Therefore as in the proof of Lemma 4, under GRH, step 3 is correct and runs in expected polynomial time in $\log(p)$ and the size of the w_i , plus one call to O_3 .

The output of step 3 is polynomial in the size of the w_i , the w'_i , and the degree of the shortest isogeny $E \rightarrow E'$, which itself is polynomial in $\log(p)$. Steps 4, 5, and 6 are basic linear algebra and are polynomial-time in the size of the w_i and the output of step 3, so in w_i , w'_i , and $\log(p)$.

Furthermore, by construction $\langle 1, w_1 \rangle \cong \text{End}_{\mathbb{F}_p}(E) \cong \text{End}_{\mathbb{F}_p}(E')$, so as U is upper triangular and the diagonal entries are minimized, we have that the \mathbb{Z} -module generated by the endomorphisms corresponding to β_0 and β_1 are exactly those which are \mathbb{F}_p -rational, hence define a basis of $\text{Hom}_{\mathbb{F}_p}(E, E')$.

The ternary refined Humbert invariant $q_{(E \times E', \theta_E \otimes \theta_{E'})}$, again using Lemma 2, is then given by

$$q_{(E \times E', \theta_E \otimes \theta_{E'})} = x^2 + 4(y\beta_0 + z\beta_1)(y\sigma(\beta_0) + z\sigma(\beta_1)).$$

□

Lemma 7. *Given an oracle O_4 for Problem 4 which outputs a refined Humbert invariant q , Algorithm 5 is correct and runs in the time taken for two calls to oracle O_4 plus factors polynomial in $\log(p)$ and the size of the output of the oracle calls to O_4 .*

Proof. Step 1 requires one call to oracle O_4 . By Lemma 2 we know that

$$q \sim x^2 + 4 \deg_{E_0, E},$$

where $\deg_{E_0, E}$ is the degree map of all \mathbb{F}_p -rational isogenies from E_0 to E and is therefore a binary quadratic form. This proves the existence of the \mathbb{Z} -equivalent Gram matrix G' in Step 15.

Steps 2-14 are identical to steps 2-14 of Algorithm 3 but for smaller matrices; we do not repeat the complexity analysis here.

It remains to prove that Step 16 is correct; if correct it is clearly polynomial in $\ell_n \approx \log(p)$. As G' is the Gram matrix of $x^2 + 4 \deg_{E_0, E}$ for some basis of $\text{Hom}(E_0, E)$, the top-left entry of \bar{M} is the shortest vector in the \mathbb{Z} -lattice defined by $\text{Hom}(E_0, E)$. That is, it is the reduced norm of the shortest isogeny $E_0 \rightarrow E$, which by assumption is $\ell_1^{e_1} \cdots \ell_n^{e_n}$. In turn, by assumption, this corresponds to the CSIDH subset ideal representative $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$.

□

Algorithm 5: Solve Problem 3 given an oracle that solves Problem 4

Input:

- A prime p ,
- The elliptic curve E_0/\mathbb{F}_p of Definition 15 with known full endomorphism ring and \mathbb{F}_p -rational endomorphism ring \mathfrak{R} ,
- primes $\ell_1 < \dots < \ell_n$ dividing $p+1$ with $\ell_n \approx \log(p)$ that are split in \mathfrak{R} ,
- prime ideals $\mathfrak{l}_1, \dots, \mathfrak{l}_n$ in \mathfrak{R} of norm ℓ_1, \dots, ℓ_n respectively,
- small integers k_1, \dots, k_n ,
- supersingular elliptic curves E and E'/\mathbb{F}_p in the CSIDH subset for $(\mathfrak{R}, \mathfrak{l}_1, \dots, \mathfrak{l}_n, k_1, \dots, k_n)$ such that the shortest isogeny $E_0 \rightarrow E$ (resp. $E_0 \rightarrow E'$) corresponds to a CSIDH subset ideal representative of E (resp. E'),
- an oracle O_4 that solves Problem 4.

Output: An isogeny from E to E' represented in a polynomial number of bits.

- 1 Invoke O_4 to compute a ternary refined Humbert invariant $q = q_{(E \times E_0, \theta_E \times \theta_{E_0})} \in \mathbb{Z}[x, y, z]$ of $(E \times E_0, \theta_E \times \theta_{E_0})$ as defined in Definition 23.
- 2 Compute the Gram matrix G of q and reduce this with LLL to get the Gram matrix
$$G' = \begin{pmatrix} 1 & \mathbf{v} \\ \mathbf{v}^* & * \end{pmatrix} = (\langle \mathbf{b}'_i, \mathbf{b}'_j \rangle)_{i,j=0,1,2}$$
of a basis $\{\mathbf{b}'_0, \mathbf{b}'_1, \mathbf{b}'_2\}$.
- 3 **If** $v = 0$ **then**
- 4 | continue to Step 15
- 5
- 6 **else**
- 7 | **For** $i = 1, 2$ **do**
- 8 | | $n \leftarrow G'_{0i}$
- 9 | | **For** $j = 1, 2$ **do**
- 10 | | | If $i \neq j$ then $G''_{ji} \leftarrow G'_{ji} - nG'_{j0}$
- 11 | | | $G'_{ij} \leftarrow G'_{ji} - nG'_{j0}$
- 12 | | | $G'_{ii} \leftarrow G'_{ii} - nG'_{i0}$
- 13 | | | $G'_{i0} \leftarrow 0$
- 14 | | | $G'_i \leftarrow 0$

15 We now have

$$G' = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & M \end{pmatrix}.$$

Run LLL on M , let the result be \bar{M} , and define $4N$ to be the top-left entry \bar{M}_{00} of \bar{M} .

- 16 Factor N : this will give $N = \ell_1^{e_1} \cdots \ell_n^{e_n}$. Compute the isogeny $\varphi : E_0 \rightarrow E$ corresponding to the class-group action of $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$ on E_0 .
 - 17 Repeat steps 1-16 for E' resulting in an isogeny $\varphi' : E_0 \rightarrow E'$.
 - 18 **Return** $\varphi' \circ \widehat{\varphi}$
-

Proof (*Proof of Theorem 3*). This follows immediately from Lemmas 6 and 7. \square

Remark 6. We have restricted our attention here to the CSIDH case predominantly for simplicity; there should be no theoretical obstruction to proving similar results in the ordinary case. The theory of refined Humbert invariants are well understood for principally polarized product abelian surfaces $A = E_1 \times E_2$ where E_1 and E_2 are ordinary elliptic curves. These invariants could be used to study computational assumptions on isogeny schemes using ordinary elliptic curves such as [9,54,11].

3 Computing refined Humbert invariants: a survey

The reductions of Section 2 show that, given as domain and codomain supersingular elliptic curves E_0 and E_A coming from a cryptographic primitive such as CSIDH or SQISign, computing an isogeny between them is as hard as computing the refined Humbert invariant of $E_0 \times E_A$ with the product polarization. This is interesting primarily as it places the isogeny problem in the context of the following more general computational problem:

Problem 5. Given a uniformly random principally polarized supersingular abelian surface (A, θ) , compute the refined Humbert invariant of (A, θ) .

In the case that (A, θ) is a product surface, this looks very similar to Problems 4 and 2, but in all other cases this is very different and there could, in principle, be different methods for computation.

