Exploring Kani's Research

Harun KIR
ENS de LYON

The SQIparty 2025
A Workshop on Isogeny-Crypto
Lleida, April 28-30, 2025

April 29, 2025

Overview

- Kani's research.

Overview

- Kani's research.
- Kani dedicated a significant portion of his research and numerous papers to the study of (N, N)-isogenies (in different languages).

Overview

- Kani's research.
- Kani dedicated a significant portion of his research and numerous papers to the study of (N, N)-isogenies (in different languages).
- The key ingredient for his approach is the use of a positive definite quadratic form, so called the refined Humbert invariant.

Overview

- Kani's research.
- Kani dedicated a significant portion of his research and numerous papers to the study of (N, N)-isogenies (in different languages).
- The key ingredient for his approach is the use of a positive definite quadratic form, so called the refined Humbert invariant.
- In 1994, Kani introduced the refined Humbert invariant q_C, which is intrinsically attached to a curve C of genus 2.

Overview

- Kani's research.
- Kani dedicated a significant portion of his research and numerous papers to the study of (N, N)-isogenies (in different languages).
- The key ingredient for his approach is the use of a positive definite quadratic form, so called the refined Humbert invariant.
- In 1994, Kani introduced the refined Humbert invariant q_C, which is intrinsically attached to a curve C of genus 2.
- Especially, over the past decade, he has significantly advanced our understanding of the refined Humbert invariant and has addressed several interesting geometric problems through the application of this theory.

Overview

- Kani's research.
- Kani dedicated a significant portion of his research and numerous papers to the study of (N, N)-isogenies (in different languages).
- The key ingredient for his approach is the use of a positive definite quadratic form, so called the refined Humbert invariant.
- In 1994, Kani introduced the refined Humbert invariant q_C, which is intrinsically attached to a curve C of genus 2.
- Especially, over the past decade, he has significantly advanced our understanding of the refined Humbert invariant and has addressed several interesting geometric problems through the application of this theory.
- I followed a similar approach during my PhD research.

Overview

- Kani's research.
- Kani dedicated a significant portion of his research and numerous papers to the study of (N, N)-isogenies (in different languages).
- The key ingredient for his approach is the use of a positive definite quadratic form, so called the refined Humbert invariant.
- In 1994, Kani introduced the refined Humbert invariant q_C, which is intrinsically attached to a curve C of genus 2.
- Especially, over the past decade, he has significantly advanced our understanding of the refined Humbert invariant and has addressed several interesting geometric problems through the application of this theory.
- I followed a similar approach during my PhD research.
- In this talk, I will advertise this theory to use as a (perhaps theoretical) ingredient in the isogeny-based crypto.

Overview

- Kani's research.
- Kani dedicated a significant portion of his research and numerous papers to the study of (N, N)-isogenies (in different languages).
- The key ingredient for his approach is the use of a positive definite quadratic form, so called the refined Humbert invariant.
- In 1994, Kani introduced the refined Humbert invariant q_C, which is intrinsically attached to a curve C of genus 2.
- Especially, over the past decade, he has significantly advanced our understanding of the refined Humbert invariant and has addressed several interesting geometric problems through the application of this theory.
- I followed a similar approach during my PhD research.
- In this talk, I will advertise this theory to use as a (perhaps theoretical) ingredient in the isogeny-based crypto.
- E. Kırımlı, C. Martindale.
- E. Kırımlı, G. Korpal, On the heuristic security assumption of SQIsign.

Overview

- Kani's research.
- Kani dedicated a significant portion of his research and numerous papers to the study of (N, N)-isogenies (in different languages).
- The key ingredient for his approach is the use of a positive definite quadratic form, so called the refined Humbert invariant.
- In 1994, Kani introduced the refined Humbert invariant q_C, which is intrinsically attached to a curve C of genus 2.
- Especially, over the past decade, he has significantly advanced our understanding of the refined Humbert invariant and has addressed several interesting geometric problems through the application of this theory.
- I followed a similar approach during my PhD research.
- In this talk, I will advertise this theory to use as a (perhaps theoretical) ingredient in the isogeny-based crypto.
- E. Kırımlı, C. Martindale.
- E. Kırımlı, G. Korpal, On the heuristic security assumption of SQIsign.
- Unless stated otherwise, the results presented here are based on Kani's work (explicit, implicit or private communications with him).

Overview

- Kani's research.
- Kani dedicated a significant portion of his research and numerous papers to the study of (N, N)-isogenies (in different languages).
- The key ingredient for his approach is the use of a positive definite quadratic form, so called the refined Humbert invariant.
- In 1994, Kani introduced the refined Humbert invariant q_C, which is intrinsically attached to a curve C of genus 2.
- Especially, over the past decade, he has significantly advanced our understanding of the refined Humbert invariant and has addressed several interesting geometric problems through the application of this theory.
- I followed a similar approach during my PhD research.
- In this talk, I will advertise this theory to use as a (perhaps theoretical) ingredient in the isogeny-based crypto.
- E. Kırımlı, C. Martindale.
- E. Kırımlı, G. Korpal, On the heuristic security assumption of SQIsign.
- Unless stated otherwise, the results presented here are based on Kani's work (explicit, implicit or private communications with him).

Motivation

- Let C be a curve of genus 2 over a field k.

Motivation

- Let C be a curve of genus 2 over a field k.

1. The refined Humbert invariant q_C gives the information about the group $\mathrm{Aut}(C)$, and determines it most of the time.

Motivation

- Let C be a curve of genus 2 over a field k.

