Counting Richelot isogenies between superspecial abelian surfaces

Toshiyuki Katsura [1]   Katsuyuki Takashima [2]

[1]Univ. of Tokyo   [2]Mitsubishi Electric / Kyushu Univ.

ANTS 2020

Outline

Introduction: Genus-2 isogeny cryptography

- Isogenies of supersingular elliptic curves give computationally intractable problems even against quantum computers, and based on them, isogeny-based cryptosystems (CGL, SIDH, SIKE, CSIDH, ...) are now widely studied as one candidate for post-quantum cryptography.

Introduction: Genus-2 isogeny cryptography

- Isogenies of supersingular elliptic curves give computationally intractable problems even against quantum computers, and based on them, isogeny-based cryptosystems (CGL, SIDH, SIKE, CSIDH, ...) are now widely studied as one candidate for post-quantum cryptography.
- Recently, genus-2 isogeny cryptography has been studied by several authors [Tak17, FT19, CDS19, CS20].

Introduction: Genus-2 isogeny cryptography

- Isogenies of supersingular elliptic curves give computationally intractable problems even against quantum computers, and based on them, isogeny-based cryptosystems (CGL, SIDH, SIKE, CSIDH, ...) are now widely studied as one candidate for post-quantum cryptography.
- Recently, genus-2 isogeny cryptography has been studied by several authors [Tak17, FT19, CDS19, CS20].
- Castryck, Decru, and Smith [CDS19] showed that superspecial genus-2 curves and their isogeny graphs give a correct foundation for genus-2 isogeny cryptography.

Introduction: Genus-2 isogeny cryptography

- Isogenies of supersingular elliptic curves give computationally intractable problems even against quantum computers, and based on them, isogeny-based cryptosystems (CGL, SIDH, SIKE, CSIDH, ...) are now widely studied as one candidate for post-quantum cryptography.
- Recently, genus-2 isogeny cryptography has been studied by several authors [Tak17, FT19, CDS19, CS20].
- Castryck, Decru, and Smith [CDS19] showed that superspecial genus-2 curves and their isogeny graphs give a correct foundation for genus-2 isogeny cryptography.
- Costello and Smith [CS20] employed the subgraph whose vertices consist of decomposed principally polarized abelian surfaces in their recent cryptanalysis.

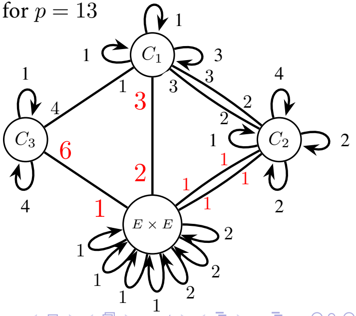
Introduction: Superspecial Richelot isogeny graphs in cryptography

- Castryck et al. [CDS19] also presented concrete algebraic formulas for computing $(2,2)$-isogenies by using the Richelot construction (cf. [Tak17] etc.).

Introduction: Superspecial Richelot isogeny graphs in cryptography

- Castryck et al. [CDS19] also presented concrete algebraic formulas for computing $(2,2)$-isogenies by using the Richelot construction (cf. [Tak17] etc.).
- Richelot isogenies may have decomposed principally polarized abelian surfaces as codomain, and we call them decomposed Richelot isogenies.

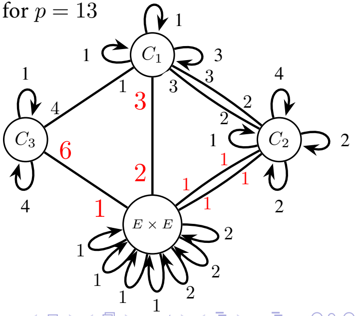
Superspecial Richelot isogeny graph for $p = 13$



Introduction: Superspecial Richelot isogeny graphs in cryptography

- Castryck et al. [CDS19] also presented concrete algebraic formulas for computing $(2, 2)$-isogenies by using the Richelot construction (cf. [Tak17] etc.).
- Richelot isogenies may have decomposed principally polarized abelian surfaces as codomain, and we call them decomposed Richelot isogenies.
- Theorem 3 in [CDS19] states that the number of decomposed Richelot isogenies outgoing from a superspecial genus-2 curve C is at most 6, but they do not precisely determine this number. Moreover, their proof is computer-aided.

Superspecial Richelot isogeny graph for $p = 13$

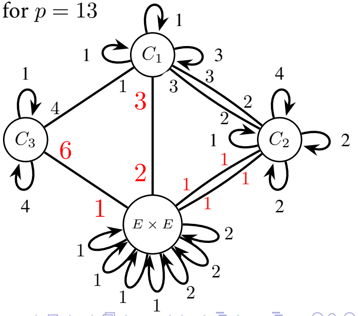


Introduction: Superspecial Richelot isogeny graphs in cryptography

- Castryck et al. [CDS19] also presented concrete algebraic formulas for computing $(2,2)$-isogenies by using the Richelot construction (cf. [Tak17] etc.).
- Richelot isogenies may have decomposed principally polarized abelian surfaces as codomain, and we call them decomposed Richelot isogenies.

- Theorem 3 in [CDS19] states that the number of decomposed Richelot isogenies outgoing from a superspecial genus-2 curve C is at most 6, but they do not precisely determine this number. Moreover, their proof is computer-aided.
- Therefore, we revisit the isogeny counting problem based on an intrinsic algebraic geometric characterization.