Suppose that there exists an efficient algorithm to compute the refined Humbert invariant of a Jacobian of a curve of genus 2. Then this could be extended to an efficient algorithm to compute the refined Humbert invariant of a product surface $E \times E'$ by computing a gluing isogeny φ from $E \times E'$ into any Jacobian $\mathcal{J}(\mathcal{C})$, computing the refined Humbert invariant of $\mathcal{J}(\mathcal{C})$, and pulling back the refined Humbert invariant of $\mathcal{J}(\mathcal{C})$ along φ to deduce the refined Humbert invariant of $E \times E'$. Furthermore, Proposition 2 below suggests that, given the refined Humbert invariant of a supersingular Jacobian $\mathcal{J}(\mathcal{C})$ of a genus 2 curve \mathcal{C} and an isogeny from $\mathcal{J}(\mathcal{C})$ to a product surface $E \times E'$, it would not be too complicated to compute this pullback.

Proposition 2. *Let (A_i, θ_i) be two principally polarized abelian surfaces for $i = 1, 2$, and let $\pi : A_1 \rightarrow A_2$ be an isogeny such that $\hat{\pi}\theta_2\pi = N\theta_1$ for some $N \geq 1$. Then $\pi^* : \text{NS}(A_2) \rightarrow \text{NS}(A_1)$ is injective with finite cokernel, and we have*

$$q_{(A_1, \theta_1)}(\pi^*(D)) = N^2 q_{(A_2, \theta_2)}(D) \text{ for all } D \in \text{NS}(A_2). \quad (4)$$

Proof. See [31, Proposition 17].

Thus, solving Problem 5 for Jacobians (over \mathbb{F}_{p^2} or \mathbb{F}_p) would solve the computational refined Humbert invariant problem for elliptic products (Problem 2 or

Problem 4) and hence the computational supersingular isogeny problem (Problem 1 or Problem 3 respectively).

In this section we address a natural question arising from this connection: what are the best known algorithms to solve Problem 5? Do there exist certain special cases in which this problem becomes easier? See Section 3.3.

In order to discuss the above questions, for the convenience of the reader, we first give a review of the theory of refined Humbert invariants in Sections 3.1 and 3.2. Finally, in Section 3.4 we discuss some potential applications of the relationship between Problem 5 and splittings of principally polarized abelian surfaces.

3.1 Refined Humbert invariants of product surfaces

Theorem 4 makes use of the classical isomorphism $\text{NS}(E_1 \times E_2) \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \text{Hom}(E_1, E_2)$ to give rise to an alternative, simple expression for refined Humbert invariants of product surfaces.

This particular case also gives an insight about understanding dimension one isogenies by using invariants of principally polarized abelian surfaces.

Definition 27. [18, Corollary of Section 6.4] *Let X and Y be varieties. If $f : X \rightarrow Y$ is a morphism of varieties, the graph $\Gamma(f)$ of f is defined to be*

$$\Gamma(f) := \{(x, y) \in X \times Y | y = f(x)\}.$$

Theorem 4. *Let $A = E_1 \times E_2$ be a product of two elliptic curves. Then, we have a group isomorphism*

$$\begin{aligned} \mathcal{D} : \mathbb{Z} \oplus \mathbb{Z} \oplus \text{Hom}(E_1, E_2) &\longrightarrow \text{NS}(A) \\ (a, b, \varphi) &\mapsto (a - 1)\theta_1 + (b - \deg(\varphi))\theta_2 + \Gamma_{-\varphi} \\ &=: D(a, b, \varphi), \end{aligned} \quad (5)$$

where $\theta_i = p_i^*(0_{E_i})$ is the pullback of the identity along the natural projection maps onto the i^{th} coordinate, and $\Gamma_{-\varphi}$ is the graph of $-\varphi$. Then the rule $(a, b, \varphi) \rightarrow [\mathcal{D}(a, b, \varphi)] := \mathcal{D}(a, b, \varphi) + \text{Div}^0(A) \in \text{NS}(A)$ defines a group isomorphism. Moreover, for two divisors $D_1 = \mathcal{D}(a, b, \varphi)$ and $D_2 = \mathcal{D}(a', b', \varphi')$ in $\text{NS}(A)$, the intersection number of the divisors is given by

$$(D_1 \cdot D_2) = ab' + a'b - \beta_d(\varphi, \varphi') \quad (6)$$

where β_d is the bilinear form associated to the \deg_{E_1, E_2} on $\text{Hom}(E_1, E_2)$ as in Definition 24. Thus

$$(\mathcal{D}(a, b, f) \cdot \mathcal{D}(a, b, f)) = 2(ab - \deg(f)), \quad (\mathcal{D}(a, b, f) \cdot (x\theta_1 + y\theta_2)) = bx + ay. \quad (7)$$

Proof. See [29, Proposition 23].

Recall from Definition 2 that a bilinear form β_d is defined by

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

Definition 28. *The intersection form on A is an integral quadratic form q_A on $\text{NS}(A)$ such that, for all $D \in \text{NS}(A)$, we have that*

$$q_A(D) = \frac{1}{2}(D \cdot D).$$

The relation between the intersection form, Definition 28 above, and the degree map, see Definition 24, is obtained by

$$q_A(x, y, \varphi) = xy - \deg_{E_1, E_2}(\varphi). \quad (8)$$

Corollary 1. *The determinant of the Néron-Severi group of $A = E \times E'$ with respect to the intersection form is given by*

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

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

Proof. See [31, Lemma 28].

The intersection form q_A is an indefinite integral quadratic form in $\rho = n + 1 = r + 2$ variables where ρ is the Picard number of A and r is the rank of $\text{Hom}(E_1, E_2)$.

Using Equation (6) above, we can easily calculate the intersection numbers of divisors on abelian product surfaces with the degree map. Moreover, we can numerically characterize principal polarizations in the following simple description.

Proposition 3. *Let A/K be a CM product surface and let $D = \mathcal{D}(a, b, \varphi) \in \text{NS}(A)$, using the notation of Theorem 4. Then $\text{cl}(D) \in \mathcal{P}(A)$ if and only if $a > 0$ and $ab - \deg(\varphi) = 1$. Thus, every principal polarization of A has the form $\mathcal{D}(n_1, n_2, n_3\varphi)$ with $\varphi \in \text{Hom}(E_1, E_2)$ and $n_1, n_2 > 0$ such that $n_1 n_2 - n_3^2(\deg(\varphi)) = 1$.*

Proof. See [29, Corollary 25].

Furthermore, Lemma 2 above, used repeatedly in the reductions, is really a consequence of Theorem 4 derived via the following corollary:

Corollary 2. *Let E/K and E'/K be elliptic curves over a field K . For $a, b \in \mathbb{Z}$ and $\varphi \in \text{Hom}(E, E')$, we have that*

$$q_{(E \times E', \theta_E \times \theta_{E'})}(\mathcal{D}(a, b, \varphi) + \mathbb{Z}(\theta_E \times \theta_{E'})) = (a - b)^2 + 4 \deg(\varphi). \quad (9)$$

Proof. See [30, Lemma 21].

Finally, one could ask when a given refined Humbert invariant is the refined Humbert invariant of a Jacobian of a curve of genus 2 with irreducible polarization or a product surface with reducible polarization. For this, we have the *irreducibility criterion* [29, Proposition 6] as follows.

