COUNTING SUPERSPECIAL RICHELOT ISOGENIES AND ITS CRYPTOGRAPHIC APPLICATION

TOSHIYUKI KATSURA AND KATSUYUKI TAKASHIMA

ABSTRACT. We give a characterization of decomposed Richelot isogenies in terms of involutive reduced automorphisms of genus-2 curves over a finite field, and explicitly count such decomposed (and non-decomposed) superspecial Richelot isogenies. The characterization implies that the decomposed principally polarized superspecial abelian surfaces are adjacent to 1-small curves in the superspecial Richelot isogeny graph, where the smallness is defined as in a similar manner to Love–Boneh’s one. We then obtain an improved isogeny path-finding algorithm in genus 2 as an application by using $M$-small genus-2 curves for some threshold $M$.

1. INTRODUCTION

Isogenies of supersingular elliptic curves give a computationally intractable problem even against quantum computers, and based on it, isogeny-based cryptosystems are now widely studied as one candidate for post-quantum cryptography. Recently, by several authors, the cryptosystems are extended to higher genus isogenies, especially, genus-2 case [14, 4, 1].

In particular, Castryck–Decru–Smith [1] showed that superspecial genus-2 curves and their isogeny graphs give a correct foundation for constructing genus-2 isogeny cryptography. They also presented concrete algebraic formulas for computing $(2, 2)$-isogenies by using the Richelot construction. In the genus-2 case, the isogenies may have decomposed principally polarized abelian surfaces as codomain, and we call them decomposed isogenies. In [1], the authors gave explicit formulas of the decomposed isogenies and a theorem stating that the number of decomposed Richelot isogenies outgoing from the Jacobian $J(C)$ for a superspecial curve $C$ of genus 2 is at most six (Theorem 3 in [1]) but not precisely determined. Moreover, their proof is computer-aided, that is, using the Gröbner basis computation.

Therefore, we revisit the isogeny counting based on an intrinsic algebraic geometric characterization. Over thirty years ago, Katsura–Oort [8, 9] classified reduced automorphisms of genus-2 superspecial Jacobians in details. According to the classification, we first count the number of Richelot isogenies from a superspecial Jacobian to decomposed surfaces (Cases (0)–(6) in Section 5) in terms of involutive (i.e., of order 2) reduced automorphisms. As a corollary, we give an algebraic geometric proof of Theorem 3 in [1] together with the precise Richelot isogeny counting (Remark 5.1). Moreover, by extending the method, we also count the total number of (decomposed) Richelot isogenies up to isomorphism outgoing from irreducible superspecial curves of genus 2 (resp. decomposed principally polarized superspecial abelian surfaces) in Theorem 6.2 (resp. Theorem 6.4).

Very recently, Costello and Smith [2] considered the isogeny path-finding algorithm in the genus-2 superspecial Richelot isogeny graph. They reduced the original problem to the elliptic curve path-finding problem and improved time complexity on the original genus-2
path-finding problem. The key ingredient of the reduction is a sub-algorithm for finding a path connecting a given irreducible genus-2 curve and the (connected) subset consisting of elliptic curve products. Our main proposition (Proposition 4.3) shows the equivalence of existence of a decomposed Richelot isogeny outgoing from $J(C)$ and existence of an element of order 2 in the reduced automorphisms of $C$. It implies that the subset of elliptic curve products are adjacent to genus-2 curves having involutive reduced automorphisms in the superspecial graph. Love and Boneh [10] focused on non-scalar endomorphisms of small degree for clarifying supersingular isogeny graph structure in the elliptic curve case. Since the above involutive reduced automorphisms in genus 2 also give 1-small curves (i.e., ones with non-scalar endomorphisms of degree 1), we can use the $M$-small curves of genus 2 (i.e., ones with non-scalar endomorphisms of a small degree) for the attack based on some appropriate hypothesis. We then give an improvement of the Costello–Smith attack (Algorithm 2) by using the $M$-small curves of genus 2 for some threshold $M$.

Our paper is organized as follows: Section 2 gives mathematical preliminaries including the Katsura–Oort classification. Section 3 presents an abstract description of Richelot isogenies and Section 4 gives the main characterization of decomposed Richelot isogenies in terms of reduced automorphism groups. Section 5 counts the number of long elements of order 2 in reduced automorphism groups based on the results in Section 4. Section 6 gives the total numbers of (decomposed) Richelot isogenies outgoing from the irreducible superspecial curves of genus 2 and products of two elliptic curves, respectively. Section 7 gives some examples in small characteristic. Finally, Section 8 shows a cryptographic application of our characterization to the Costello–Smith attack.

For an abelian surface $A$ or a nonsingular projective variety $X$, we use the following notation:

- $A[n]$: the group of $n$-torsion points of $A$.
- $A^t$: the dual of $A$.
- $\text{NS}(A)$: the Néron-Severi group of $A$.
- $T_v$: the translation by an element $v$ of $A$.
- $D \sim D'$: linear equivalence for divisors $D$ and $D'$ on $X$.
- $D \approx D'$: numerical equivalence for divisors $D$ and $D'$ on $X$.
- $\text{id}_X$: the identity morphism of a variety $X$.