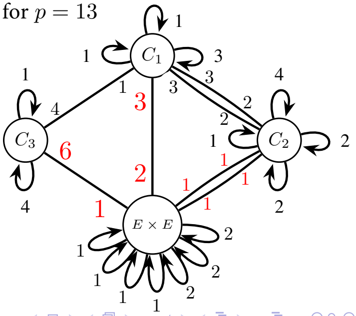
Superspecial Richelot isogeny graph for $p = 13$



Introduction: Superspecial Richelot isogeny graphs in cryptography

- Castryck et al. [CDS19] also presented concrete algebraic formulas for computing $(2, 2)$-isogenies by using the Richelot construction (cf. [Tak17] etc.).
- Richelot isogenies may have decomposed principally polarized abelian surfaces as codomain, and we call them decomposed Richelot isogenies.
- Theorem 3 in [CDS19] states that the number of decomposed Richelot isogenies outgoing from a superspecial genus-2 curve C is at most 6, but they do not precisely determine this number. Moreover, their proof is computer-aided.
- Therefore, we revisit the isogeny counting problem based on an intrinsic algebraic geometric characterization.
- Our starting point is an explicit counting of superspecial genus-2 curves by Ibukiyama, Katsura, and Oort [IKO86].

Superspecial Richelot isogeny graph for $p = 13$



Our results

1. We give a new characterization of decomposed Richelot isogenies outgoing from a nonsingular genus-2 curve C in terms of “long” elements (of order 2) in the reduced group of automorphisms $\mathrm{RA}(C)$.

Our results

1. We give a new characterization of decomposed Richelot isogenies outgoing from a nonsingular genus-2 curve C in terms of “long” elements (of order 2) in the reduced group of automorphisms $\mathrm{RA}(C)$.
2. Based on the characterization, we give a precise count of (decomposed) Richelot isogenies up to isomorphism for each reduced group $\mathrm{RA}(C)$.
   - It not only implies another algebraic geometric proof of Theorem 3 in [CDS19], but also shows the number of decomposed Richelot isogenies up to isomorphism is at most 2.

Our results

1. We give a new characterization of decomposed Richelot isogenies outgoing from a nonsingular genus-2 curve C in terms of "long" elements (of order 2) in the reduced group of automorphisms $\mathrm{RA}(C)$.
2. Based on the characterization, we give a precise count of (decomposed) Richelot isogenies up to isomorphism for each reduced group $\mathrm{RA}(C)$.
   - It not only implies another algebraic geometric proof of Theorem 3 in [CDS19], but also shows the number of decomposed Richelot isogenies up to isomorphism is at most 2.
3. We also count the total number of Richelot isogenies up to isomorphism between principally polarized superspecial abelian surfaces.
   - While [IKO86] counts the total number of vertices of the superspecial Richelot isogeny graphs, the above result is related to the edge counting in the graphs of cryptographic interest (see [JZ20] for their connectivity).

Superspecial abelian surfaces

- Let k be an algebraically closed field of characteristic $p > 5$.
  An abelian surface A defined over k is said to be superspecial if A is isomorphic to $E_1 \times E_2$ with E_i supersingular elliptic curves $(i = 1, 2)$.

Superspecial abelian surfaces

- Let k be an algebraically closed field of characteristic $p > 5$.
  An abelian surface A defined over k is said to be superspecial if A is isomorphic to $E_1 \times E_2$ with E_i supersingular elliptic curves $(i = 1, 2)$.
- Since we have an isomorphism $E_1 \times E_2 \cong E_3 \times E_4$ for any supersingular elliptic curves E_i $(i = 1, 2, 3, 4)$ (cf. [Shi79]), this notion does not depend on the choice of supersingular elliptic curves.

Superspecial abelian surfaces

- Let k be an algebraically closed field of characteristic $p > 5$.
  An abelian surface A defined over k is said to be superspecial if A is isomorphic to $E_1 \times E_2$ with E_i supersingular elliptic curves $(i = 1, 2)$.
- Since we have an isomorphism $E_1 \times E_2 \cong E_3 \times E_4$ for any supersingular elliptic curves E_i $(i = 1, 2, 3, 4)$ (cf. [Shi79]), this notion does not depend on the choice of supersingular elliptic curves.
- For a nonsingular projective curve C of genus 2 over k, we denote by $J(C)$ the (canonically polarized) Jacobian variety of C.
  The curve C is said to be superspecial if the Jacobian variety $J(C)$ is superspecial as an abelian surface (without polarization).

Reduced groups of automorphisms

- Let $\iota \in \mathrm{Aut}(C)$ be the hyperelliptic involution. We put $\mathrm{RA}(C) = \mathrm{Aut}(C)/\langle\iota\rangle$ and we call it the reduced group of automorphisms of C and an element of $\mathrm{RA}(C)$ a reduced automorphism of C, respectively.
- For $\sigma \in \mathrm{RA}(C)$, $\tilde{\sigma}$ is an element of $\mathrm{Aut}(C)$ such that $\tilde{\sigma} \bmod \langle\iota\rangle = \sigma$.

Reduced groups of automorphisms

- Let $\iota \in \mathrm{Aut}(C)$ be the hyperelliptic involution. We put $\mathrm{RA}(C) = \mathrm{Aut}(C)/\langle\iota\rangle$ and we call it the reduced group of automorphisms of C and an element of $\mathrm{RA}(C)$ a reduced automorphism of C, respectively.
- For $\sigma \in \mathrm{RA}(C)$, $\tilde{\sigma}$ is an element of $\mathrm{Aut}(C)$ such that $\tilde{\sigma} \bmod \langle\iota\rangle = \sigma$.