1. The refined Humbert invariant q_C gives the information about the group $\mathrm{Aut}(C)$, and determines it most of the time.
2. The refined Humbert invariant q_C detects whether J_C is (n, n)-split or not.

Motivation

- Let C be a curve of genus 2 over a field k.

1. The refined Humbert invariant q_C gives the information about the group $\mathrm{Aut}(C)$, and determines it most of the time.
2. The refined Humbert invariant q_C detects whether J_C is (n, n)-split or not.
3. The refined Humbert invariant q_C gives the number of equivalence classes of the elliptic subcovers of degree n of C.

Motivation

- Let C be a curve of genus 2 over a field k.

1. The refined Humbert invariant q_C gives the information about the group $\mathrm{Aut}(C)$, and determines it most of the time.
2. The refined Humbert invariant q_C detects whether J_C is (n, n)-split or not.
3. The refined Humbert invariant q_C gives the number of equivalence classes of the elliptic subcovers of degree n of C.
4. Given genus 2 curves C and C' (where $J_C \simeq E \times E'$, for CM elliptic curves E and E'), the refined Humbert invariants q_C and $q_{C'}$ detects whether C and C' are isomorphic or not (theoretically at least!).

Motivation

- Let C be a curve of genus 2 over a field k.

1. The refined Humbert invariant q_C gives the information about the group $\mathrm{Aut}(C)$, and determines it most of the time.
2. The refined Humbert invariant q_C detects whether J_C is (n, n)-split or not.
3. The refined Humbert invariant q_C gives the number of equivalence classes of the elliptic subcovers of degree n of C.
4. Given genus 2 curves C and C' (where $J_C \simeq E \times E'$, for CM elliptic curves E and E'), the refined Humbert invariants q_C and $q_{C'}$ detects whether C and C' are isomorphic or not (theoretically at least!).

- By using (1)-(3), I'll reprove (and generalize) a property of the superspecial isogeny graph that was proved by Castryck, Decru, Smith (2020), and also by Katsura and Takashima (2020).

The refined Humbert invariant

- Let K be an algebraically closed field.

The refined Humbert invariant

- Let K be an algebraically closed field.
- Let A be an abelian surface over K, and assume that A has a principal polarization $\theta \in \mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$, where $\equiv$ denotes numerical equivalence.
- Call (A, θ) as a principally polarized abelian surface.

The refined Humbert invariant

- Let K be an algebraically closed field.
- Let A be an abelian surface over K, and assume that A has a principal polarization $\theta \in \mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$, where $\equiv$ denotes numerical equivalence.
- Call (A, θ) as a principally polarized abelian surface.
- If $A \simeq E_1 \times E_2$, then

$$\mathbf{D} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathrm{Hom}\,(E_1, E_2) \xrightarrow{\sim} \mathrm{NS}(A).$$

The refined Humbert invariant

- Let K be an algebraically closed field.
- Let A be an abelian surface over K, and assume that A has a principal polarization $\theta \in \mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$, where $\equiv$ denotes numerical equivalence.
- Call (A, θ) as a principally polarized abelian surface.
- If $A \simeq E_1 \times E_2$, then

$$\mathbf{D} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathrm{Hom}\,(E_1, E_2) \xrightarrow{\sim} \mathrm{NS}(A).$$

- $\mathbf{D}(a, b, h)$ is a principal polarization $\Leftrightarrow$ $a > 0$ and $ab - \deg(h) = 1$, where deg denotes the *degree map* on $\mathrm{Hom}(E_1, E_2)$.

The refined Humbert invariant

- Let K be an algebraically closed field.
- Let A be an abelian surface over K, and assume that A has a principal polarization $\theta \in \mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$, where $\equiv$ denotes numerical equivalence.
- Call (A, θ) as a principally polarized abelian surface.
- If $A \simeq E_1 \times E_2$, then

$$\mathbf{D} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathrm{Hom}\,(E_1, E_2) \xrightarrow{\sim} \mathrm{NS}(A).$$

- $\mathbf{D}(a, b, h)$ is a principal polarization $\Leftrightarrow$ $a > 0$ and $ab - \deg(h) = 1$, where deg denotes the *degree map* on $\mathrm{Hom}(E_1, E_2)$.
- For two divisors $D_1 = \mathbf{D}(a, b, f)$ and $D_2 = \mathbf{D}(a', b', f')$ in $\mathrm{NS}(A)$, the *intersection number* of the divisors is given by

$$(D_1.D_2) = ab' + a'b - \beta_d(f, f'),$$

where $\beta_d(f, f') = \deg(f + f') - \deg(f) - \deg(f')$ is the bilinear form.

The refined Humbert invariant

- Let K be an algebraically closed field.
- Let A be an abelian surface over K, and assume that A has a principal polarization $\theta \in \mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$, where $\equiv$ denotes numerical equivalence.
- Call (A, θ) as a principally polarized abelian surface.
- If $A \simeq E_1 \times E_2$, then

$$\mathbf{D} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathrm{Hom}\,(E_1, E_2) \xrightarrow{\sim} \mathrm{NS}(A).$$

- $\mathbf{D}(a, b, h)$ is a principal polarization $\Leftrightarrow$ $a > 0$ and $ab - \deg(h) = 1$, where deg denotes the *degree map* on $\mathrm{Hom}(E_1, E_2)$.
- For two divisors $D_1 = \mathbf{D}(a, b, f)$ and $D_2 = \mathbf{D}(a', b', f')$ in $\mathrm{NS}(A)$, the *intersection number* of the divisors is given by

$$(D_1.D_2) = ab' + a'b - \beta_d(f, f'),$$

where $\beta_d(f, f') = \deg(f + f') - \deg(f) - \deg(f')$ is the bilinear form.