2. Preliminaries

Let $k$ be an algebraically closed field of characteristic $p > 5$, and $C$ a nonsingular projective curve 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 isomorphic to $E_1 \times E_2$ with $E_i$ supersingular elliptic curves ($i = 1, 2$). Since for any supersingular elliptic curves $E_i$ ($i = 1, 2, 3, 4$) we have an isomorphism $E_1 \times E_2 \cong E_3 \times E_4$ (cf. Shioda [12], Theorem 3.5, for instance), this notion doesn’t depend on the choice of supersingular elliptic curves. We denote by $\text{Aut}(C)$ the automorphism group of $C$. Since $C$ is hyperelliptic, $C$ has the natural involution $\iota$ such that the quotient curve $C/\langle \iota \rangle$ is isomorphic to the projective line $\mathbb{P}^1$:

$$\psi : C \longrightarrow \mathbb{P}^1.$$ 

There exist 6 ramification points on $C$. We denote them by $P_i$ ($1 \leq i \leq 6$). Then, $Q_i = \psi(P_i)$’s are branch points of $\psi$ on $\mathbb{P}^1$. The group $\langle \iota \rangle$ is a normal subgroup of $\text{Aut}(C)$. We put $\text{RA}(C) = \text{Aut}(C)/\langle \iota \rangle$ and we call it the reduced automorphism group of $C$. For $\sigma \in \text{RA}(C)$, $\tilde{\sigma}$ is an element $\text{Aut}(C)$ such that $\tilde{\sigma} \bmod \langle \iota \rangle = \sigma$. 

Definition 2.1. An element $\sigma \in \text{RA}(C)$ of order 2 is said to be long if $\tilde{\sigma}$ is of order 2. Otherwise, an element $\sigma \in \text{RA}(C)$ of order 2 is said to be short (cf. Katsura–Oort [8], Definition 7.15).

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

Lemma 2.2. If an element $\sigma \in \text{RA}(C)$ of order 2 acts freely on 6 branch points, then $\sigma$ is long.

Proof. By a suitable choice of coordinate $x$ of $A^1 \subset P^1$, taking 0 as a fixed point of $\sigma$, we may assume $\sigma(x) = -x$, and $Q_1 = 1, Q_2 = -1, Q_3 = a, Q_4 = -a, Q_5 = b, Q_6 = -b$ $(a \neq 0, \pm 1; b \neq 0, \pm 1; a \neq \pm b)$. Then, the curve is defined by
\[
y^2 = (x^2 - 1)(x^2 - a^2)(x^2 - b^2),
\]
and $\tilde{\sigma}$ is given by $x \mapsto -x, y \mapsto \pm y$. Therefore, $\tilde{\sigma}$ is of order 2.

Lemma 2.3. If $\text{RA}(C)$ has an element $\sigma$ of order two, then there exists a long element $\tau \in \text{RA}(C)$ of order 2.

Proof. If $\sigma$ acts freely on 6 branch points, then by Lemma 2.2, $\sigma$ itself is a long element of order 2. We assume that the branch point $Q_1 = \psi(P_1)$ is a fixed point of $\sigma$. Since $\sigma$ is of order 2, it must have one more fixed point among the branch points, say $Q_2 = \psi(P_2)$. By a suitable choice of coordinate $x$ of $A^1 \subset P^1$, we may assume $Q_1 = 0$ and $Q_2 = \infty$. We may also assume $Q_3 = 1$. Then, $\sigma$ is given by $x \mapsto -x$ and the six branch points are 0, 1, $-1$, $a$, $-a$, $\infty$ $(a \neq \pm 1)$. The curve $C$ is given by
\[
y^2 = x(x^2 - 1)(x^2 - a^2) \quad (a \neq 0, \pm 1).
\]
We consider an element $\tau \in \text{Aut}(P^1)$ defined by $x \mapsto \frac{a}{x}$. Then, we have an automorphisms $\tilde{\tau}$ of $C$ defined by $x \mapsto \frac{a}{x}, y \mapsto \frac{a\sqrt{2}y}{\sqrt{2}}$. Therefore, we see $\tilde{\tau} \in \text{RA}(C)$. Since $\tilde{\tau}$ is of order 2, $\tau$ is long.