Definition (Long and short elements, cf. Katsura–Oort [KO87])

An element $\sigma \in \mathrm{RA}(C)$ of order 2 is said to be long if $\tilde{\sigma}$ is of order 2. Otherwise, it is said to be short.

This definition does not depend on the choice of $\tilde{\sigma}$.

Reduced groups of automorphisms

- Let $\iota \in \mathrm{Aut}(C)$ be the hyperelliptic involution. We put $\mathrm{RA}(C) = \mathrm{Aut}(C)/\langle\iota\rangle$ and we call it the reduced group of automorphisms of C and an element of $\mathrm{RA}(C)$ a reduced automorphism of C, respectively.
- For $\sigma \in \mathrm{RA}(C)$, $\tilde{\sigma}$ is an element of $\mathrm{Aut}(C)$ such that $\tilde{\sigma} \bmod \langle\iota\rangle = \sigma$.

Definition (Long and short elements, cf. Katsura–Oort [KO87])

An element $\sigma \in \mathrm{RA}(C)$ of order 2 is said to be long if $\tilde{\sigma}$ is of order 2.
Otherwise, it is said to be short.

This definition does not depend on the choice of $\tilde{\sigma}$.

- The structure of $\mathrm{RA}(C)$ is classified as follows:

$$(0)\ 0,\quad (1)\ \mathbf{Z}/2\mathbf{Z},\quad (2)\ S_3,\quad (3)\ \mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z},\quad (4)\ D_{12},\quad (5)\ S_4,\quad (6)\ \mathbf{Z}/5\mathbf{Z}.$$

Counting superspecial curves of genus 2 [IKO86]

We denote by n_i the number of superspecial curves C of genus 2 whose $\mathrm{RA}(C)$ is isomorphic to the group (i), and n the total number of such curves.

(0) $n_0 = (p-1)(p^2-35p+346)/2880 - \{1-(\frac{-1}{p})\}/32 - \{1-(\frac{-2}{p})\}/8 - \{1-(\frac{-3}{p})\}/9 + \begin{cases} 0 & \text{if } p \equiv 1, 2 \text{ or } 3 \pmod 5, \\ -1/5 & \text{if } p \equiv 4 \pmod 5, \end{cases}$

(1) $n_1 = (p-1)(p-17)/48 + \{1-(\frac{-1}{p})\}/8 + \{1-(\frac{-2}{p})\}/2 + \{1-(\frac{-3}{p})\}/2,$

(2) $n_2 = (p-1)/6 - \{1-(\frac{-2}{p})\}/2 - \{1-(\frac{-3}{p})\}/3,$

(3) $n_3 = (p-1)/8 - \{1-(\frac{-1}{p})\}/8 - \{1-(\frac{-2}{p})\}/4 - \{1-(\frac{-3}{p})\}/2,$

(4) $n_4 = \{1-(\frac{-3}{p})\}/2,$ (5) $n_5 = \{1-(\frac{-2}{p})\}/2,$ (6) $n_6 = \begin{cases} 0 & \text{if } p \equiv 1, 2 \text{ or } 3 \pmod 5, \\ 1 & \text{if } p \equiv 4 \pmod 5. \end{cases}$

- $n = n_0 + n_1 + n_2 + n_3 + n_4 + n_5 + n_6$
  $= (p-1)(p^2+25p+166)/2880 - \{1-(\frac{-1}{p})\}/32 + \{1-(\frac{-2}{p})\}/8 + \{1-(\frac{-3}{p})\}/18 + \begin{cases} 0 & \text{if } p \equiv 1, 2 \text{ or } 3 \pmod 5, \\ 4/5 & \text{if } p \equiv 4 \pmod 5. \end{cases}$

Richelot isogenies

- Let A be an abelian surface with a principal polarization C. There are two cases for such (A, C) (shown by A. Weil).
  1. There exists a nonsingular curve C of genus 2 in A s.t. $A \cong J(C)$ and C is the divisor with self-intersection $C^2 = 2$. In this case, $(J(C), C)$ is said to be non-decomposed.
  2. There exist two elliptic curves E_1, E_2 in A with $(E_1 \cdot E_2) = 1$ s.t. $A \cong E_1 \times E_2$ and $C = E_1 \times \{0\} + \{0\} \times E_2$ is a divisor with self-intersection 2. In this case, (A, C) is said to be decomposed. We denote by $E_1 + E_2$ the divisor $E_1 \times \{0\} + \{0\} \times E_2$.

Richelot isogenies

- Let A be an abelian surface with a principal polarization C. There are two cases for such (A, C) (shown by A. Weil).
  1. There exists a nonsingular curve C of genus 2 in A s.t. $A \cong J(C)$ and C is the divisor with self-intersection $C^2 = 2$. In this case, $(J(C), C)$ is said to be non-decomposed.
  2. There exist two elliptic curves E_1, E_2 in A with $(E_1 \cdot E_2) = 1$ s.t. $A \cong E_1 \times E_2$ and $C = E_1 \times \{0\} + \{0\} \times E_2$ is a divisor with self-intersection 2. In this case, (A, C) is said to be decomposed. We denote by $E_1 + E_2$ the divisor $E_1 \times \{0\} + \{0\} \times E_2$.
- Let $G \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ be a maximal isotropic subgroup of $A[2]$ with respect to the Weil pairing. We have a quotient homomorphism $\pi : A \longrightarrow A/G$.
- By the standard descent theorem, there exists a divisor C' on A/G s.t. $2C \sim \pi^* C'$. We see that C' is a principal polarization on A/G and that C' is either a nonsingular curve of genus 2 or $E_1' + E_2'$ with elliptic curves E_1', E_2' and $(E_1' \cdot E_2') = 1$.