Definition 29. [67, Satz 2] A polarization $\theta \in \mathcal{P}(A)$ is called *reducible* (or decomposable) if $\theta = \text{cl}(E_1 + E_2)$ for some elliptic curves E_1 and E_2 on A . Note that we can assume E_1 and E_2 to be elliptic subgroups of A . The set of reducible polarizations on A is denoted by $\mathcal{P}(A)^{\text{red}}$.

The reducible polarizations can be classified as follows.

Proposition 4. [33, Proposition 4] Let $E_1, E_2 \leq A$ be elliptic subgroups of an abelian surface A . If $\theta = \text{cl}(E_1 + E_2) \in \mathcal{P}(A)$, then there is an isomorphism $\omega : E_1 \times E_2 \xrightarrow{\sim} A$ such that $\omega(\theta_{E_i}) = E_i$ for $i = 1, 2$ where $\theta_{E_1} = E_1 \times \{0\}$ and $\theta_{E_2} = \{0\} \times E_2$, so in particular $\omega^*\theta = \theta_{E_1, E_2} := \text{cl}(\theta_{E_1} + \theta_{E_2})$. Thus $\mathcal{P}(A)^{\text{red}} \neq \emptyset$ if and only if A is an abelian product surface, i.e., $A \sim E_1 \times E_2$ for elliptic curves E_i where $i = 1, 2$. Furthermore, if $\theta \in \mathcal{P}(A)$ is any principal polarization, then

$$\theta \in \mathcal{P}(A)^{\text{red}} \iff q_{(A, \theta)}([D]) = 1 \text{ for some } [D] \in \text{NS}(A, \theta). \quad (10)$$

Moreover, if $\theta \in \mathcal{P}(A)^* := \mathcal{P}(A) \setminus \mathcal{P}(A)^{\text{red}}$, then $\theta = \theta_C$ for some smooth genus 2 curve on A .

Remark 7. A polarization θ comes from some smooth genus 2 curve C on an abelian surface A as in Proposition 4, then it is a theta divisor as in Definition 16.

3.2 Elliptic subcovers of abelian surfaces

Definition 30. Let C be a curve of genus 2 and let $\mathcal{J}(C)$ be its Jacobian with the theta divisor θ_C . For ease of notation, we write

$$q_C := q_{(\mathcal{J}(C), \theta_C)}.$$

Definition 31. Let C be a curve of genus 2 over an arbitrary field K . An elliptic subcover is a finite morphism $F : C \rightarrow E$ to an elliptic curve E/K which does not factor over a non-trivial isogeny of E . The degree of a subcover F is its degree as a morphism.

If $f' : C \rightarrow E'$ is another elliptic subcover, then F' is said to be *equivalent* to f if there is an isomorphism $\varphi : E \xrightarrow{\sim} E'$ such that $F' = \varphi \circ F$. The understanding of the set of equivalence classes of elliptic subcovers $\mathcal{E}(C)$ of a genus 2 curve C is equivalent to studying the set of maximal elliptic subfields of the function field $\kappa(C)$ of C . It is well-known that $\mathcal{E}(C)$ has 0, 2, or infinitely many elements [3]. We have that C has infinitely many elliptic subcovers when there exists an elliptic curve E/K such that the Jacobian $\mathcal{J}(C)$ of C is K -isogenous to some $E \times E$. A first understanding of the problem $\mathcal{E}(C)$ was established in [26] for the case $K = \overline{K}$; it was shown that the refined Humbert invariant q_C (as in Definition 30) gives a theoretical description of $\mathcal{E}(C)$. It establishes a bijection between $\mathcal{E}(C)$ and the set of primitive solutions x of $q(x) = n^2$ for $n \in \mathbb{Z}_{>0}$ [26, Theorem 4.5]. Later, Kani [31] extended this result to an arbitrary field, and we state the related theorems.

Theorem 5. *The curve \mathcal{C}/K has an elliptic subcover of degree n if and only if the refined Humbert invariant $q_{\mathcal{C}}$ primitively represents n^2 .*

Proof. See [31, Theorem 20].

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

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

Proof. See [31, Lemma 30].

Definition 32. *A presentation (E, E', ψ) of degree N of \mathcal{C}/K arises from a given elliptic subcover $F : \mathcal{C} \rightarrow E$ of degree N and is a triple consisting of E , an isogenous elliptic curve E'/K , and an isomorphism $\psi : E[N] \rightarrow E'[N]$ that is an anti-isometry with respect to the Weil pairing e_N . The isogeny defect m_ψ is defined as*

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

Let $\deg_{E, E'}$ denote the degree quadratic form on $\text{Hom}(E, E')$ as in Definition 24, and let $\det(\deg_{E, E'})$ denote its determinant.

Theorem 6. *If \mathcal{C}/K has a presentation (E, E', ψ) of degree N with $\text{char}(K) \nmid N$ and isogeny defect $m = m_\psi$, and if $r = \text{rank}(\text{Hom}(E, E')) \geq 1$, then the refined Humbert invariant $q_{\mathcal{C}}$ is a positive definite quadratic form of rank $r+1$ which satisfies properties*

- (i) $\det(q_{\mathcal{C}}) = 2^{2r+1}m^2 \det(\deg_{E, E'})$.
- (ii) $q_{\mathcal{C}}$ primitively represents N^2 .
- (iii) $q_{\mathcal{C}}(x_1, \dots, x_{r+1}) \equiv 0, 1 \pmod{4}$, for all $x_1, \dots, x_{r+1} \in \mathbb{Z}$.
- (iv) $q_{\mathcal{C}}(x'_1, \dots, x'_{r+1}) \neq 1$ for any solution $x'_1, \dots, x'_{r+1} \in \mathbb{Z}$.

Proof. See [31, Theorem 3].

Theorem 7. *If (E, E', ψ) is a presentation of degree N of a curve \mathcal{C}/K of genus 2 with $\text{char}(K) \nmid N$, then $m_\psi = 1$ if and only if $\mathcal{J}(\mathcal{C}) \cong E \times E'$.*

Proof. See [31, Theorem 4].

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

Proof. See [31, Corollary 5].

Remark 8. An advantage of a refined Humbert invariant $q_{(A, \theta)}$ of a principally polarized abelian surface (A, θ) is that it makes explicit use of the intersection theory of divisors on surfaces, see Chapter V.1 of [22]. At first sight, it may seem like, for $A = E_1 \times E_2$, it is sufficient to look at the degree map \deg_{E_1, E_2} on $\text{Hom}(E_1, E_2)$ instead of a refined Humbert invariant $q_{(A, \theta)}$ of the surface (A, θ) . To the best of our knowledge, there is no generic method to understand degree maps on \deg_{E_1, E_2} on $\text{Hom}(E_1, E_2)$ without knowing the endomorphosm rings of (or equations defining) E_1 and E_2 and using a variant of KLPT algorithm [36].

3.3 Computing refined Humbert invariants - known methods

In this section we summarize algorithms from the literature looking at the computational refined Humbert invariant problem; the main cases that have been studied to date are the CM abelian product surface case and cases in which the abelian surface has special automorphisms.