$\text{RA}(C)$ acts on the projective line $P^1$ as a subgroup of $\text{PGL}_2(k)$. The structure of $\text{RA}(C)$ is classified as follows (cf. Igusa [7], and Ibukiyama–Katsura–Oort [5]):

\[
\begin{align*}
(0) & \quad 0, \ (1) Z/2Z, \ (2) S_3, \ (3) Z/2Z \times Z/2Z, \ (4) D_{12}, \ (5) S_4, \ (6) Z/5Z.
\end{align*}
\]

We denote by $n_i$ the number of superspecial curves of genus 2 whose reduced automorphism group is isomorphic to the group $(i)$. Then, $n_i$’s are given as follows (cf. Ibukiyama–Katsura–Oort [5]):

\[
\begin{align*}
(0) & \quad n_0 = (p-1)(p^2-35p+346)/2880 - \{1 - (\frac{1}{p})\}/32 - \{1 - (\frac{2}{p})\}/8 - \{1 - (\frac{3}{p})\}/9 \\
& \quad + \begin{cases} 0 & \text{if } p \equiv 1, 2 \text{ or } 3 \pmod{5}, \\
-1/5 & \text{if } p \equiv 4 \pmod{5}, \end{cases} \\
(1) & \quad n_1 = (p-1)(p-17)/48 + \{1 - (\frac{1}{p})\}/8 + \{1 - (\frac{2}{p})\}/2 + \{1 - (\frac{3}{p})\}/2, \\
(2) & \quad n_2 = (p-1)/6 - \{1 - (\frac{2}{p})\}/2 - \{1 - (\frac{3}{p})\}/3, \\
(3) & \quad n_3 = (p-1)/8 - \{1 - (\frac{1}{p})\}/8 - \{1 - (\frac{2}{p})\}/4 - \{1 - (\frac{3}{p})\}/2, \\
(4) & \quad n_4 = \{1 - (\frac{2}{p})\}/2, \\
(5) & \quad n_5 = \{1 - (\frac{3}{p})\}/2, \\
(6) & \quad n_6 = \begin{cases} 0 & \text{if } p \equiv 1, 2 \text{ or } 3 \pmod{5}, \\
1 & \text{if } p \equiv 4 \pmod{5}. \end{cases}
\end{align*}
\]
Here, for a prime number \( q \) and an integer \( a \), \( \left( \frac{a}{q} \right) \) is the Legendre symbol. The total number \( n \) of superspecial curves of genus 2 is given by

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

For an abelian surface \( A \), we have \( A^t = \text{Pic}^0(A) \) (Picard variety of \( A \)), and for a divisor \( D \) on \( A \), there exists a homomorphism

\[
\varphi_D : A \longrightarrow A^t
\]

\[
v \longmapsto T_v^*D - D.
\]

If \( D \) is ample, then \( \varphi_D \) is surjective, i.e., an isogeny. We know \( (D \cdot D)^2 = 4 \deg \varphi_D \). We set \( K(D) = \text{Ker} \varphi_D \). If \( D \) is ample, then \( K(D) \) is finite and it has a non-degenerate alternating bilinear form \( e^D(v, w) \) on \( K(D) \) (cf. Mumford [11]). Let \( G \) be an isotropic subgroup scheme of \( K(D) \) with respect to \( e^D(v, w) \). In case \( D \) is ample, \( G \) is finite and we have an isogeny

\[
\pi : A \longrightarrow A/G.
\]

The following theorem is due to Mumford [11], Section 23:

**Theorem 2.4.** Let \( G \) be an isotropic subgroup scheme of \( K(D) \). Then, there exists an divisor \( D' \) on \( A/G \) such that \( \pi^*D' \sim D \).

Let \( n \) be a positive integer which is prime to \( p \). Then, we have the Weil pairing \( e_n : A[n] \times A^t[n] \longrightarrow \mu_n \). Here, \( \mu_n \) is the multiplicative group of order \( n \). By Mumford [11], Section 23 “Functional Properties of \( e^\ell \) (5)”, we have the following.

**Lemma 2.5.** For \( v \in A[n] \) and \( w \in \varphi_D^{-1}(A^t[n]) \), we have

\[
e_n(v, \varphi_D(w)) = e^{nD}(v, w).
\]

If \( D \) is a principal polarization, the homomorphism \( \varphi_D : A \longrightarrow A^t \) is an isomorphism. Therefore, by this identification we can identify the pairing \( e^{nD} \) with the Weil pairing \( e_n \).

### 3. Richelot Isogeny

We recall the abstract description of Richelot isogeny. (For the concrete construction of Richelot isogeny, see Castryck–Decru–Smith [1], for instance.)

Let \( A \) be an abelian surface with a principal polarization \( C \). Then, we may assume that \( C \) is effective, and we have the self-intersection number \( C^2 = 2 \). It is easy to show (or as was shown by A. Weil) that there are two cases for effective divisors with self-intersection 2 on an abelian surface \( A \):

1. There exists a nonsingular curve \( C \) of genus 2 such that \( A \) is isomorphic to the Jacobian variety \( J(C) \) of \( C \) and that \( C \) is the divisor with self-intersection 2. In this case, \( (J(C), C) \) is said to be non-decomposed.

2. There exist two elliptic curves \( E_1, E_2 \) with \( (E_1 \cdot E_2) = 1 \) such that \( E_1 \times \{0\} + \{0\} \times E_2 \) is a divisor with self-intersection 2 and that \( A \cong E_1 \times E_2 \). In this case, \( (A, E_1 \times \{0\} + \{0\} \times E_2) \) is said to be decomposed.