• $D \sim D'$ means linear equivalence for divisors D and D'.

Richelot isogenies

Definition (Richelot isogenies)

The correspondence from (A, C) to $(A/G, C')$ is called a Richelot isogeny. It is called decomposed if C' consists of two elliptic curves. Otherwise, it is called non-decomposed.

Richelot isogenies

Definition (Richelot isogenies)

The correspondence from (A, C) to $(A/G, C')$ is called a Richelot isogeny. It is called decomposed if C' consists of two elliptic curves. Otherwise, it is called non-decomposed.

- If there exists a Richelot isogeny from (A, C) to $(A/G, C')$, then there exists a Richelot isogeny from $(A/G, C')$ to (A, C).
- Since π is separable, when A is superspecial, A/G is also superspecial.

Richelot isogenies

Definition (Richelot isogenies)

The correspondence from (A, C) to $(A/G, C')$ is called a Richelot isogeny. It is called decomposed if C' consists of two elliptic curves. Otherwise, it is called non-decomposed.

- If there exists a Richelot isogeny from (A, C) to $(A/G, C')$, then there exists a Richelot isogeny from $(A/G, C')$ to (A, C).
- Since π is separable, when A is superspecial, A/G is also superspecial.

Definition (Isomorphism of Richelot isogenies)

Let (A, C), (A', C') and (A'', C'') be principally polarized abelian surfaces. The Richelot isogeny $\pi : A \longrightarrow A'$ is said to be isomorphic to the Richelot isogeny $\varpi : A \longrightarrow A''$ if there exist an automorphism $\sigma \in \mathrm{Aut}(A)$ with $\sigma^* C \approx C$ and an isomorphism $g : A' \longrightarrow A''$ with $g^* C'' \approx C'$ s.t. the right diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & A \\ \pi \downarrow & & \downarrow \varpi \\ A' & \xrightarrow{g} & A'' \end{array}$$

• $D \approx D'$ means numerical equivalence for divisors D and D'.

Characterization of decomposed Richelot isog. by long elements

Proposition (Characterization of decomposed Richelot isog. by long elements)

For a nonsingular projective curve C of genus 2, the following 3 conditions are equivalent.

1. *C has a decomposed Richelot isogeny outgoing from $J(C)$.*
2. *$\mathrm{RA}(C)$ has an element of order 2.*
3. *$\mathrm{RA}(C)$ has a long element of order 2.*

Characterization of decomposed Richelot isog. by long elements

Proposition (Characterization of decomposed Richelot isog. by long elements)

For a nonsingular projective curve C of genus 2, the following 3 conditions are equivalent.

1. *C has a decomposed Richelot isogeny outgoing from $J(C)$.*
2. *$\mathrm{RA}(C)$ has an element of order 2.*
3. *$\mathrm{RA}(C)$ has a long element of order 2.*

Proposition

Let C be a nonsingular projective superspecial curve of genus 2. Among 15 Richelot isogenies outgoing from $J(C)$, the number of decomposed Richelot isogenies is equal to the number of long elements of $\mathrm{RA}(C)$ of order 2.

We denote the set of long elements in $\mathrm{RA}(C)$ by $\mathrm{L(C)}$.

Classification of long elements $\mathrm{L}(C)$ for each $\mathrm{RA}(C)$

- Long elements $f \in \mathrm{L}(C)$ ($\subset \mathrm{RA}(C)$) are given by the action $f : x \mapsto f(x)$ on x-coord.
- This result $\#\mathrm{L}(C) \leq 6$ coincides with Theorem 3 in [CDS19].

$\mathrm{RA}(C)$	genus-2 curve C	$\#\mathrm{L}(C)$	$f(x)$
0	—	0	—
$\mathbf{Z}/2\mathbf{Z}$	$y^2 = (x^2-1)(x^2-a^2)(x^2-b^2)$	1	$f(x) = -x$
S_3	$y^2 = (x^3-1)(x^3-a^3)$	3	$f(x) = \frac{a}{x}, \frac{\omega a}{x}, \frac{\omega^2 a}{x}$
$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$	$y^2 = x(x^2-1)(x^2-a^2)$	2	$f(x) = \frac{a}{x}, \frac{-a}{x}$
D_{12}	$y^2 = x^6 - 1$	4	$f(x) = -x, \frac{\zeta}{x}, \frac{\zeta^3}{x}, \frac{\zeta^5}{x}$
S_4	$y^2 = x(x^4-1)$	6	$f(x) = \frac{x+1}{x-1}, -\frac{x-1}{x+1}, \frac{i(x+i)}{x-i}, \frac{i}{x}, -\frac{i}{x}, -\frac{i(x-i)}{x+i}$
$\mathbf{Z}/5\mathbf{Z}$	$y^2 = x^5 - 1$	0	—

Here, we denote by ω, i, ζ a primitive cube, fourth, sixth root of unity, respectively.

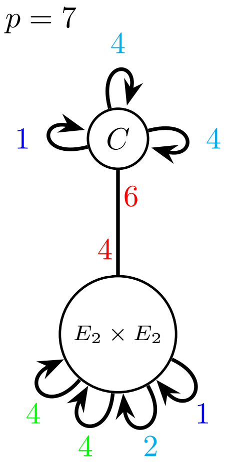
Counting Richelot isogenies up to isomorphism in characteristic 7

Two different Richelot isogenies may be isomorphic to each other by an automorphism.