CM abelian product surfaces In this section, we present an overview of the state-of-the-art on computing the refined Humbert invariant of a CM abelian product surface $(A, \theta) = (E_1 \times E_2, \theta_{E_1} \times \theta_{E_2})$, whose refined Humbert invariant $q_{(A, \theta)}$ is a ternary integral quadratic form [27, Theorem 2]. The method we present relies on an oracle to compute cyclic isogenies $h : E_1 \rightarrow E_2$. To calculate $q_{(A, \theta)}$ by using [29, Proposition 29], it requires finding a suitable basis of $\text{NS}(A, \theta)$. The easiest way is to extend θ to a basis of $\text{NS}(A)$ which can be achieved by [29, Proposition 29] again. To do this, we use Theorem 4 about the structure of the Néron-Severi group.

We have that $\text{rank}(\text{Hom}(E_1, E_2)) = 2$ as $\text{Hom}(E_1, E_2)$ is a $\text{End}(E_1)$ -ideal and E_1 is a CM elliptic curve, so $\text{rank}(\text{NS}(A)) = 4$. The first aim is to find a basis of $\text{NS}(A)$ that contains θ . By Proposition 3 above, the polarization θ can be written as $\mathcal{D}(n_1, n_2, n_3\varphi)$ for some $n_1, n_2, n_3 \in \mathbb{Z}$ and a cyclic isogeny $\varphi \in \text{Hom}(E_1, E_2)$. Since φ is a (nonzero) cyclic isogeny, it is primitive in $\text{Hom}(E_1, E_2)$ and can be extended to a basis $\{\varphi = \varphi_1, \varphi_2\}$ of $\text{Hom}(E_1, E_2)$. Then

$$\{\text{cl}(\theta), \text{cl}(\theta_2), \text{cl}(\Gamma_{\varphi_1}^*), \text{cl}(\Gamma_{\varphi_2}^*)\}$$

is a basis of $\text{NS}(E_1 \times E_2)$ by Corollary 1 above (or [29, Corollary 24]). Let $d = \deg(\varphi)$, and let $\theta_2 = \mathcal{D}(0, 1, 0)$, $D_3 := \mathcal{D}(-n_3d, 0, -n_2\varphi)$ and $D_4 := \mathcal{D}(0, 0, \varphi_2)$. Then by [29, Proposition 29], we have that

$$\beta = \{\theta, \theta_2, D_3, D_4\}$$

is a basis of $\text{NS}(A)$. We therefore get a basis of $\text{NS}(A, \theta)$ as $\tilde{\beta} = \{\tilde{\theta}_2, \tilde{D}_3, \tilde{D}_4\}$, where $\tilde{-}$ is the image of $-$ in $\text{NS}(A, \theta)$. Therefore, we obtain the following equality by Proposition 29 in [28],

$$q_{(A, \theta)}(x\tilde{\theta}_2 + y\tilde{D}_3 + z\tilde{D}_4) = q(x, y, z).$$

By using Equation (6) above, we can explicitly find the ternary quadratic form $q(x, y, z)$.

The classification of refined Humbert invariants A first natural question is how to classify the integral quadratic forms q which are equivalent to a refined Humbert invariant $q_{(A, \theta)}$ for a principally polarized abelian surface (A, θ) .

Question: For a randomly chosen integral quadratic form q , does there exist a curve \mathcal{C}/K of genus 2 such that $q \sim qc$?

In the case that q is a binary quadratic form which represents a square, the refined Humbert invariants were classified by Kani [30]. Later, Kani [25] gave a similar classification when q is a primitive ternary quadratic form. Kir [38] proved a similar classification when f is an imprimitive ternary quadratic form, so the classification is complete for the ternary case.

Theorem 8. *Let (A, θ) be a principally polarized abelian surface over a field K and let f be a positive primitive ternary quadratic form satisfying the following conditions:*

- (a) $f(x, y, z) \equiv 0, 1 \pmod{4}$ for all $x, y, z \in \mathbb{Z}$,
- (b) $f(x_0, y_0, z_0) = n^2$ for some $x_0, y_0, z_0, n \in \mathbb{Z}$ with $\gcd(n, \Delta(f)) = 1$.

Then there exists $(A, \theta)/K$ such that f is equivalent to a refined Humbert invariant $q_{(A, \theta)}$ if and only if f satisfies conditions (a) and (b).

Proof. See [25, Theorem 1]. □

Moreover, this result is the key to prove Theorem 9 below, which gives a classification of the imprimitive ternary forms f that are equivalent to a refined Humbert invariant $q_{(A, \theta)}$ for a principally polarized abelian surface (A, θ) . Theorem 8 appears in [37, Theorem 3.1.1.] and is frequently used in [38].

Theorem 9. *Let (A, θ) be a principally polarized abelian surface over a field K and let f be an imprimitive positive ternary quadratic form satisfying the following two conditions:*

- (c) $\frac{1}{2}f$ is an improperly primitive form,
- (d) $f(x_0, y_0, z_0) = (2n)^2$ for some $x_0, y_0, z_0, n \in \mathbb{Z}$ with $\gcd(n, \text{disc}(f)) = 1$.

Then there exists $(A, \theta)/K$ such that f is equivalent to a refined Humbert invariant $q_{(A, \theta)}$ if and only if f satisfies conditions (c) and (d).

Proof. See [38, Theorem 2] for the case of $\text{char}(K) = 0$. See the comments of Kani in [32, p.32] stating that the results of [38] can be extended to arbitrary characteristic by using the argument of the proof of [25, Theorem 2]. □

Even though there is no classification yet for a generic principally polarized abelian surface (A, θ) , there does exist a necessary condition for an integral quadratic form to appear as a refined Humbert invariant, including a quintic refined Humbert invariant, as follows.

Theorem 10. *If there exists $(A, \theta)/K$ such that a given integral quadratic form f is equivalent to a refined Humbert invariant $q_{(A, \theta)}$ then $f \equiv 0, 1 \pmod{4}$.*

Proof. See [25, Theorem 1]. This result appeared in [37, Theorem 3.1.1] □

For cryptographic applications, we are primarily interested in the supersingular/superspecial abelian surfaces. In this case, the refined Humbert invariant corresponding to such a surface is a *quintic integral quadratic form*. In order to understand when a quintic integral quadratic form is a refined Humbert invariant, we would need a classification of such quadratic forms. As mentioned in Section 3.3, the classification has been done for the surfaces for which their corresponding refined Humbert invariants are binary quadratic forms representing a square or ternary quadratic forms. For a similar classification for quintic quadratic forms, we would require well-developed genus theory for this case, which unfortunately does not yet exist in the literature.

Remark 9. Theorems 8 and 9 were later used to give a formula for the number of isomorphism classes of smooth curves of genus 2 lying on an abelian surface A in many cases in [32]. It has also been used to calculate the number of curves of genus 2 with a given refined Humbert invariant in [35].

Remark 10. Note that Algorithm 6 below may return Failure even if q is a refined Humbert invariant as checks are only done up to given bound B . For this to return a definitive answer, meaning returning failure if and only if q is not a refined Humbert invariant, the bound B needs to be chosen to be large enough that the corresponding square n^2 or $(2n)^2$ to be found is the maximum taken over all Jacobians in the isogeny graph of the minimum isogeny degree to an elliptic product.