Since \( \varphi_C \) is an isomorphism by the fact that \( C \) is a principal polarization, we have \( K'(2C) = \text{Ker} \varphi_{2C} = \text{Ker} 2\varphi_C = A[2] \). Let \( G \) be a maximal isotropic subgroup of \( K(2C) = A[2] \) with respect to the pairing \( e^{2C} \). Since we have \( |G|^2 = |A[2]| = 2^4 \) (cf. Mumford [11]), we have \( |G| = 4 \) and \( G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \). We have a quotient homomorphism

\[
\pi : A \longrightarrow A/G.
\]
Now, we fix a supersingular elliptic curve \( E \), and assume that \( A \) is a superspecial abelian surface. Then, we have an isomorphism \( A \cong E \times E \). Since \( \pi \) is separable, we see that \( A/G \) is also a superspecial abelian surface. By Theorem 2.4, there exists a divisor \( C' \) such that \( 2C \sim \pi^*C' \). Since \( \pi \) is a finite morphism and \( 2C \) is ample, we see that \( C' \) is also ample.

We have the self-intersection number \( (2C \cdot 2C) = 8 \), and we have
\[
8 = (2C \cdot 2C) = (\pi^*C' \cdot \pi^*C') = \deg(\pi(C' \cdot C')) = 4(C' \cdot C').
\]
Therefore, we have \( (C' \cdot C') = 2 \), that is, \( C' \) is a principal polarization on \( A/G \). By the Riemann–Roch theorem of an abelian surface for ample divisors, we have
\[
\dim H^0(A/G, \mathcal{O}_{A/G}(C')) = (C' \cdot C')/2 = 1.
\]
Therefore, we may assume \( C' \) is an effective divisor.

Using these facts, we see that \( C' \) is either a nonsingular curve of genus two or \( E_1 \cup E_2 \) with elliptic curves \( E_i \) \((i = 1, 2)\) which intersect each other transversely. In this situation, the correspondence from \( \{A, C\} \) to \( \{A/G, C'\} \) is called a Richelot isogeny. Note that the Richelot isogeny is invertible. That is, in this situation, it is easy to show that there exists a Richelot isogeny from \( \{A/G, C'\} \) to \( \{A, C\} \).

From here on, for abelian surface \( E_1 \times E_2 \) with elliptic curves \( E_i \) \((i = 1, 2)\) we denote by \( E_1 + E_2 \) the divisor \( E_1 \times \{0\} + \{0\} \times E_2 \), if no confusion occurs. We sometimes call \( E_1 \times E_2 \) a principally polarized abelian surface. In this case, the principal polarization on \( E_1 \times E_2 \) is given by \( E_1 + E_2 \).

**Definition 3.1.** Let \((A, C), (A', C')\) and \((A'', C'')\) be principally polarized abelian surfaces with principal polarizations \( C, C', C'', \) respectively. The Richelot isogeny \( \varphi : A \rightarrow A' \) is said to be isomorphic to the Richelot isogeny \( \psi : A \rightarrow A'' \) if there exist an automorphism \( \sigma \in A \) with \( \sigma^*C \approx C \) and an isomorphism \( g : A' \rightarrow A'' \) with \( g^*C'' \approx C' \) such that the following diagram commutes:
\[
\begin{array}{ccc}
\sigma & : & A \\
\downarrow \varphi & & \downarrow \psi \\
A' & \rightarrow & A''
\end{array}
\]

4. **DECOMPOSED RICHELOT ISOGONY**

In this section, we use the same notation as in Section 3.

**Definition 4.1.** Let \( A \) and \( A' \) be abelian surfaces with principal polarizations \( C, C', \) respectively. A Richelot isogeny \( A \rightarrow A' \) is said to be decomposed if \( C' \) consists of two elliptic curves. Otherwise, the Richelot isogeny is said to be non-decomposed.

**Example 4.2.** Let \( C_{a,b} \) be a nonsingular projective model of the curve of genus 2 defined by the equation
\[
y^2 = (x^2 - 1)(x^2 - a)(x^2 - b) \quad (a \neq 0, 1; b \neq 0, 1; a \neq b).
\]
Let \( \iota \) be the natural involution defined by \( x \mapsto x, \ y \mapsto -y \). \( RA(C_{a,b}) \) has an element of order 2 defined by
\[
\sigma : x \mapsto -x, \ y \mapsto y.
\]
We put \( \tau = \iota \circ \sigma \). We have two elliptic curves \( E_\sigma = C_{a,b}/\langle \sigma \rangle \) and \( E_\tau = C_{a,b}/\langle \tau \rangle \). The elliptic curve \( E_\sigma \) is isomorphic to an elliptic curve \( E_\lambda : y^2 = x(x - 1)(x - \lambda) \) with
\[
\lambda = (b - a)/(1 - a)
\]
(4.1)
and the elliptic curve $E_\tau$ is isomorphic to an elliptic curve $E_\mu : y^2 = x(x-1)(x-\mu)$ with
\begin{equation}
\mu = (b-a)/b(1-a).
\end{equation}