Definition 2.1.

The refined Humbert invariant of a principally polarized abelian surface (A, θ) is the positive definite quadratic form $q_{(A,\theta)}$ on $\mathrm{NS}(A)/\mathbb{Z}\theta$ defined by

$$q_{(A,\theta)}(D) = (D.\theta)^2 - 2(D.D), \text{ for } D \in \mathrm{NS}(A, \theta).$$

Examples

- $\theta := \mathbf{D}(1,1,0)$ is a product principal polarization on A.

Examples

- $\theta := \mathbf{D}(1, 1, 0)$ is a product principal polarization on A. In this case, $q_{(A,\theta)}$ is equivalent to $x^2 + 4\deg$.

Examples

- $\theta := \mathbf{D}(1,1,0)$ is a product principal polarization on A. In this case, $q_{(A,\theta)}$ is equivalent to $x^2 + 4\deg$.
- If there is an isogeny $h \in \mathrm{Hom}(E_1, E_2)$ such that $\deg(h) \equiv 3 \bmod 4$, then $\mathbf{D}(2, (1+\deg(h))/2, h)$ is a (non-product) principal polarization on A.

Examples

- $\theta := \mathbf{D}(1,1,0)$ is a product principal polarization on A. In this case, $q_{(A,\theta)}$ is equivalent to $x^2 + 4\deg$.
- If there is an isogeny $h \in \mathrm{Hom}(E_1, E_2)$ such that $\deg(h) \equiv 3 \bmod 4$, then $\mathbf{D}(2, (1+\deg(h))/2, h)$ is a (non-product) principal polarization on A.
- Kani's irreducibility criterion:

$$q_{(A,\theta)} = 1 \text{ has a solution } \Leftrightarrow \theta \text{ is a product principal polarization.}$$

Examples

- $\theta := \mathbf{D}(1,1,0)$ is a product principal polarization on A. In this case, $q_{(A,\theta)}$ is equivalent to $x^2 + 4\deg$.
- If there is an isogeny $h \in \mathrm{Hom}(E_1, E_2)$ such that $\deg(h) \equiv 3 \bmod 4$, then $\mathbf{D}(2, (1+\deg(h))/2, h)$ is a (non-product) principal polarization on A.
- Kani's irreducibility criterion:

$$q_{(A,\theta)} = 1 \text{ has a solution } \Leftrightarrow \theta \text{ is a product principal polarization.}$$

- If $(A,\theta) = (J_C, \theta_C)$, for some curve C of genus 2, $q_C := q_{(J_C,\theta_C)}$.

Automorphism groups

- Let C be a curve of genus 2 over K.

Automorphism groups

- Let C be a curve of genus 2 over K.
- Let $\iota(\mathrm{Aut}(C))$ be the number of involutions of the group $\mathrm{Aut}(C)$,

Automorphism groups

- Let C be a curve of genus 2 over K.
- Let $\iota(\mathrm{Aut}(C))$ be the number of involutions of the group $\mathrm{Aut}(C)$, and $R_n(q_C) = \{v : v \text{ is primitive and } q_C(v) = n\}$.

Automorphism groups

- Let C be a curve of genus 2 over K.
- Let $\iota(\mathrm{Aut}(C))$ be the number of involutions of the group $\mathrm{Aut}(C)$, and $R_n(q_C) = \{v : v \text{ is primitive and } q_C(v) = n\}$.
- $\iota(\mathrm{Aut}(C)) - 1 = |R_4(q_C)|$.

Automorphism groups

- Let C be a curve of genus 2 over K.
- Let $\iota(\mathrm{Aut}(C))$ be the number of involutions of the group $\mathrm{Aut}(C)$, and $R_n(q_C) = \{v : v \text{ is primitive and } q_C(v) = n\}$.
- $\iota(\mathrm{Aut}(C)) - 1 = |R_4(q_C)|$.
- The quantity $R_4(q_C)$ completely determines $\mathrm{Aut}(C)$ when C is not superspecial.

Automorphism groups

- Let C be a curve of genus 2 over K.
- Let $\iota(\mathrm{Aut}(C))$ be the number of involutions of the group $\mathrm{Aut}(C)$, and $R_n(q_C) = \{v : v \text{ is primitive and } q_C(v) = n\}$.
- $\iota(\mathrm{Aut}(C)) - 1 = |R_4(q_C)|$.
- The quantity $R_4(q_C)$ completely determines $\mathrm{Aut}(C)$ when C is not superspecial.
- In 2023, I classified genus 2 curves C with $J_C \sim E \times E$, where E is an ordinary CM elliptic curve, according to $\mathrm{Aut}(C)$ using the refined Humbert invariant.

Automorphism groups

- Let C be a curve of genus 2 over K.
- Let $\iota(\mathrm{Aut}(C))$ be the number of involutions of the group $\mathrm{Aut}(C)$, and $R_n(q_C) = \{v : v \text{ is primitive and } q_C(v) = n\}$.
- $\iota(\mathrm{Aut}(C)) - 1 = |R_4(q_C)|$.
- The quantity $R_4(q_C)$ completely determines $\mathrm{Aut}(C)$ when C is not superspecial.
- In 2023, I classified genus 2 curves C with $J_C \sim E \times E$, where E is an ordinary CM elliptic curve, according to $\mathrm{Aut}(C)$ using the refined Humbert invariant.
- Example: Let $C : y^2 = x^6 - 1$.