Automorphism groups The computation of refined Humbert invariants is comparatively easier in the case of a product surface $A = E_1 \times E_2$ due to the existence of the isomorphism in Theorem 4. This is no longer true in the generic case; a generic principally polarized abelian surface is a Jacobian of a curve of genus 2, i.e., $(A, \theta) = (\mathcal{J}(\mathcal{C}), \theta_{\mathcal{C}})$. For this, one tool at our disposal is the use of automorphism groups. Refined Humbert invariants $q_{\mathcal{C}}$ of a genus 2 curve \mathcal{C} have a close relation to the automorphism group of the curve \mathcal{C} .

For the ternary refined Humbert invariant, we recall the results obtained for refined Humbert invariants given the automorphism group by following [39]. For an integral quadratic form q , define

$$R_n(q) = \{(x_1, \dots, x_r) \in \mathbb{Z}^r : q(x_1, \dots, x_r) = n\}$$

and $r_n(q) = |R_n(q)|$. For a ternary quadratic form q , define also

$$\mathbf{a}(q) := \max\{1, r_4(q), 3r_4(q) - 12\}.$$

By [32, Proposition 24], we have that

$$r_4(q_{\mathcal{C}}) = |i(\text{Aut}(\mathcal{C})) - 1|,$$

where denotes the number of involutions of the group $\text{Aut}(\mathcal{C})$, and by [39, Remark 2.1]

$$2\mathbf{a}(q_{\mathcal{C}}) = |\text{Aut}(\mathcal{C})|. \tag{11}$$

Algorithm 6: Check whether a ternary quadratic form is a refined Humbert invariant

Input: • A prime p and a bound $B \in \mathbb{Z}$.
• A ternary quadratic form q .

Output: ‘ q is a refined Humbert invariant’ (of some $(A, \theta)/K$ where $\text{char}(K) = p$), or failure.

```
1 Compute the discriminant  $\Delta(q)$  of  $q$ 
2 If  $\left(\frac{\Delta(q)}{p}\right) \neq 1$  then
3   Return Failure
4 If  $q$  is a primitive form then
5   If for all  $x, y, z \in \mathbb{Z}$ , we have  $q(x, y, z) \equiv 0, 1 \pmod{4}$  then
6     For  $|x_0|, |y_0|, |z_0| \leq B$  do
7       If  $q(x_0, y_0, z_0) = n^2$  and  $\gcd(n, \Delta(q)) = 1$  then
8         Return  $q$  is a refined Humbert invariant
9       else
10      Return Failure
11    else
12    Return Failure
13 If  $q$  is an imprimitive form then
14   If  $\frac{1}{2}q$  improperly primitive then
15     For  $|x_0|, |y_0|, |z_0| \leq B$  do
16       If  $q(x_0, y_0, z_0) = (2n)^2$  and  $\gcd(n, \Delta(q)) = 1$  then
17         Return  $q$  is a refined Humbert invariant
18       else
19     Return Failure
20   else
21   Return Failure
```

Kani [32] showed that the automorphism group $\text{Aut}(\mathcal{C})$ of a genus 2 curve \mathcal{C} can be determined from its associated refined Humbert invariant $q_{\mathcal{C}}$, see [32, Theorem 29]. The list of possibilities for $\text{Aut}(\mathcal{C})$ for any curve \mathcal{C} genus of 2 is given in the first column of Table 2, c.f. [56, Theorem 2].

In Table 3 we list the imprimitive ternary quadratic forms $q_{\mathcal{C}}$ with given $\text{Aut}(\mathcal{C})$, together with $\mathbf{a}(q_{\mathcal{C}})$, $|\text{Aut}^+(q_{\mathcal{C}})|$, and $\mathbf{k}(q_{\mathcal{C}}) = |\text{Aut}^+(q_{\mathcal{C}})|/\mathbf{a}(q_{\mathcal{C}})$, taken from [39]. These are in Eisenstein reduced form (c.f. [13, Theorem 103]). Similarly Table 4, also from [39], lists the primitive Eisenstein reduced ternary forms $q_{\mathcal{C}}$ along with the formulas $\mathbf{a}(q_{\mathcal{C}})$ and $\mathbf{k}(q_{\mathcal{C}})$.

Theorem 11. *Let $q_{\mathcal{C}}$ be a ternary quadratic form so that the Jacobian $\mathcal{J}(\mathcal{C})$ is isogenous to a product $E \times E$ of an elliptic curve E/K with complex multiplication. Then $|\text{Aut}(\mathcal{C})| > 2$ if and only if the refined Humbert invariant $q_{\mathcal{C}}$ is equivalent to one of the ternary quadratic forms listed in Tables 3 and 4 below. In addition, if q is one of the forms listed in Tables 3 and 4 below, then there is a curve \mathcal{C}/K of genus 2 such that $q_{\mathcal{C}}$ is equivalent to q .*

Proof. See [39, Theorem 1.1.]. □

Remark 11. Regarding Theorem 11, some automorphism groups are missing in Table 3. Even though they have been classified for the ternary case in Propositions 5.4.4, 5.4.6, 5.4.7 and 5.4.8 of [38], we do not include these forms in Table 4 as the second part of Theorem 11 cannot be proved with the same method as in the imprimitive case. For details, see [39].

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

$\text{Aut}(\mathcal{C})$	$\mathbf{a}(q_{\mathcal{C}})$	$r_4(q_{\mathcal{C}})$
C_2	1	0
C_{10}	1	0
$C_2 \times C_2$	2	2
D_4	4	4
D_6	6	6
$C_3 \rtimes D_4$	12	8
$\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$	24	12

Table 3. Imprimitive ternary forms q_C corresponding to $\text{Aut}(\mathcal{C})$ when $\mathbf{a}(q_C) \neq 1$.

$\text{Aut}(\mathcal{C})$	q_C	$ \text{Aut}^+(q_C) $	$\mathbf{a}(q_C)$	$\mathbf{k}(q_C)$
$C_2 \times C_2$	$[4, b, c, 4, 4]$ with $b \neq c$	2	2	1
	$[4, b, c, 2r, 0, -4]$ with $r < 0$	2	2	1
	$[4, b, c, 2r, -4, 0]$ with $r < 0$	2	2	1
	$[4, b, c, 0, 0, -4]$	4	2	2
	$[4, b, b, 2r, 4, 4]$ with $r > 0$	4	2	2
	$[4, b, c, 0, -4, 0]$ with $b \neq c$	4	2	2
	$[4, b, c, -b, -4, 0]$ with $b \neq c$	4	2	2
	$[4, c, c, -4, 0, 0]$	4	2	2
D_4	$[4, 4, c, 0, -4, 0]$	4	4	1
	$[4, 4, c, -4, -4, 0]$	8	4	2
D_6	$[4, 4, c, 4, 4, 4]$	6	6	1
	$[4, 4, c, 0, 0 - 4]$	12	6	2
$C_3 \rtimes D_4$	$[4, 4, 4, 0, 0 - 4]$	12	12	1
$\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$	$[4, 4, 4, 4, 4, 4]$	24	24	1

Notation: In the table, we suppose that $|2r| \leq b$, $4 \mid b, c, 2r$ and $4 < b \leq c$. In addition, we suppose that if $r < 0$, then $b \neq -2r$.

Table 4. Primitive ternary forms q_C corresponding to $\text{Aut}(\mathcal{C})$ when $\mathbf{a}(q_C) > 2$.