Counting Richelot isogenies up to isomorphism in characteristic 7

Two different Richelot isogenies may be isomorphic to each other by an automorphism.

- Assume the characteristic $p = 7$.
  - only one supersingular $E_2 : y^2 = x^3 - x \quad (\mathrm{RA}(E_2) \cong \mathbf{Z}/2\mathbf{Z})$,
  - only one superspecial $C : y^2 = x(x^4 - 1) \quad (\mathrm{RA}(C) \cong S_4)$.

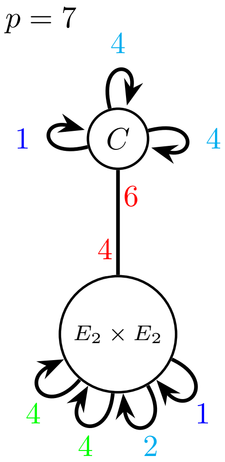


Counting Richelot isogenies up to isomorphism in characteristic 7

Two different Richelot isogenies may be isomorphic to each other by an automorphism.

- Assume the characteristic $p = 7$.
  - only one supersingular $E_2 : y^2 = x^3 - x \quad (\mathrm{RA}(E_2) \cong \mathbf{Z}/2\mathbf{Z})$,
  - only one superspecial $C : y^2 = x(x^4 - 1) \quad (\mathrm{RA}(C) \cong S_4)$.
- The number of Richelot isogenies up to isomorphism outgoing from C: 4 Richelot isogenies, 1 decomposed one, local type: $(1 \times 1, 4 \times 2)(6 \times 1)$.
- $(1 \times 1, 4 \times 2)(6 \times 1)$ means that there exist for non-decomposed Richelot isogenies,
  - 1 orbit which contains 1 element
  - 2 orbits which contain 4 elements and

  for decomposed Richelot isogenies,
  - 1 orbit which contains 6 elements.



Counting Richelot isogenies from irreducible genus-2 curves

Proposition

The number of Richelot isogenies up to isomorphism in each case and the number of elements in each orbit are listed as follows.

Counting Richelot isogenies from irreducible genus-2 curves

Proposition

The number of Richelot isogenies up to isomorphism in each case and the number of elements in each orbit are listed as follows.

(0) $\mathrm{RA}(C) \cong \{0\} : 15$ *Richelot isogenies. No decomposed one.* $(1 \times 15)(0)$.

(1) $\mathbf{Z}/2\mathbf{Z} : 11$ *Richelot isogenies.* 1 *decomposed one.* $(1 \times 6, 2 \times 4)(1 \times 1)$.

(2) $S_3 : 7$ *Richelot isogenies.* 1 *decomposed one.* $(1 \times 3, 3 \times 3)(3 \times 1)$.

(3) $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} : 8$ *Richelot isogenies.* 2 *decomposed ones.* $(1 \times 1, 2 \times 4, 4 \times 1)(1 \times 2)$.

(4) $D_{12} : 5$ *Richelot isogenies.* 2 *decomposed ones.* $(2 \times 1, 3 \times 1, 6 \times 1)(1 \times 1, 3 \times 1)$.

(5) $S_4 : 4$ *Richelot isogenies.* 1 *decomposed one.* $(1 \times 1, 4 \times 2)(6 \times 1)$.

(6) $\mathbf{Z}/5\mathbf{Z} : 3$ *Richelot isogenies. No decomposed one.* $(5 \times 3)(0)$.

The total number of Richelot isog. from irreducible genus-2 curves

Let $N_{\mathrm{nd}\to\mathrm{d}}$ (resp. $N_{\mathrm{nd}\to\mathrm{nd}}$) be the total number of decomposed (resp. non-decomposed) Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus 2, and $N_{\mathrm{nd}} = N_{\mathrm{nd}\to\mathrm{d}} + N_{\mathrm{nd}\to\mathrm{nd}}$ the total number of such Richelot isog. up to isom.

Theorem (The total number of Richelot isogenies from $J(C)$)

$$\begin{aligned} N_{\mathrm{nd}} &= 15n_0 + 11n_1 + 7n_2 + 8n_3 + 5n_4 + 4n_5 + 3n_6 \\ &= \frac{(p-1)(p+2)(p+7)}{192} - 3\{1 - (\frac{-1}{p})\}/32 + \{1 - (\frac{-2}{p})\}/8, \\ N_{\mathrm{nd}\to\mathrm{d}} &= n_1 + n_2 + 2n_3 + 2n_4 + n_5 \\ &= \frac{(p-1)(p+3)}{48} - \{1 - (\frac{-1}{p})\}/8 + \{1 - (\frac{-3}{p})\}/6. \end{aligned}$$

The total number of Richelot isog. from irreducible genus-2 curves

Let $N_{\mathrm{nd}\to\mathrm{d}}$ (resp. $N_{\mathrm{nd}\to\mathrm{nd}}$) be the total number of decomposed (resp. non-decomposed) Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus 2, and $N_{\mathrm{nd}} = N_{\mathrm{nd}\to\mathrm{d}} + N_{\mathrm{nd}\to\mathrm{nd}}$ the total number of such Richelot isog. up to isom.