Automorphism groups

- Let C be a curve of genus 2 over K.
- Let $\iota(\mathrm{Aut}(C))$ be the number of involutions of the group $\mathrm{Aut}(C)$, and $R_n(q_C) = \{v : v \text{ is primitive and } q_C(v) = n\}$.
- $\iota(\mathrm{Aut}(C)) - 1 = |R_4(q_C)|$.
- The quantity $R_4(q_C)$ completely determines $\mathrm{Aut}(C)$ when C is not superspecial.
- In 2023, I classified genus 2 curves C with $J_C \sim E \times E$, where E is an ordinary CM elliptic curve, according to $\mathrm{Aut}(C)$ using the refined Humbert invariant.
- Example: Let $C : y^2 = x^6 - 1$.
- $q_C(x, y, z) = 4x^2 + 4y^2 + 4z^2 + 4yz + 4xz + 4xy$ and $|R_4(q_C)| = 12$.

Automorphism groups

- Let C be a curve of genus 2 over K.
- Let $\iota(\mathrm{Aut}(C))$ be the number of involutions of the group $\mathrm{Aut}(C)$, and $R_n(q_C) = \{v : v \text{ is primitive and } q_C(v) = n\}$.
- $\iota(\mathrm{Aut}(C)) - 1 = |R_4(q_C)|$.
- The quantity $R_4(q_C)$ completely determines $\mathrm{Aut}(C)$ when C is not superspecial.
- In 2023, I classified genus 2 curves C with $J_C \sim E \times E$, where E is an ordinary CM elliptic curve, according to $\mathrm{Aut}(C)$ using the refined Humbert invariant.
- Example: Let $C : y^2 = x^6 - 1$.
- $q_C(x, y, z) = 4x^2 + 4y^2 + 4z^2 + 4yz + 4xz + 4xy$ and $|R_4(q_C)| = 12$.
- $\mathrm{Aut}(C) \simeq \mathrm{GL}_2(3)$.

Elliptic subcovers

- Let k be any field. (Promise: I'll define q_C for any field).

Elliptic subcovers

- Let k be any field. (Promise: I'll define q_C for any field).
- An (minimal) **elliptic subcover** of C is a finite morphism $f : C \to E$, where E is an elliptic curve E/k which does not factor over a non-trivial isogeny of E.

Elliptic subcovers

- Let k be any field. (Promise: I'll define q_C for any field).
- An (minimal) **elliptic subcover** of C is a finite morphism $f : C \to E$, where E is an elliptic curve E/k which does not factor over a non-trivial isogeny of E.
- If $f : C \to E$ and $f' : C \to E'$ are two elliptic subcovers and if there is an isomorphism $\phi : E \xrightarrow{\sim} E'$ such that $f' = \phi \circ f$, then f' and f are **equivalent**.

Elliptic subcovers

- Let k be any field. (Promise: I'll define q_C for any field).
- An (minimal) **elliptic subcover** of C is a finite morphism $f : C \to E$, where E is an elliptic curve E/k which does not factor over a non-trivial isogeny of E.
- If $f : C \to E$ and $f' : C \to E'$ are two elliptic subcovers and if there is an isomorphism $\phi : E \xrightarrow{\sim} E'$ such that $f' = \phi \circ f$, then f' and f are **equivalent**.
- Let $\mathcal{E}_n(C)$ be the set of equivalence classes of elliptic subcovers of degree n of C.

Elliptic subcovers

- Let k be any field. (Promise: I'll define q_C for any field).
- An (minimal) **elliptic subcover** of C is a finite morphism $f : C \to E$, where E is an elliptic curve E/k which does not factor over a non-trivial isogeny of E.
- If $f : C \to E$ and $f' : C \to E'$ are two elliptic subcovers and if there is an isomorphism $\phi : E \xrightarrow{\sim} E'$ such that $f' = \phi \circ f$, then f' and f are **equivalent**.
- Let $\mathcal{E}_n(C)$ be the set of equivalence classes of elliptic subcovers of degree n of C.
- By Kani (1994 and 2018), there is a bijection (by the rule $f \mapsto f^* J_E + \mathbb{Z}\theta_C$) between

$$\mathcal{E}_n(C) \xrightarrow{\sim} R_{n^2}(q_C)$$

Elliptic subcovers

- Let k be any field. (Promise: I'll define q_C for any field).
- An (minimal) **elliptic subcover** of C is a finite morphism $f : C \to E$, where E is an elliptic curve E/k which does not factor over a non-trivial isogeny of E.
- If $f : C \to E$ and $f' : C \to E'$ are two elliptic subcovers and if there is an isomorphism $\phi : E \xrightarrow{\sim} E'$ such that $f' = \phi \circ f$, then f' and f are **equivalent**.
- Let $\mathcal{E}_n(C)$ be the set of equivalence classes of elliptic subcovers of degree n of C.
- By Kani (1994 and 2018), there is a bijection (by the rule $f \mapsto f^* J_E + \mathbb{Z}\theta_C$) between

$$\mathcal{E}_n(C) \xrightarrow{\sim} R_{n^2}(q_C)$$

  - The genus 2 curve C/k has an elliptic subcover of degree $n \Leftrightarrow q_C \to n^2$.