$\text{Aut}(\mathcal{C})$	q_C	$ \text{Aut}^+(q_C) $	$\mathbf{a}(q_C)$	$\mathbf{k}(q_C)$
D_4	$[4, 4, c, 0, -4, 0]$	4	4	1
	$[4, 4, c, 0, 0, 0]$	8	4	2
	$[4, 4, c', -4, -4, 0]$	8	4	2
D_6	$[4, 4, c, 4, 4, 4]$	6	6	1
	$[4, 4, c, 0, 0 - 4]$	12	6	2

Notation: In the table, we suppose that $4 < c, c'$, and $c \equiv 1 \pmod{4}$ and $c' \equiv 1 \pmod{8}$.

For the quintic refined Humbert invariant, we do not have a nice classification given the automorphism of a genus 2 curve as above. But, there is still a nice connection arising from [30, Theorem 20] and [30, Proposition 35] as follows.

Proposition 6. [32, Proposition 26] *Let $i(\text{Aut}(\mathcal{C}))$ be the number of involutions of $\text{Aut}(\mathcal{C})$. If \mathcal{C}/K is a genus 2 curve, then*

$$|i(\text{Aut}(\mathcal{C})) - 1| = r_4(q_C).$$

Thus, if $r_4(q_C) > 0$, then $\mathcal{J}(\mathcal{C}) \sim E_1 \times E_2$ for some elliptic curves E_i/K , $i = 1, 2$. Moreover, if $r_4(q_C) \geq 3$, then $E_1 \sim E_2$.

More on the intersection of divisors Grieve [21] computed an intersection formula for the self product of a supersingular elliptic curve. Let $p := \text{char}(K) > 0$ and let $A = E \times E$ where E is a supersingular elliptic curve. The elements of $\text{End}_{\theta_E \times \theta_E}^0(A)$ have the following shape:

$$\alpha = \begin{pmatrix} u & x + y\mathbf{i} + z\mathbf{j} + w\mathbf{ij} \\ x - y\mathbf{i} - z\mathbf{j} - w\mathbf{ij} & v \end{pmatrix}, \quad (12)$$

for $v, u, w, x, z, y \in \mathbb{Q}$, and it follows that $\dim_{\mathbb{Q}} \text{End}_{\theta_E \times \theta_E}^0(A) = 6$. If D is a divisor on A with

$$\Phi_{\theta_E \times \theta_E}(D) = \alpha = \begin{pmatrix} u & x + y\mathbf{i} + z\mathbf{j} + w\mathbf{ij} \\ x - y\mathbf{i} - z\mathbf{j} - w\mathbf{ij} & v \end{pmatrix}, \quad (13)$$

then

$$(D \cdot D)/2 = -w^2ab + z^2b + y^2a + uv - x^2. \quad (14)$$

The Equation (14) can be used to compute intersection numbers. If D_1 and D_2 are divisors on A , therefore, we obtain

$$D_1 \cdot D_2 = 2w_1w_2ab + 2z_1z_2b + 2y_1y_2a + u_1v_2 + u_2v_1 - 2x_1x_2. \quad (15)$$

The method can be extended to a product of two supersingular elliptic curves. By using the above formulas, one can re-verify that the refined Humbert invariant of a principally polarized superspecial surface $E \times E'$ can be written as $x^2 + 4 \deg_{E,E'}$ as stated in Lemma 2.

Algorithm 7: Refined Humbert invariant of supersingular $E \times E$.

Input: • A prime p
• A supersingular elliptic curves E/\mathbb{F}_{p^2}
• A \mathbb{Z} -basis $\{b_1, b_2, b_3, b_4\}$ of $\text{End}(E)$
Output: The (quintic) refined Humbert invariant of $E \times E$

- 1 $\deg_{E,E} \leftarrow \text{nrd}(wb_1 + xb_2 + yb_3 + zb_4)$
- 2 $q \leftarrow v^2 + 4 \deg_{E,E}$
- 3 **Return** q

Remark 12. 1. Note that Steps 9 and 18 in Algorithm 8 and Steps 4 and 8 in Algorithm 9 are highly nontrivial checks. Checking something is *not* represented is quick as this can be done locally. In practise a probabilistic algorithm is probably the most practical solution to this problem.
2. Note that once c has been computed in Algorithm 8, we can also read off whether qc is primitive or imprimitive just using the conditions stated under Tables 2 and 3.

Algorithm 8: Known automorphisms - D₄ or D₆

Input:

- A prime p ,
- $\text{Aut}(\mathcal{C}) \cong D_4$ or D_6 of a genus 2 curve \mathcal{C} over \mathbb{F}_p such that there exists a presentation (E, E', ψ) of unknown degree N with $p \nmid N$ and known isogeny defect $m = m_\psi$ (c.f. Theorem 6),
- $\Delta(\deg_{E, E'})$

Output:

- The refined Humbert invariant q_C of $(\mathcal{J}(\mathcal{C}), \theta_C)$,
- N

```

1 If  $\text{Aut}(\mathcal{C}) = D_4$  then
2    $q_1 \leftarrow 4x^2 + 4y^2 + cz^2 - 4xz$ 
3    $q_2 \leftarrow 4x^2 + 4y^2 + cz^2$ 
4    $q_3 \leftarrow 4x^2 + 4y^2 + cz^2 - 4yz - 4xz$ 
5   For  $i = 1, 2, 3$  do
6      $\quad$  Compute  $c$  via  $\Delta(q_i) = 2^5 m^2 \Delta(\deg_{E, E'})$ 
7   For  $n \in \mathbb{Z}_{>0}$  do
8     For  $i = 1, 2, 3$  do
9       If  $q_i$  represents  $n^2$  then
10       $\quad$  Return  $q_i, n$ 

11 If  $\text{Aut}(\mathcal{C}) = D_6$  then
12    $q_1 \leftarrow 4x^2 + 4y^2 + cz^2 + 4yz + 4xz + 4xy$ 
13    $q_2 \leftarrow 4x^2 + 4y^2 + cz^2 - 4xy$ 
14   For  $i = 1, 2$  do
15      $\quad$  Compute  $c$  via  $\Delta(q_i) = 2^5 m^2 \Delta(\deg_{E, E'})$ 
16   For  $n \in \mathbb{Z}_{>0}$  do
17     For  $i = 1, 2$  do
18       If  $q_i$  represents  $n^2$  then
19          $\quad$  Return  $q_i, n$ 

```

Algorithm 9: Known automorphisms - $C_3 \rtimes D_4$ or $GL_2(\mathbb{Z}/3\mathbb{Z})$

Input:

- A prime p ,
- $\text{Aut}(\mathcal{C}) \cong C_3 \rtimes D_4$ or $GL_2(\mathbb{Z}/3\mathbb{Z})$ of a genus 2 curve \mathcal{C} over \mathbb{F}_p

Output:

- The refined Humbert invariant q_C of $(\mathcal{J}(\mathcal{C}), \theta_C)$,
- The minimum $N \in \mathbb{Z}_{>0}$ such that there exists an (N, N) -splitting of $\mathcal{J}(\mathcal{C})$

```

1 If  $\text{Aut}(\mathcal{C}) = C_3 \rtimes D_4$  then
2    $qc \leftarrow 4x^2 + 4y^2 + 4z^2 - 4xy$ 
3   For  $n \in \mathbb{Z}_{>0}$  do
4     If  $q$  represents  $n^2$  then
5       Return  $q, n$ 
6 If  $\text{Aut}(\mathcal{C}) = GL_2(\mathbb{Z}/3\mathbb{Z})$  then
7    $qc \leftarrow 4x^2 + 4y^2 + 4z^2 + 4yz + 4xz + 4yz$ 
8   For  $n \in \mathbb{Z}_{>0}$  do
9     If  $q$  represents  $n^2$  then
10      Return  $q, n$ 

```

Remark 13. There is a special family of curves, namely Legendre curves,

$$C_{u,v}/\mathbb{F}_q : \quad y^2 = x^5 + ux^3 + vx,$$

for which we can compute the refined Humbert invariant, see [30, Example 46]. Furthermore, splitting behaviors of these curves $C_{u,v}$ over finite fields \mathbb{F}_q have been studied in [34].