The map given by (4.1) and (4.2) yields a bijection
\[
\{(a, b) \mid a, b \in k; a \neq 0, 1; b \neq 0, 1; a \neq b, \text{ and } J(C_{a,b}) \text{ is superspecial}\}
\rightarrow \{\mu, \eta \mid \lambda, \mu \in k; \lambda \neq \mu; E_\lambda, E_\mu \text{ are supersingular}\}
\]
(for the details, see Katsura–Oort [9], p259). We have a natural morphism $C_{a,b} \rightarrow E_\sigma \times E_\tau$. We have a natural morphism $C_{a,b} \rightarrow E_\sigma \times E_\tau$ and this morphism induces an isogeny
\[
\pi : J(C_{a,b}) \rightarrow E_\sigma \times E_\tau.
\]

By Igusa [7], we know Ker $\pi \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and Ker $\pi$ consists of $P_1 - \sigma(P_1), P_3 - \sigma(P_3), P_5 - \sigma(P_5)$ and the zero point. Here, $P_1 = (1, 0), P_3 = (a, 0), P_5 = (b, 0)$. Since $P_1 - \sigma(P_1)$ is a divisor of order 2, we have $P_1 - \sigma(P_1) \sim \sigma(P_1) - P_1$.

Comparing the calculation in Castryck–Decru–Smith [1] with the one in Katsura–Oort [9], we see that $\pi : J(C_{a,b}) \rightarrow E_\sigma \times E_\tau$ is a decomposed Richelot isogeny with $C_{a,b} = E_\sigma + E_\tau$ (also see Katsura–Oort [8], Proof of Proposition 7.18 (iii)). We will use the bijection above to calculate decomposed Richelot isogenies.

**Proposition 4.3.** Let $C$ be a nonsingular projective curve of genus 2. Then, the following three conditions are equivalent.

(i) $C$ has a decomposed Richelot isogeny outgoing from $J(C)$.

(ii) RA($C$) has an element of order 2.

(iii) RA($C$) has a long element of order 2.

**Proof.** (i) $\Rightarrow$ (ii). By assumption, we have a Richelot isogeny
\begin{equation}
\eta : J(C) \rightarrow J(C)/G
\end{equation}
such that $G$ is an isotropic subgroup of $J(C)$ [2] with respect to $2C$, and that $C'$ is a principal polarization consisted of two elliptic curves $E_i$ $(i = 1, 2)$ on $J(C)/G$ with $2C \sim \pi^*(E_1 + E_2)$. Since $C$ is superspecial, we see $J(C) \cong J(C)$ and $(J(C)/G) \cong J(C)/G$. Dualizing (4.3), we have
\[
\eta = \pi^* : J(C)/G \rightarrow J(C)
\]
with $J(C)/G \cong E_1 \times E_2, C' = E_1 + E_2$ and $\eta^*(C) \sim 2(E_1 + E_2)$. The kernel Ker $\eta$ is an isotropic subgroup of $(E_1 \times E_2)[2]$ with respect to the divisor $2(E_1 + E_2)$.

Denoting by $t_{E_1}$ the inversion of $E_1$, we set
\[
\tilde{\tau} = t_{E_1} \times id_{E_2}.
\]

Then, $\tilde{\tau}$ is an automorphism of order two which is not the inversion of $E_1 \times E_2$. By the definition, we have
\[
\tilde{\tau}^*(E_1 + E_2) = E_1 + E_2.
\]
Moreover, since Ker $\eta$ consists of elements of order 2, $\tilde{\tau}$ preserves Ker $\eta$. Therefore, $\tilde{\tau}$ induces an automorphism $\tau : J(C) \cong (J(C)/G)/\text{Ker } \eta \cong (E_1 \times E_2)/\text{Ker } \eta$. Therefore, we have the following diagram:
\[
\begin{array}{ccc}
E_1 \times E_2 & \xrightarrow{\tilde{\tau}} & E_1 \times E_2 \\
\eta \downarrow & & \eta \downarrow \\
J(C) & \xrightarrow{\tau} & J(C).
\end{array}
\]
We have
\[
\eta^* \tau^* C = \tilde{\tau}^* \eta\eta C = \tilde{\tau}^*(2(E_1 + E_2)) = 2(E_1 + E_2).
\]
On the other hand, we have
\[ \eta^* C = 2(E_1 + E_2). \]
Since \( \eta^* \) is an injective homomorphism from \( \text{NS}(J(C)) \) to \( \text{NS}(E_1 \times E_2) \), we have \( C \cong \tau^* C \). Therefore, \( \tau^* C - C \) is an element of \( \text{Pic}^0(J(C)) = J(C)^\dagger \). Since \( C \) is ample, the homomorphism
\[ \varphi_C : J(C) \longrightarrow J(C)^\dagger \]
is surjective. Therefore, there exists an element \( v \in J(C) \) such that
\[ T_v^* C - C \sim \tau^* C - C, \]
that is, \( T_v^* C \sim \tau^* C \). Since \( T_v^* C \) is a principal polarization, we see
\[ \dim H^0(J(C), O_{J(C)}(T_v^* C)) = 1. \]
Therefore, we have \( T_v^* C = \tau^* C \), that is, \( T_v^* \tau C = C \). Since \( \tau \) is of order 2, we have \( (\tau \circ T_{-v})^2 = T_{-v} - \tau(v) \), a translation. Therefore, we have \( T_{-v} - \tau(v) C = C \). However, since \( C \) is a principal polarization, we have \( \text{Ker} \varphi_C = \{0\} \). Therefore, we have \( T_{-v} - \tau(v) = \text{id} \).
This means \( \tau \circ T_{-v} \) is an automorphism of order 2 of \( C \). By definition, this is not the inversion \( \iota \). Hence, this gives an element of order 2 in \( \text{RA}(C) \).