Elliptic subcovers

- Let k be any field. (Promise: I'll define q_C for any field).
- An (minimal) **elliptic subcover** of C is a finite morphism $f : C \to E$, where E is an elliptic curve E/k which does not factor over a non-trivial isogeny of E.
- If $f : C \to E$ and $f' : C \to E'$ are two elliptic subcovers and if there is an isomorphism $\phi : E \xrightarrow{\sim} E'$ such that $f' = \phi \circ f$, then f' and f are **equivalent**.
- Let $\mathcal{E}_n(C)$ be the set of equivalence classes of elliptic subcovers of degree n of C.
- By Kani (1994 and 2018), there is a bijection (by the rule $f \mapsto f^* J_E + \mathbb{Z}\theta_C$) between

$$\mathcal{E}_n(C) \xrightarrow{\sim} R_{n^2}(q_C)$$

  - The genus 2 curve C/k has an elliptic subcover of degree $n \Leftrightarrow q_C \to n^2$.
  - J_C is (n, n)-split $\Leftrightarrow q_C \to n^2$.

The superspecial isogeny graph

- For each prime p, a directed multigraph $\mathcal{G}_p(\ell)$, where ℓ is a prime different from p, is defined as follows:

The superspecial isogeny graph

- For each prime p, a directed multigraph $\mathcal{G}_p(\ell)$, where ℓ is a prime different from p, is defined as follows:
- The **vertices** of $\mathcal{G}_p(\ell)$ represent the isomorphism classes of superspecial principally polarized abelian surfaces (s.p.p.a.s) over $\overline{\mathbb{F}}_p$ and

The superspecial isogeny graph

- For each prime p, a directed multigraph $\mathcal{G}_p(\ell)$, where ℓ is a prime different from p, is defined as follows:
- The **vertices** of $\mathcal{G}_p(\ell)$ represent the isomorphism classes of superspecial principally polarized abelian surfaces (s.p.p.a.s) over $\overline{\mathbb{F}}_p$ and the **edges** of the graph are the (ℓ, ℓ)-isogenious up to isomorphism.

The superspecial isogeny graph

- For each prime p, a directed multigraph $\mathcal{G}_p(\ell)$, where ℓ is a prime different from p, is defined as follows:
- The **vertices** of $\mathcal{G}_p(\ell)$ represent the isomorphism classes of superspecial principally polarized abelian surfaces (s.p.p.a.s) over $\overline{\mathbb{F}}_p$ and the **edges** of the graph are the (ℓ, ℓ)-isogenious up to isomorphism.
- Recall: if (A_1, λ_1) and (A_2, λ_2) are s.p.p.a.s over$\overline{\mathbb{F}}_p$, and if $\phi : A_1 \to A_2$ is an isogeny with $\hat{\phi}\lambda_2\phi = [\ell]\lambda_1$ such that $\operatorname{Ker}\phi \leqslant A_1[\ell]$ is maximally isotropic with respect to the ℓ-Weil pairing, we say ϕ is $(\ell, \ell)-$isogeny.

The superspecial isogeny graph

- For each prime p, a directed multigraph $\mathcal{G}_p(\ell)$, where ℓ is a prime different from p, is defined as follows:
- The **vertices** of $\mathcal{G}_p(\ell)$ represent the isomorphism classes of superspecial principally polarized abelian surfaces (s.p.p.a.s) over $\overline{\mathbb{F}}_p$ and the **edges** of the graph are the (ℓ, ℓ)-isogenious up to isomorphism.
- Recall: if (A_1, λ_1) and (A_2, λ_2) are s.p.p.a.s over$\overline{\mathbb{F}}_p$, and if $\phi : A_1 \to A_2$ is an isogeny with $\hat{\phi}\lambda_2\phi = [\ell]\lambda_1$ such that $\mathrm{Ker}\,\phi \leqslant A_1[\ell]$ is maximally isotropic with respect to the ℓ-Weil pairing, we say ϕ is $(\ell, \ell)-$isogeny.
- Let $\mathit{split}_\ell(J_C)$ be the set of isomorphism classes of **split** (**decomposed**) (ℓ, ℓ)-isogenies from J_C to a superspecial abelian surface with a product principal polarization.

The superspecial isogeny graph

- For each prime p, a directed multigraph $\mathcal{G}_p(\ell)$, where ℓ is a prime different from p, is defined as follows:
- The **vertices** of $\mathcal{G}_p(\ell)$ represent the isomorphism classes of superspecial principally polarized abelian surfaces (s.p.p.a.s) over $\overline{\mathbb{F}}_p$ and the **edges** of the graph are the (ℓ, ℓ)-isogenious up to isomorphism.
- Recall: if (A_1, λ_1) and (A_2, λ_2) are s.p.p.a.s over$\overline{\mathbb{F}}_p$, and if $\phi : A_1 \to A_2$ is an isogeny with $\hat{\phi}\lambda_2\phi = [\ell]\lambda_1$ such that $\operatorname{Ker}\phi \leqslant A_1[\ell]$ is maximally isotropic with respect to the ℓ-Weil pairing, we say ϕ is $(\ell, \ell)-$isogeny.
- Let $\mathit{split}_\ell(J_C)$ be the set of isomorphism classes of **split** (**decomposed**) (ℓ, ℓ)-isogenies from J_C to a superspecial abelian surface with a product principal polarization.
- By Castryck, Decru, Smith (2020), $|\mathit{split}_2(J_C)| \leq 6$.