3.4 Splittings from Problem 5

Finally, recall that $q_{(A, \theta)}$ is an integral quadratic form in certain variables and for every positive integer N^2 represented by q there exists an (N, N) -splitting of (A, θ) ; that is, there exists an (N, N) -isogeny from (A, θ) to a split abelian surface. Some potential cases of interest for this fact are:

- Improving our understanding of splittings of generic ordinary principally polarized abelian surfaces. The classical treatment in terms of elliptic integrals for the cases $n \leq 4$, can be found in the works of Legendre, Jacobi, Goursat, and others in [3,5,20,23]. For a modern treatment, we refer to [14,15].
- Improving our understanding of the distribution of split surfaces in the dimension two superspecial isogeny graph. This is something that could be tested on average if we had a classification of quintic refined Humbert invariants, without necessarily solving Problem 5 or related problems such as Problem 2 and in turn the computational isogeny problem.

The heuristic that split surfaces are randomly distributed in the graph contributes to the security arguments of SQISign2D and its variants [10,49,2,16],

and any other schemes making explicit use of the superspecial isogeny graph in dimension 2.

The splitting behaviour of an isogeny graph of a principally polarized superspecial abelian surface has been studied in [41] with refined Humbert invariants. Another application of refined Humbert invariants is also examined in [40] to understand the fixed isogeny problem and a heuristic security assumption on SQISign [12].

References

1. Auffarth, R.: II. Elliptic curves on abelian varieties. *Illinois J. Math.* p. 319– 336 (2015). [10.48550/arXiv.1507.08617](https://doi.org/10.48550/arXiv.1507.08617)
2. Basso, A., De Feo, L., Dartois, P., Leroux, A., Maino, L., Pope, G., Robert, D., Wesolowski, B.: SQISign2D-West: The fast, the small, and the safer. *Cryptology ePrint Archive*, Paper 2024/760 (2024), <https://eprint.iacr.org/2024/760>
3. Bolza, O.: Zur Reduction hyperelliptischer Integrale erster Ordnung auf elliptische mittels einer Transformation dritten Grades. *Math. Ann.* **50**(2-3), 314–324 (1898), <https://doi.org/10.1007/BF01448072>
4. Bosma, W., Cannon, J., Playoust, C.: The Magma Algebra System i: The user language. *Journal of Symbolic Computation* **24**(3), 235–265 (1997). <https://doi.org/10.1006/jsco.1996.0125>
5. Brioschi, F.: Sur la réduction de l'intégrale hyperelliptique à l'elliptique par une transformation du troisième degré. *Ann. Sci. École Norm. Sup. (3)* **8**, 227–230 (1891), <https://doi.org/10.24033/asens.357>
6. Buell, D.A.: Binary quadratic forms. Classical theory and modern computations. Springer-Verlag, New York (1989)
7. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. *Advances in Cryptology – ASIACRYPT 2018* **11274**, 395–427 (2018). https://doi.org/10.1007/978-3-030-03332-3_15
8. Conway, J.H., Sloane, N.J.A.: Sphere packings, lattices and groups, Grundlehren der mathematischen Wissenschaften, Fundamental Principles of Mathematical Sciences, vol. 290. Springer-Verlag, New York, 3 edn. (1999). <https://doi.org/10.1007/978-1-4757-6568-7>
9. Couveignes, J.M.: Hard homogeneous spaces. *Cryptology ePrint Archive*, Paper 2006/291 (2006), <https://eprint.iacr.org/2006/291>
10. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQISignHD: New dimensions in cryptography. *Advances in Cryptology – EUROCRYPT 2024* pp. 3–32 (2024). https://doi.org/10.1007/978-3-031-58716-0_1
11. De Feo, L., Kieffer, J., Smith, B.: Towards practical key exchange from ordinary isogeny graphs. In: *Advances in Cryptology – ASIACRYPT 2018*. pp. 365–394. Springer International Publishing, Cham (2018), https://link.springer.com/chapter/10.1007/978-3-030-03332-3_14
12. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: Compact post-quantum signatures from quaternions and isogenies. In: *Advances in Cryptology – ASIACRYPT*. pp. 64–93. Springer International Publishing (2020). https://doi.org/10.1007/978-3-030-64837-4_3
13. Dickson, L.: *Studies in Number Theory*. U Chicago Press, Chicago, first ed. 1930. Chelsea Publ. Co., New York (1957)

14. Djukanović, M.: Split jacobians and lower bounds on heights. Ph.D. thesis, Universiteit Leiden (2017), <http://hdl.handle.net/1887/54944>
15. Djukanović, M.: Families of (3,3)-split Jacobians (2019), <https://arxiv.org/abs/1811.10075>
16. Duparc, M., Fouotsa, T.B.: SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies. In: Advances in Cryptology – ASIACRYPT 2024. p. 396–429. Springer-Verlag, Berlin, Heidelberg (2024), https://doi.org/10.1007/978-981-96-0891-1_13
17. 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. pp. 329–368. Springer International Publishing (2018). https://doi.org/10.1007/978-3-319-78372-7_11
18. Fulton, W.: Algebraic Curves: An Introduction to Algebraic Geometry. Addison-Wesley Publishing Company, Advanced Book Program (1989)
19. Goren, E.Z., Love, J.R.: Supersingular elliptic curves, quaternion algebras and applications to cryptography (2025), <https://arxiv.org/abs/2410.06123>
20. Goursat, E.: Sur la réduction des intégrales hyperelliptiques. Bull. Soc. Math. France **13**, 143–162 (1885), <https://doi.org/10.24033/bsmf.300>
21. Grieve, N.: Reduced norms and the Riemann-Roch theorem for abelian varieties. New York Journal of Mathematics, 23 (2017), <https://nyjm.albany.edu/j/2017/23-47p.pdf>
22. Hartshorne, R.: Algebraic Geometry. Springer, New York (1977)
23. Jacobi, C.G.J.: Review of Legendre’s ‘Traité des fonctions elliptiques, troisième supplément’. J. reine angew. Math. **8**, 413–417 (1832)
24. Jones, B.: The Arithmetic theory of Quadratic Forms. Carus Math. Monogr., Wiley, New York (1950)
25. Kani, E.: The refined Humbert invariant for abelian product surfaces with complex multiplication. Preprint, 23 pages
26. Kani, E.: Elliptic curves on abelian surfaces. Manuscripta mathematica **84**, 199–223 (1994), <https://doi.org/10.1007/BF02567454>
27. Kani, E.: Products of CM elliptic curves. Collect. Math. **62**(3), 297–339 (2011), <https://doi-org.proxy.queensu.ca/10.1007/s13348-010-0029-1>
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), <https://doi.org/10.1016/j.jnt.2013.12.006>
29. Kani, E.: The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. Collectanea Mathematica **67**, 21–54 (2016), <https://doi-org.proxy.queensu.ca/10.1007/s13348-015-0148-9>
30. Kani, E.: Elliptic subcovers of a curve of genus 2. II. The refined Humbert invariant. Journal of Number Theory **193**, 302–335 (2018). <https://doi.org/10.1016/j.jnt.2018.05.011>
31. Kani, E.: Elliptic subcovers of a curve of genus 2. I. The isogeny defect. Annales mathématiques du Québec **43**, 281–303 (2019). <https://doi.org/10.1007/s40316-018-0105-6>
32. Kani, E.: Curves of genus 2 on abelian surfaces. Preprint, 37 pages (2023), <https://mast.queensu.ca/~kani/papers/CurvesAS2.pdf>
33. Kani, E.: Principal polarizations on abelian product surfaces. preprint (2024), <https://mast.queensu.ca/~kani/papers/prinpol15.pdf>
34. Kani, E., Chou, K.M.J.: Simple geometrically split abelian surfaces over finite fields. Journal of the Ramanujan Mathematical Society, 29 pp. 31–62 (2014), <http://www.mathjournals.org/jrms/2014-029-001/2014-029-001-003.html>