Theorem (The total number of Richelot isogenies from $J(C)$)

$$
\begin{aligned}
N_{\mathrm{nd}} &= 15n_0 + 11n_1 + 7n_2 + 8n_3 + 5n_4 + 4n_5 + 3n_6 \\
&= \frac{(p-1)(p+2)(p+7)}{192} - 3\{1 - (\frac{-1}{p})\}/32 + \{1 - (\frac{-2}{p})\}/8, \\
N_{\mathrm{nd}\to\mathrm{d}} &= n_1 + n_2 + 2n_3 + 2n_4 + n_5 \\
&= \frac{(p-1)(p+3)}{48} - \{1 - (\frac{-1}{p})\}/8 + \{1 - (\frac{-3}{p})\}/6.
\end{aligned}
$$

We also give the number of Richelot isogenies up to isomorphism outgoing from a decomposed pp superspecial abelian surface, the number of elements in each orbit, and the total number of such Richelot isog. up to isom.

Concluding remark

- Our results clarified a concrete situation on decomposed Richelot isogenies, and it gave a firm understanding of the isogeny graphs in genus-2 isogeny cryptography. Further application of our results to cryptography is left as an open problem.

Concluding remark

- Our results clarified a concrete situation on decomposed Richelot isogenies, and it gave a firm understanding of the isogeny graphs in genus-2 isogeny cryptography. Further application of our results to cryptography is left as an open problem.
- For example, a very recent cryptanalytic algorithm by Costello and Smith [CS20] is an interesting target. They proposed a new isogeny path-finding algorithm in the superspecial Richelot isogeny graphs.

  We hope that our new characterization can be applied to analysing and/or improving the Costello–Smith attack.

Concluding remark

- Our results clarified a concrete situation on decomposed Richelot isogenies, and it gave a firm understanding of the isogeny graphs in genus-2 isogeny cryptography. Further application of our results to cryptography is left as an open problem.
- For example, a very recent cryptanalytic algorithm by Costello and Smith [CS20] is an interesting target. They proposed a new isogeny path-finding algorithm in the superspecial Richelot isogeny graphs.

  We hope that our new characterization can be applied to analysing and/or improving the Costello–Smith attack.

Thank you for your attention !

References I

[CDS19] Wouter Castryck, Thomas Decru, and Benjamin Smith.
Hash functions from superspecial genus-2 curves using Richelot isogenies.
In *NutMiC 2019: Number-Theoretic Methods in Cryptology*, 2019.
To appear in J. of Math. Crypt.

[CS20] Craig Costello and Benjamin Smith.
The supersingular isogeny problem in genus 2 and beyond.
In *PQCrypto 2020*, pages 151–168, 2020.

[FT19] E. Victor Flynn and Yan Bo Ti.
Genus two isogeny cryptography.
In *PQCrypto 2019*, pages 286–306, 2019.

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

References II

[JZ20] Bruce W. Jordan and Yevgeny Zaytman.
Isogeny graphs of superspecial abelian varieties and generalized Brandt matrices.
ArXiv, abs/2005.09031, 2020.

[KO87] Toshiyuki Katsura and Frans Oort.
Families of supersingular abelian surfaces.
Compositio Math., 62:107–167, 1987.

[Shi79] Tetsuji Shioda.
Supersingular K3 surfaces.
In *Algebraic Geometry, Proc. Copenhagen 1978 (K. Lϕnsted, ed.)*, Lecture Notes in Math. 732, pages 563–591. Springer Verlag, 1979.

[Tak17] Katsuyuki Takashima.
Efficient algorithms for isogeny sequences and their cryptographic applications.
In *Mathematical Modelling for Next-Generation Cryptography: CREST Crypto-Math Project*, pages 97–114. Springer Verlag, 2017.

Appendices

Counting Richelot isogenies from products of elliptic curves

Let $E_2 : y^2 = x^3 - x \ (p \equiv 3 \pmod 4)$, $E_3 : y^2 = x^3 - 1 \ (p \equiv 2 \pmod 3)$ and E, E' be two non-isomorphic supersingular elliptic curves which are neither isomorphic to E_2 nor to E_3.

Counting Richelot isogenies from products of elliptic curves

Let $E_2 : y^2 = x^3 - x \ (p \equiv 3 \pmod 4)$, $E_3 : y^2 = x^3 - 1 \ (p \equiv 2 \pmod 3)$ and E, E' be two non-isomorphic supersingular elliptic curves which are neither isomorphic to E_2 nor to E_3.

Proposition

The number of Richelot isog. up to isom. outgoing from a decomposed pp superspecial abelian surface and the number of elements in each orbit are listed as follows.

Counting Richelot isogenies from products of elliptic curves

Let $E_2 : y^2 = x^3 - x$ ($p \equiv 3 \pmod 4$), $E_3 : y^2 = x^3 - 1$ ($p \equiv 2 \pmod 3$) and E, E' be two non-isomorphic supersingular elliptic curves which are neither isomorphic to E_2 nor to E_3.

Proposition

The number of Richelot isog. up to isom. outgoing from a decomposed pp superspecial abelian surface and the number of elements in each orbit are listed as follows.

(i) $E \times E' : 15$ *Richelot isogenies,* 6 *non-decomposed ones.* $(1 \times 6)(1 \times 9)$.

(ii) $E \times E : 11$ *Richelot isogenies,* 4 *non-decomposed ones.* $(1 \times 3, 2 \times 1)(1 \times 4, 2 \times 3)$.

(iii) $E \times E_2 : 9$ *Richelot isog.,* 3 *non-decomp. ones* ($p \equiv 3 \pmod 4$). $(2 \times 3)(1 \times 3, 2 \times 3)$.