The superspecial isogeny graph

- For each prime p, a directed multigraph $\mathcal{G}_p(\ell)$, where ℓ is a prime different from p, is defined as follows:
- The **vertices** of $\mathcal{G}_p(\ell)$ represent the isomorphism classes of superspecial principally polarized abelian surfaces (s.p.p.a.s) over $\overline{\mathbb{F}}_p$ and the **edges** of the graph are the (ℓ, ℓ)-isogenious up to isomorphism.
- Recall: if (A_1, λ_1) and (A_2, λ_2) are s.p.p.a.s over$\overline{\mathbb{F}}_p$, and if $\phi : A_1 \to A_2$ is an isogeny with $\hat{\phi}\lambda_2\phi = [\ell]\lambda_1$ such that $\operatorname{Ker}\phi \leqslant A_1[\ell]$ is maximally isotropic with respect to the ℓ-Weil pairing, we say ϕ is $(\ell, \ell)-$isogeny.
- Let $\mathit{split}_\ell(J_C)$ be the set of isomorphism classes of **split** (**decomposed**) (ℓ, ℓ)-isogenies from J_C to a superspecial abelian surface with a product principal polarization.
- By Castryck, Decru, Smith (2020), $|\mathit{split}_2(J_C)| \leq 6$.
- Katsura and Takashita (2020) calculate $|\mathit{split}_2(J_C)|$ in each case in terms of $\mathcal{A}ut(C)/\langle\sigma_C\rangle$, where σ_C is the hyperelliptic involution.

The superspecial isogeny graph

- For each prime p, a directed multigraph $\mathcal{G}_p(\ell)$, where ℓ is a prime different from p, is defined as follows:
- The **vertices** of $\mathcal{G}_p(\ell)$ represent the isomorphism classes of superspecial principally polarized abelian surfaces (s.p.p.a.s) over $\overline{\mathbb{F}}_p$ and the **edges** of the graph are the (ℓ, ℓ)-isogenious up to isomorphism.
- Recall: if (A_1, λ_1) and (A_2, λ_2) are s.p.p.a.s over$\overline{\mathbb{F}}_p$, and if $\phi : A_1 \to A_2$ is an isogeny with $\hat{\phi}\lambda_2\phi = [\ell]\lambda_1$ such that $\operatorname{Ker}\phi \leqslant A_1[\ell]$ is maximally isotropic with respect to the ℓ-Weil pairing, we say ϕ is $(\ell, \ell)-$isogeny.
- Let $\mathit{split}_\ell(J_C)$ be the set of isomorphism classes of **split** (**decomposed**) (ℓ, ℓ)-isogenies from J_C to a superspecial abelian surface with a product principal polarization.
- By Castryck, Decru, Smith (2020), $|\mathit{split}_2(J_C)| \leq 6$.
- Katsura and Takashita (2020) calculate $|\mathit{split}_2(J_C)|$ in each case in terms of $\mathcal{A}ut(C)/\langle\sigma_C\rangle$, where σ_C is the hyperelliptic involution.
- Let us reprove these results in the more general setting by using the theory of the refined Humbert invariant.

Reprove

- Recall that *elliptic subcovers* occur in pairs.

Reprove

- Recall that *elliptic subcovers* occur in pairs.
- If $f : C \to E$ is an *elliptic subcover* of degree ℓ, then there is a "complementary" elliptic subcover $f' : C \to E'$ of degree ℓ.

Reprove

- Recall that *elliptic subcovers* occur in pairs.
- If $f : C \to E$ is an *elliptic subcover* of degree ℓ, then there is a "complementary" elliptic subcover $f' : C \to E'$ of degree ℓ.
- By using f and f', we can create an (ℓ, ℓ)-isogeny

$$\varphi : J_C \to E \times E', \text{ i.e., } \varphi \in \mathit{split}_\ell(J_C).$$

Reprove

- Recall that *elliptic subcovers* occur in pairs.
- If $f : C \to E$ is an *elliptic subcover* of degree ℓ, then there is a "complementary" elliptic subcover $f' : C \to E'$ of degree ℓ.
- By using f and f', we can create an (ℓ, ℓ)-isogeny

$$\varphi : J_C \to E \times E', \text{ i.e., } \varphi \in \mathit{split}_\ell(J_C).$$

- Every split (ℓ, ℓ)-isogeny arises from an elliptic subcover of degree ℓ.

Reprove

- Recall that *elliptic subcovers* occur in pairs.
- If $f : C \to E$ is an *elliptic subcover* of degree ℓ, then there is a "complementary" elliptic subcover $f' : C \to E'$ of degree ℓ.
- By using f and f', we can create an (ℓ, ℓ)-isogeny

$$\varphi : J_C \to E \times E', \text{ i.e., } \varphi \in \mathit{split}_\ell(J_C).$$

- Every split (ℓ, ℓ)-isogeny arises from an elliptic subcover of degree ℓ.
- Observe that the size $|\mathcal{E}_\ell(C)|$ is a double of $|\mathit{split}_\ell(J_C)|$.

Reprove

- Recall that *elliptic subcovers* occur in pairs.
- If $f : C \to E$ is an *elliptic subcover* of degree ℓ, then there is a "complementary" elliptic subcover $f' : C \to E'$ of degree ℓ.
- By using f and f', we can create an (ℓ, ℓ)-isogeny

$$\varphi : J_C \to E \times E', \text{ i.e., } \varphi \in \mathit{split}_\ell(J_C).$$

- Every split (ℓ, ℓ)-isogeny arises from an elliptic subcover of degree ℓ.
- Observe that the size $|\mathcal{E}_\ell(C)|$ is a double of $|\mathit{split}_\ell(J_C)|$.
- Remember: $\mathcal{E}_n(C) \xrightarrow{\sim} R_{n^2}(q_C)$.