(ii) \( \Rightarrow \) (iii) This follows from Lemma 2.3.
(iii) \( \Rightarrow \) (i) This follows from Lemma 2.2 and Example 4.2.

**Remark 4.4.** In the proof of the proposition, the automorphism \( \tau \circ T_{-v} \) gives really a long element of order 2 of \( C \).

By Castryck–Decru–Smith [1], if the curve \( C \) of genus 2 is obtained from a decomposed principally polarized abelian surface by a Richelot isogeny, then the curve \( C \) has a long reduced automorphism of order 2. As is well-known, for a curve \( C \) of genus 2, the Jacobian variety \( J(C) \) has 15 Richelot isogenies (cf. Castryck–Decru–Smith [1], for instance). Considering that Richelot isogeny is invertible, we have the following proposition.

**Proposition 4.5.** 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 \( \text{RA}(C) \) of order 2.

In this proposition, we consider a different isotropic subgroup gives a different Richelot isogeny. However, two different Richelot isogenies may be isomorphic to each other by a suitable automorphism (see Definition 3.1). From the next section, we will compute the number of Richelot isogenies up to isomorphism.

## 5. The Number of Long Elements of Order 2

In this section, we count the number of long elements of order 2 in \( \text{RA}(C) \). For an element \( f \in \text{RA}(C) \), we express the reduced automorphism by
\[ f : x \mapsto f(x) \]
with a suitable coordinate \( x \) of \( \mathbb{A}^1 \subset \mathbb{P}^1 \). We will give the list of \( f(x) \) which corresponds to an element of order 2. Here, we denote by \( \omega \) a primitive cube root of unity, by \( i \) a primitive fourth root of unity, and by \( \zeta \) a primitive sixth root of unity.

Case (0) \( \text{RA}(C) = \{0\} \).
There exists no such elements.
Case (1) \( \text{RA}(C) = \mathbb{Z}/2\mathbb{Z} \).
The curve \( C \) is given by \( y^2 = (x^2 - 1)(x^2 - a^2)(x^2 - b^2) \).
There exists only one long element of order 2 given by $f(x) = -x$.

**Case (2) RA($C$) = $S_3$.**

The curve $C$ is given by $y^2 = (x^3 - 1)(x^3 - a^3)$.

There exist three long elements of order 2 given by $f(x) = \frac{a}{x}, \frac{a^2}{x}, \frac{a^3}{x}$.

**Case (3) RA($C$) = $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.**

The curve $C$ is given by $y^2 = x(x^2 - 1)(x^2 - a^2)$.

There exist two long elements of order 2 given by $f(x) = \frac{a}{x}, \frac{a^2}{x}$, and there exists one short element of order 2 given by $f(x) = -x$.

**Case (4) RA($C$) = $D_{12}$.**

The curve is given by $y^2 = x^6 - 1$.

There exist four long elements of order 2 given by $f(x) = -x, \frac{x^2}{x}, \frac{x^3}{x}, \frac{x^4}{x}$, and there exist three short elements of order 2 given by $f(x) = \frac{1}{x}, \frac{x^2}{x}, \frac{x^3}{x}$.

**Case (5) RA($C$) = $S_4$.**

The curve $C$ is given by $y^2 = x(x^4 - 1)$.

There exist six long elements of order 2 given by $f(x) = \frac{x+1}{x-1}, \frac{x-1}{x+1}, \frac{1-i(x+i)}{1+i}, \frac{i-x}{x+i}, \frac{-i(x-1)}{x+1}$, and there exist three short elements of order 2 given by $f(x) = -x, \frac{1}{x}, -\frac{1}{x}$.

**Case (6) RA($C$) = $\mathbb{Z}/5\mathbb{Z}$.**

The curve is given by $y^2 = x^5 - 1$.

There exist no such elements.

**Remark 5.1.** By Proposition 4.5 and the calculation above, we see that for a curve $C$ of genus 2, the number of outgoing decomposed Richelot isogenies from $J(C)$ is at most six. This result coincides with the one given by Castryck–Decru–Smith [1], Theorem 3.