(iv) $E \times E_3 : 5$ *Richelot isog.,* 2 *non-decomp. ones* ($p \equiv 2 \pmod 3$). $(3 \times 2)(3 \times 3)$.

(v) $E_2 \times E_2 : 5$ *Richelot isog.,* 1 *non-decomp. one* ($p \equiv 3\ (4)$). $(4 \times 1)(1 \times 1, 2 \times 1, 4 \times 2)$.

(vi) $E_3 \times E_3 : 3$ *Richelot isog.,* 1 *non-decomp. one* ($p \equiv 2 \pmod 3$). $(3 \times 1)(3 \times 1, 9 \times 1)$.

(vii) $E_2 \times E_3 : 3$ *Richelot isog.,* 1 *non-decomp. one* ($p \equiv 11\ (12)$). $(6 \times 1)(3 \times 1, 6 \times 1)$.

The total number of Richelot isog. from products of elliptic curves

Theorem (The total number of Richelot isogenies from elliptic curve products)

The total number of *non-decomposed* *Richelot isogenies* $N_{\mathrm{d}\to\mathrm{nd}}$ *(resp. decomposed Richelot isogenies* $N_{\mathrm{d}\to\mathrm{d}}$*) up to isomorphism* *outgoing from decomposed principally polorized superspecial abelian surfaces* *is equal to*

$$\begin{aligned} N_{\mathrm{d}\to\mathrm{nd}} &= \frac{(p-1)(p+3)}{48} - \{1 - (\frac{-1}{p})\}/8 + \{1 - (\frac{-3}{p})\}/6, \\ N_{\mathrm{d}\to\mathrm{d}} &= \frac{(p-1)(3p+17)}{96} + (p+6)\{1 - (\frac{-1}{p})\}/16 + \{1 - (\frac{-3}{p})\}/3. \end{aligned}$$

The total number of Richelot isog. from products of elliptic curves

Theorem (The total number of Richelot isogenies from elliptic curve products)

The total number of non-decomposed *Richelot isogenies* $N_{\mathrm{d}\to\mathrm{nd}}$ *(resp. decomposed Richelot isogenies* $N_{\mathrm{d}\to\mathrm{d}}$*) up to isomorphism* *outgoing from decomposed principally polorized superspecial abelian surfaces* *is equal to*

$$N_{\mathrm{d}\to\mathrm{nd}} = \frac{(p-1)(p+3)}{48} - \{1-(\frac{-1}{p})\}/8 + \{1-(\frac{-3}{p})\}/6,$$
$$N_{\mathrm{d}\to\mathrm{d}} = \frac{(p-1)(3p+17)}{96} + (p+6)\{1-(\frac{-1}{p})\}/16 + \{1-(\frac{-3}{p})\}/3.$$

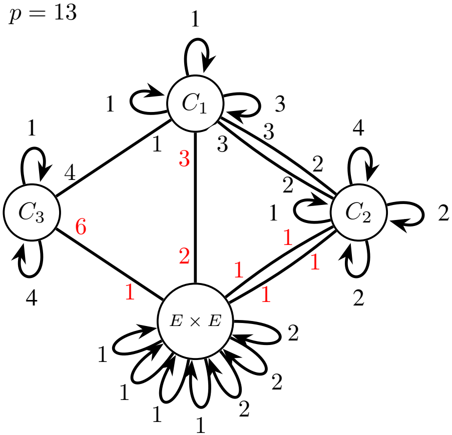
Remark

The number of decomposed Richelot isogenies $N_{\mathrm{nd}\to\mathrm{d}}$ from irreducible curves
= the number of non-decomposed Richelot isogenies $N_{\mathrm{d}\to\mathrm{nd}}$ from elliptic curve products

Example in characteristic 13

Assume the characteristic $p = 13$.

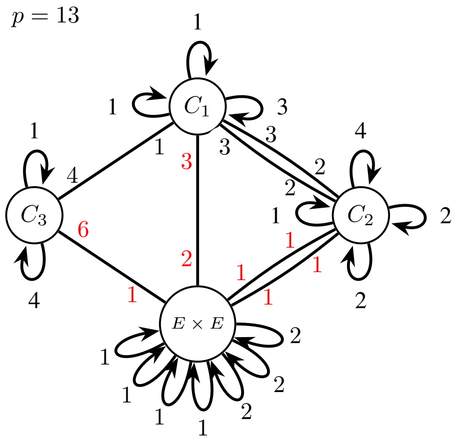
- C_1: $y^2 = (x^3 - 1)(x^3 + 4 - \sqrt{2})$ $(\mathrm{RA}(C_1) \cong S_3)$, type of R. isog. outgoing from C_1 : $(1 \times 3, 3 \times 3)(3 \times 1)$.



Example in characteristic 13

Assume the characteristic $p = 13$.