Reprove

- Recall that *elliptic subcovers* occur in pairs.
- If $f : C \to E$ is an *elliptic subcover* of degree ℓ, then there is a "complementary" elliptic subcover $f' : C \to E'$ of degree ℓ.
- By using f and f', we can create an (ℓ, ℓ)-isogeny

$$\varphi : J_C \to E \times E', \text{ i.e., } \varphi \in \mathit{split}_\ell(J_C).$$

- Every split (ℓ, ℓ)-isogeny arises from an elliptic subcover of degree ℓ.
- Observe that the size $|\mathcal{E}_\ell(C)|$ is a double of $|\mathit{split}_\ell(J_C)|$.
- Remember: $\mathcal{E}_n(C) \xrightarrow{\sim} R_{n^2}(q_C)$.
- $2|\mathit{split}_\ell(J_C)| = |\mathcal{E}_\ell(C)| = |R_{\ell^2}(q_C)|$

Reprove

- Recall that *elliptic subcovers* occur in pairs.
- If $f : C \to E$ is an *elliptic subcover* of degree ℓ, then there is a "complementary" elliptic subcover $f' : C \to E'$ of degree ℓ.
- By using f and f', we can create an (ℓ, ℓ)-isogeny

$$\varphi : J_C \to E \times E', \text{ i.e., } \varphi \in \mathit{split}_\ell(J_C).$$

- Every split (ℓ, ℓ)-isogeny arises from an elliptic subcover of degree ℓ.
- Observe that the size $|\mathcal{E}_\ell(C)|$ is a double of $|\mathit{split}_\ell(J_C)|$.
- Remember: $\mathcal{E}_n(C) \xrightarrow{\sim} R_{n^2}(q_C)$.
- $2|\mathit{split}_\ell(J_C)| = |\mathcal{E}_\ell(C)| = |R_{\ell^2}(q_C)| \Rightarrow 2|\mathit{split}_\ell(J_C)| = |R_{\ell^2}(q_C)|$.
- In particular, when $\ell = 2$,

$$2|\mathit{split}_2(J_C)| = |R_4(q_C)|$$

Reprove

- Recall that *elliptic subcovers* occur in pairs.
- If $f : C \to E$ is an *elliptic subcover* of degree ℓ, then there is a "complementary" elliptic subcover $f' : C \to E'$ of degree ℓ.
- By using f and f', we can create an (ℓ, ℓ)-isogeny

$$\varphi : J_C \to E \times E', \text{ i.e., } \varphi \in \mathit{split}_\ell(J_C).$$

- Every split (ℓ, ℓ)-isogeny arises from an elliptic subcover of degree ℓ.
- Observe that the size $|\mathcal{E}_\ell(C)|$ is a double of $|\mathit{split}_\ell(J_C)|$.
- Remember: $\mathcal{E}_n(C) \xrightarrow{\sim} R_{n^2}(q_C)$.
- $2|\mathit{split}_\ell(J_C)| = |\mathcal{E}_\ell(C)| = |R_{\ell^2}(q_C)| \Rightarrow 2|\mathit{split}_\ell(J_C)| = |R_{\ell^2}(q_C)|$.
- In particular, when $\ell = 2$,

$$2|\mathit{split}_2(J_C)| = |R_4(q_C)| = |\iota(C)| - 1.$$

Reprove

- Recall that *elliptic subcovers* occur in pairs.
- If $f : C \to E$ is an *elliptic subcover* of degree ℓ, then there is a "complementary" elliptic subcover $f' : C \to E'$ of degree ℓ.
- By using f and f', we can create an (ℓ, ℓ)-isogeny

$$\varphi : J_C \to E \times E', \text{ i.e., } \varphi \in \mathit{split}_\ell(J_C).$$

- Every split (ℓ, ℓ)-isogeny arises from an elliptic subcover of degree ℓ.
- Observe that the size $|\mathcal{E}_\ell(C)|$ is a double of $|\mathit{split}_\ell(J_C)|$.
- Remember: $\mathcal{E}_n(C) \xrightarrow{\sim} R_{n^2}(q_C)$.
- $2|\mathit{split}_\ell(J_C)| = |\mathcal{E}_\ell(C)| = |R_{\ell^2}(q_C)| \Rightarrow 2|\mathit{split}_\ell(J_C)| = |R_{\ell^2}(q_C)|$.
- In particular, when $\ell = 2$,

$$2|\mathit{split}_2(J_C)| = |R_4(q_C)| = |\iota(C)| - 1.$$

- $|\mathit{split}_2(J_C)|$ is equal to the half of the number of elliptic involutions of $\mathcal{A}ut(C)$.

A generalization of the refined Humbert invariant

- Let (A, λ) be a principally polarized abelian surface over any field k.

A generalization of the refined Humbert invariant

- Let (A, λ) be a principally polarized abelian surface over any field k.
- Let $\mathrm{End}_\lambda(A) := \{\alpha \in \mathrm{End}(A) : \lambda^{-1}\hat{\alpha}\lambda = \alpha\}$, and put

A generalization of the refined Humbert invariant

- Let (A, λ) be a principally polarized abelian surface over any field k.
- Let $\mathrm{End}_\lambda(A) := \{\alpha \in \mathrm{End}(A) : \lambda^{-1}\hat{\alpha}\lambda = \alpha\}$, and put $\mathbb{E}_\lambda(A) := \mathrm{End}_\lambda(A)/\mathbb{Z}1_A$.