**6. Counting Richelot Isogenies**

**6.1. Richelot isogenies from Jacobians of irreducible genus-two curves.** Let $C$ be a non-singular complete curve of genus 2, and let $J(C)$ be the Jacobian variety of $C$. For a fixed $C$, we consider the set $\{(J(C), G)\}$ of pairs of $J(C)$ and an isotropic subgroup $G$ for the polarization $2C$. The automorphism group $Aut(C)$ acts on the ramification points of $C \rightarrow \mathbb{P}^1$. Using this action, $Aut(C)$ induces the action on the set $\{(J(C), G)\}$. Since the inversion $i$ of $C$ acts on $J(C)[2]$ trivially, the reduced automorphism group RA($C$) acts on the set $\{(J(C), G)\}$ which consists of 15 elements.

Let $P_i$ ($i = 1, 2, \ldots, 6$) be the ramification points of $\psi : C \rightarrow \mathbb{P}^1$. A division into 3 sets of pairs of these 6 points gives an isotropic subgroup $G$, that is,

$$\{P_{i_1} - P_{i_2}, P_{i_3} - P_{i_4}, P_{i_5} - P_{i_6}, \text{the identity}\}$$

gives an isotropic subgroup of $J(C)[2]$. The action of RA($C$) on the set $\{(J(C), G)\}$ is given by the action of RA($C$) on the set

$$\{\{(P_{i_1}, P_{i_2}), (P_{i_3}, P_{i_4}), (P_{i_5}, P_{i_6})\}\},$$

which contains 15 sets. In this section, we count the number of orbits of this action for each case.

Let $C$ be a curve of genus 2 with RA($C$) $\cong \mathbb{Z}/2\mathbb{Z}$. Such a curve is given by the equation

$$y^2 = (x^2 - 1)(x^2 - a)(x^2 - b)$$

with suitable conditions for $a$ and $b$. The branch points $Q_i = \psi(P_i)$ are given by

$Q_1 = 1, Q_2 = -1, Q_3 = \sqrt{a}, Q_4 = -\sqrt{a}, Q_5 = \sqrt{b}, Q_6 = -\sqrt{b}$.
The generator of the reduced automorphism group $RA(C)$ is given by

$$\sigma : x \mapsto -x.$$ 

Since the inversion $i$ acts trivially on the ramification points, $RA(C)$ acts on the set of the ramification points $\{P_1, P_2, P_3, P_4, P_5, P_6\}$, and the action of $\sigma$ on the ramification points is given by

$$P_{2i-1} \mapsto P_{2i}, \quad P_{2i} \mapsto P_{2i-1} \quad (i = 1, 2, 3).$$ 

The isotropic subgroup which corresponds to $\langle (P_1, P_2), (P_3, P_4), (P_5, P_6) \rangle$ gives a decomposed Richelot isogeny and the other isotropic subgroups give non-decomposed isogenies. Moreover, $\langle (\sigma(P_1), \sigma(P_2)), (\sigma(P_3), \sigma(P_4)), (\sigma(P_5), \sigma(P_6)) \rangle$ gives the Richelot isogeny isomorphic to the one given by $\langle (P_1, P_2), (P_3, P_4), (P_5, P_6) \rangle$. We denote $P_i$ by $i$ for the sake of simplicity. Then, the action $\sigma$ is given by the permutation $\langle 1, 2 \rangle\langle 3, 4 \rangle\langle 5, 6 \rangle$, and by the action of $RA(C)$, the set $\{\langle (P_{11}, P_{12}), (P_{13}, P_{14}), (P_{15}, P_{16}) \rangle\}$ of 15 elements is divided into the following 11 loci:

- $\langle (1, 2), (3, 4), (5, 6) \rangle$, $\langle (1, 2), (3, 5), (4, 6) \rangle$, $\langle (1, 2), (3, 6), (4, 5) \rangle$,
- $\langle (1, 3), (2, 4), (5, 6) \rangle$, $\langle (1, 3), (2, 5), (4, 6) \rangle$, $\langle (1, 3), (2, 4), (3, 5) \rangle$,
- $\langle (1, 4), (2, 6), (3, 5) \rangle$, $\langle (1, 4), (2, 3), (4, 5) \rangle$,
- $\langle (1, 5), (2, 6), (3, 4) \rangle$, $\langle (1, 5), (2, 3), (4, 6) \rangle$,
- $\langle (1, 6), (2, 5), (3, 4) \rangle$.

The reduced automorphism $\sigma$ is a long one of order 2 and the element $[1, 2, (3, 4), (5, 6)]$ is pairwise fixed by $\sigma$. Therefore, the element $[1, 2, (3, 4), (5, 6)]$ gives a decomposed isogeny. The other 10 loci give non-decomposed isogenies. In the same way, we have the following proposition.

**Proposition 6.1.** Under the notation above, the numbers of Richelot isogenies up to isomorphism in each case are given as follows:

1. $RA(C) = 0$: 15 Richelot isogenies. No decomposed one.
2. $RA(C) = \mathbb{Z}/2\mathbb{Z}$: 11 Richelot isogenies. 1 decomposed one.
3. $RA(C) = S_3$: 7 Richelot isogenies. 1 decomposed one.
4. $RA(C) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: 8 Richelot isogenies. 2 decomposed ones.
5. $RA(C) = \mathbb{D}_{12}$: 5 Richelot isogenies. 2 decomposed ones.
6. $RA(C) = S_4$: 4 Richelot isogenies. 1 decomposed one.
7. $RA(C) = \mathbb{Z}/5\mathbb{Z}$: 3 Richelot isogenies. No decomposed one.