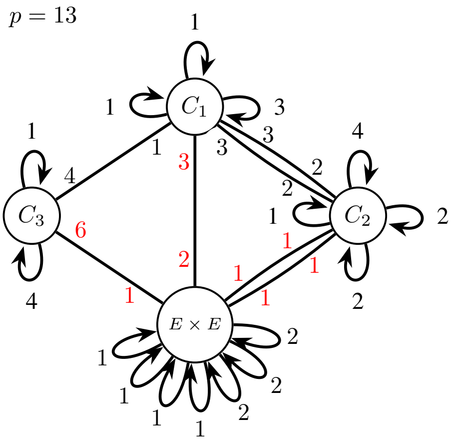
- C_1: $y^2 = (x^3 - 1)(x^3 + 4 - \sqrt{2})$ $(\mathrm{RA}(C_1) \cong S_3)$,
  type of R. isog. outgoing from C_1 :
  $(1 \times 3, 3 \times 3)(3 \times 1)$.
- C_2: $y^2 = x(x^2 - 1)(x^2 + 5 + 2\sqrt{6})$
  $(\mathrm{RA}(C_2) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})$,
  type of R. isog. outgoing from C_2 :
  $(1 \times 1, 2 \times 4, 4 \times 1)(1 \times 2)$.
- C_3: $y^2 = x(x^4 - 1)$ $(\mathrm{RA}(C_3) \cong S_4)$,
  $(1 \times 1, 4 \times 2)(6 \times 1)$.



Example in characteristic 13

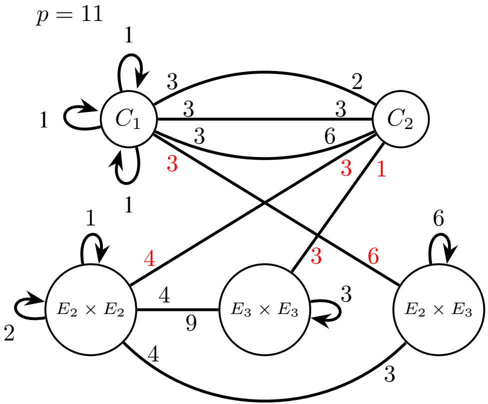
Assume the characteristic $p = 13$.

- C_1: $y^2 = (x^3 - 1)(x^3 + 4 - \sqrt{2})$ $(\mathrm{RA}(C_1) \cong S_3)$,
  type of R. isog. outgoing from C_1 :
  $(1 \times 3, 3 \times 3)(3 \times 1)$.
- C_2: $y^2 = x(x^2 - 1)(x^2 + 5 + 2\sqrt{6})$
  $(\mathrm{RA}(C_2) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})$,
  type of R. isog. outgoing from C_2 :
  $(1 \times 1, 2 \times 4, 4 \times 1)(1 \times 2)$.
- C_3: $y^2 = x(x^4 - 1)$ $\quad (\mathrm{RA}(C_3) \cong S_4)$,
  $(1 \times 1, 4 \times 2)(6 \times 1)$.
- E: $y^2 = x(x - 1)(x - 3 + 2\sqrt{2})$ $(\mathrm{RA}(E) \cong \{0\})$,
  type of R. isog. outgoing from $E \times E$:
  $(1 \times 3, 2 \times 1)(1 \times 4, 2 \times 3)$.



Example in characteristic 11

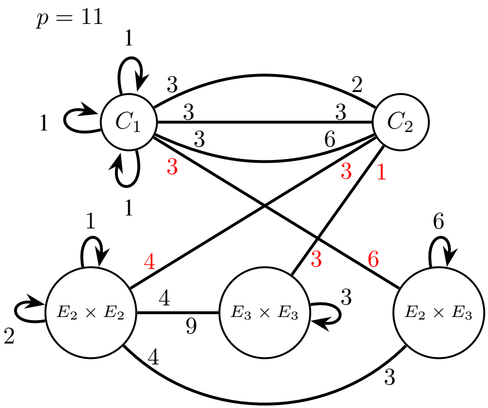
- C_1: $y^2 = (x^3-1)(x^3-3)$ $(\mathrm{RA}(C_1) \cong S_3)$, type of R. isog. outgoing from C_1 : $(1\times 3, 3\times 3)(3\times 1)$.
- C_2: $y^2 = x^6 - 1$ $\quad(\mathrm{RA}(C_2) \cong D_{12})$, type of R. isog. outgoing from C_2 : $(2\times 1, 3\times 1, 6\times 1)(1\times 1, 3\times 1)$.



Example in characteristic 11

- C_1: $y^2 = (x^3-1)(x^3-3)$ $(\mathrm{RA}(C_1) \cong S_3)$, type of R. isog. outgoing from C_1 : $(1\times 3, 3\times 3)(3\times 1)$.
- C_2: $y^2 = x^6 - 1$ $\quad(\mathrm{RA}(C_2) \cong D_{12})$, type of R. isog. outgoing from C_2 : $(2\times 1, 3\times 1, 6\times 1)(1\times 1, 3\times 1)$.

E_2: $y^2 = x^3 - x$ and E_3: $y^2 = x^3 - 1$.



Example in characteristic 11

- C_1: $y^2 = (x^3-1)(x^3-3)$ $(\mathrm{RA}(C_1) \cong S_3)$,
  type of R. isog. outgoing from C_1 :
  $(1\times 3, 3\times 3)(3\times 1)$.
- C_2: $y^2 = x^6 - 1$ $\quad (\mathrm{RA}(C_2) \cong D_{12})$,
  type of R. isog. outgoing from C_2 :
  $(2\times 1, 3\times 1, 6\times 1)(1\times 1, 3\times 1)$.

E_2: $y^2 = x^3 - x$ and E_3: $y^2 = x^3 - 1$.

- type of R. isog. outgoing from $E_2 \times E_2$:
  $(4\times 1)(1\times 1, 2\times 1, 4\times 2)$.
- type of R. isog. outgoing from $E_3 \times E_3$:
  $(3\times 1)(3\times 1, 6\times 1)$.
- type of R. isog. outgoing from $E_2 \times E_3$:
  $(6\times 1)(3\times 1, 6\times 1)$.