A generalization of the refined Humbert invariant

- Let (A, λ) be a principally polarized abelian surface over any field k.
- Let $\mathrm{End}_\lambda(A) := \{\alpha \in \mathrm{End}(A) : \lambda^{-1}\hat{\alpha}\lambda = \alpha\}$, and put $\mathbb{E}_\lambda(A) := \mathrm{End}_\lambda(A)/\mathbb{Z}1_A$.

Definition 3.1.

The refined Humbert invariant of a principally polarized abelian surface $(A, \lambda)/k$ is the positive definite quadratic form $q_{(A,\lambda)}$ on $\mathbb{E}_\lambda(A)$ defined by

$$q_{(A,\lambda)}(\alpha) \;=\; \mathrm{Tr}_r(\alpha^2) - \frac{1}{4}\,\mathrm{Tr}_r(\alpha)^2, \quad \text{for} \;\; \alpha \in \mathbb{E}_\lambda(A),$$

where Tr_r is the *rational trace*.

A generalization of the refined Humbert invariant

- Let (A, λ) be a principally polarized abelian surface over any field k.
- Let $\mathrm{End}_\lambda(A) := \{\alpha \in \mathrm{End}(A) : \lambda^{-1}\hat{\alpha}\lambda = \alpha\}$, and put $\mathbb{E}_\lambda(A) := \mathrm{End}_\lambda(A)/\mathbb{Z}1_A$.

Definition 3.1.

The refined Humbert invariant of a principally polarized abelian surface $(A, \lambda)/k$ is the positive definite quadratic form $q_{(A,\lambda)}$ on $\mathbb{E}_\lambda(A)$ defined by

$$q_{(A,\lambda)}(\alpha) \;=\; \mathrm{Tr}_r(\alpha^2) - \frac{1}{4}\,\mathrm{Tr}_r(\alpha)^2, \quad \text{for} \quad \alpha \in \mathbb{E}_\lambda(A),$$

where Tr_r is the *rational trace*.

- This is a generalization of the refined Humbert invariant defined in terms of the intersections numbers.

A generalization of the refined Humbert invariant

- Let (A, λ) be a principally polarized abelian surface over any field k.
- Let $\mathrm{End}_\lambda(A) := \{\alpha \in \mathrm{End}(A) : \lambda^{-1}\hat{\alpha}\lambda = \alpha\}$, and put $\mathbb{E}_\lambda(A) := \mathrm{End}_\lambda(A)/\mathbb{Z}1_A$.

Definition 3.1.

The refined Humbert invariant of a principally polarized abelian surface $(A, \lambda)/k$ is the positive definite quadratic form $q_{(A,\lambda)}$ on $\mathbb{E}_\lambda(A)$ defined by

$$q_{(A,\lambda)}(\alpha) \;=\; \mathrm{Tr}_r(\alpha^2) - \frac{1}{4}\,\mathrm{Tr}_r(\alpha)^2, \quad \text{for} \quad \alpha \in \mathbb{E}_\lambda(A),$$

where Tr_r is the *rational trace*.

- This is a generalization of the refined Humbert invariant defined in terms of the intersections numbers.
- This was suggested by Kani in his article, and I provided a proof in my thesis.

A generalization of the refined Humbert invariant

- Let (A, λ) be a principally polarized abelian surface over any field k.
- Let $\mathrm{End}_\lambda(A) := \{\alpha \in \mathrm{End}(A) : \lambda^{-1}\hat{\alpha}\lambda = \alpha\}$, and put $\mathbb{E}_\lambda(A) := \mathrm{End}_\lambda(A)/\mathbb{Z}1_A$.

Definition 3.1.

The refined Humbert invariant of a principally polarized abelian surface $(A, \lambda)/k$ is the positive definite quadratic form $q_{(A,\lambda)}$ on $\mathbb{E}_\lambda(A)$ defined by

$$q_{(A,\lambda)}(\alpha) \;=\; \mathrm{Tr}_r(\alpha^2) - \frac{1}{4}\,\mathrm{Tr}_r(\alpha)^2, \quad \text{for} \quad \alpha \in \mathbb{E}_\lambda(A),$$

where Tr_r is the *rational trace*.

- This is a generalization of the refined Humbert invariant defined in terms of the intersections numbers.
- This was suggested by Kani in his article, and I provided a proof in my thesis.
- This definition is suitable to generalize the refined Humbert invariant for any principally polarized abelian variety of dimension g over a field k.

Some References

[1] W. Castryck, T. Decru, B. Smith, Hash functions from superspecial genus 2 curves using Richelot isogenies, (2020).

[2] T. Katsura, K. Takashima, Counting Richelot isogenies between superspecial abelian surfaces, (2020).

[3] E. Kani, Elliptic curves on abelian surfaces, (1994).

[4] E. Kani, Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms, (2014).

[5] E. Kani, The moduli spaces of Jacobians isomorphic to a product of two elliptic curves, (2016).

[6] E. Kani, Elliptic subcovers of a curve of genus 2. I. The isogeny defect, (2018).

[7] E. Kani, Elliptic subcovers of a curve of genus 2. II. The refined Humbert invariant, (2018).

[8] E. Kani, Curves of genus 2 on abelian surfaces, (2023).

[9] H. Kir, The classification of the refined Humbert invariant for curves of genus 2, (2022).

[10] H. Kir, The Refined Humbert Invariant for a Given Automorphism Group of a Genus 2 Curve (2023).

THANK YOU

Thank You!