35. Kani, E., Kir, H.: The number of curves of genus 2 with a given refined Humbert invariant. Preprint (2023), <https://mast.queensu.ca/~kani/papers/cardHq13.pdf>
36. Kohel, D., Lauter, K., Petit, C., Tignol, J.P.: On the quaternion ℓ -isogeny path problem. LMS J. Comput. Math. **17**, 418–432 (2014). <https://doi.org/10.1112/S1461157014000151>
37. Kir, H.: Curves of Genus 2 and Quadratic Forms. Ph.D. thesis, Queen's University at Kingston, Ontario, Canada (2024), <https://qspace.library.queensu.ca/items/119efd2b-59b4-4e19-9ff0-9eea3914560e>
38. Kir, H.: The classification of the refined humbert invariant for curves of genus 2. International Journal of Number Theory **21**(06), 1247–1279 (2025). <https://doi.org/10.1142/S1793042125500654>
39. Kir, H.: The refined Humbert invariant for an automorphism group of a genus 2 curve. Contemporary Mathematics (2025), <https://arxiv.org/abs/2310.19076>
40. Kirimh, E., Korpal, G.: On the heuristic security assumption of SQIsign. Preprint (2025)
41. Kirimh, E., Korpal, G.: Testing the folklore, detecting split surfaces, and minimum walks on isogeny graphs of abelian surfaces. Preprint (2025)
42. Lang, S.: Abelian varieties. Springer-Verlag New York (1983)
43. Leroux, A.: Quaternion algebras and isogeny-based cryptography. Ph.D. thesis, Ecole doctorale de l'Institut Polytechnique de Paris (2022), https://www.lix.polytechnique.fr/Labo/Antonin.LEROUX/manuscrit{ }_these.pdf
44. Li, K.Z., Oort, F.: Moduli of Supersingular Abelian Varieties. Lecture Notes in Mathematics, Vol. 1680, Springer, Berlin (1998)
45. Merdy, A.H.L., Wesolowski, B.: Unconditional foundations for supersingular isogeny-based cryptography. Cryptology ePrint Archive, Paper 2025/271 (2025), <https://eprint.iacr.org/2025/271>
46. Milne, J.: Abelian varieties. In: Cornell, G., Silverman, J. (eds.) Arithmetic geometry pp. 103–150 (1986)
47. Milne, J.: Jacobian varieties. In: Cornell, G., Silverman, J. (eds.) Arithmetic geometry pp. 165–212 (1986)
48. Mumford, D.: Abelian Varieties. Oxford University Press, Oxford (1970)
49. Nakagawa, K., Onuki, H.: SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies. Cryptology ePrint Archive, Paper 2024/771 (2024), <https://eprint.iacr.org/2024/771>
50. Nguyen, P.Q., Stehlé, D.: An LLL algorithm with quadratic complexity. SIAM J. of Computing **39**(3), 874—903 (2009). <https://doi.org/10.1137/07070570>
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), https://www.numdam.org/item/AST_1979__64__3_0/
52. Oort, F.: Subvarieties of moduli spaces. Inventiones mathematicae **24**, 95–120 (1974), <http://eudml.org/doc/142272>
53. Pizer, A.K.: An algorithm for computing modular forms on $\gamma_0(n)$. Journal of Algebra **64**(2), 340–390 (1980). [https://doi.org/10.1016/0021-8693\(80\)90151-9](https://doi.org/10.1016/0021-8693(80)90151-9)
54. Rostovtsev, A., Stolbunov, A.: Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Paper 2006/145 (2006), <https://eprint.iacr.org/2006/145>
55. Shafarevich, I.R.: Basic Algebraic Geometry 1: Varieties in Projective Space, Third Edition. Springer-Verlag Berlin Heidelberg 2013 (2013)

56. Shaska, T., Völklein, H.: Elliptic subfields and automorphisms of genus 2 function fields. In: Algebra, arithmetic and geometry with applications, pp. 703–723. Springer (2004), [arXiv:math/0107142](https://arxiv.org/abs/math/0107142)
57. Shioda, T.: Supersingular K3 surfaces. In: Algebraic Geometry. pp. 564–591. Springer, Berlin, Heidelberg (1979). <https://doi.org/10.1007/BFb0066664>
58. Silverman, J.H.: The arithmetic of elliptic curves. Graduate Texts in Mathematics, vol. 106. Springer, New York (2009)
59. Stein, W., et al.: Sage Mathematics Software (Version 10.6). The Sage Development Team (2025), <http://www.sagemath.org>
60. The PARI Group, Univ. Bordeaux: PARI/GP version 2.15.4 (2023), available from <http://pari.math.u-bordeaux.fr/>
61. Tomoyoshi Ibukiyama, Toshiyuki Katsura, F.O.: Supersingular curves of genus two and class numbers. Compositio Mathematica **57**, 127–152 (1986), <http://eudml.org/doc/89752>
62. Torelli, R.: Sulle varietà di Jacobi. Rendiconti A. R. A. d. Lincei **22**, 98–103 (1913)
63. Vignéras, M.F.: Arithmétique des algèbres de quaternions. Springer (1980)
64. Voight, J.: Quaternion Algebras, Graduate Texts in Mathematics, vol. 288. Springer Cham (2021). <https://doi.org/10.1007/978-3-030-56694-4>
65. Voight, J.: Characterizing quaternion rings over an arbitrary base. Journal für die reine und angewandte Mathematik **2011**(657), 113–134 (2011). <https://doi.org/10.1515/crelle.2011.054>
66. Watson, G.L.: Integral Quadratic Forms. Cambridge Univ. Press., Cambridge (1960)
67. Weil, A.: Zum Beweis des Torellischen Satzes. In: Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa. pp. 33–55 (1957), <https://api.semanticscholar.org/CorpusID:125362965>
68. Wesolowski, B.: The supersingular isogeny path and endomorphism ring problems are equivalent. In: FOCS 2021 - 62nd Annual IEEE Symposium on Foundations of Computer Science (2022), <https://hal.science/hal-03340899>