**Theorem 6.2.** The total number of Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus 2 is equal to

$$\frac{(p-1)(p+2)(p+17)}{192} - 3\{1 - \left(\frac{-1}{p}\right)\}/32 + \{1 - \left(\frac{-2}{p}\right)\}/8.$$ 

The total number of decomposed Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus 2 is equal to

$$\frac{(p-1)(p-17)}{48} - \{1 - \left(\frac{-1}{p}\right)\}/8 + \{1 - \left(\frac{-3}{p}\right)\}/6.$$ 

**Proof.** The total number of Richelot isogenies up to isomorphism is equal to

$$15n_0 + 11n_1 + 7n_2 + 8n_3 + 5n_4 + 4n_5 + 3n_6$$

and the total number of decomposed Richelot isogenies up to isomorphism is equal to

$$n_1 + n_2 + 2n_3 + 2n_4 + n_5.$$ 

The results follow from these facts. □
6.2. Richelot isogenies from elliptic curve products. Let $E$, $E'$ be supersingular elliptic curves, and we consider a decomposed principally polarization $E + E'$ and a Richelot isogeny $(E \times E', E + E') \rightarrow (J(C), C)$. For the principally polarized abelian surface $(E \times E', E + E')$, we put $\text{RA}(E \times E') = \text{Aut}(E)/\langle \iota_E \rangle \times \text{Aut}(E')/\langle \iota_E' \rangle$, and call it the reduced automorphism group of $E \times E'$. Let $\{P_1, P_2, P_3\}$ (resp. $\{P_4, P_5, P_6\}$) be the 2-torsion points of $E$ (resp. $E'$). Then, the six points $P_i$ ($1 \leq i \leq 6$) on $E \times E'$ play the role of ramification points of irreducible curves of genus 2, and $\text{RA}(E \times E')$ acts on the set $\{P_1, P_2, P_3, P_4, P_5, P_6\}$. In this section, let $E_2$ be the elliptic curve defined by $y^2 = x^3 - x$ and $E_3$ the elliptic curve defined by $y^2 = x^3 - 1$. We know $\text{Aut}E_2 \cong \mathbb{Z}/4\mathbb{Z}$ and $\text{Aut}E_3 \cong \mathbb{Z}/6\mathbb{Z}$. The elliptic curve $E_2$ is supersingular if and only if $p \equiv 3 \pmod{4}$ and $E_3$ is supersingular if and only if $p \equiv 2 \pmod{3}$. In this section, the abelian surface $E \times E'$ means an abelian surface $E \times E'$ with principal polarization $E + E'$.

Now, let $E$, $E'$ be supersingular elliptic curves which are neither isomorphic to $E_2$ nor to $E_3$. We assume also $E$ is not isomorphic to $E'$. Using these notation, we have the following list of the orders of reduced automorphism groups.

$$|\text{RA}(E \times E')| = 1, \quad |\text{RA}(E \times E)| = 2, \quad |\text{RA}(E \times E_2)| = 2, \quad |\text{RA}(E \times E_3)| = 3,$$

$$|\text{RA}(E_2 \times E_2)| = 8, \quad |\text{RA}(E_3 \times E_3)| = 18, \quad |\text{RA}(E_2 \times E_3)| = 6.$$  

The isotropic subgroups for the polarization $(E + E')$ are determined in Castryck–Decru–Smith [1], Subsection 3.3. Using their results and the same method as in Subsection 6.1, we have the following proposition.

**Proposition 6.3.** Let $E$, $E'$ be supersingular elliptic curves which are neither isomorphic to $E_2$ nor to $E_3$. We assume also $E$ is not isomorphic to $E'$. The numbers of Richelot isogenies up to isomorphism outgoing from a decomposed principally polarized superspecial abelian surface in each case are given as follows:

(1) $E \times E'$: 15 Richelot isogenies, 6 non-decomposed ones.
(2) $E \times E$: 11 Richelot isogenies, 4 non-decomposed ones.
(3) $E \times E_2$: 9 Richelot isogenies, 3 non-decomposed ones ($p \equiv 3 \pmod{4}$).
(4) $E \times E_3$: 5 Richelot isogenies, 2 non-decomposed ones ($p \equiv 2 \pmod{3}$).
(5) $E_2 \times E_2$: 5 Richelot isogenies, 1 non-decomposed one ($p \equiv 3 \pmod{4}$).
(6) $E_3 \times E_3$: 3 Richelot isogenies, 1 non-decomposed one ($p \equiv 2 \pmod{3}$).
(7) $E_2 \times E_3$: 3 Richelot isogenies, 1 non-decomposed one ($p \equiv 11 \pmod{12}$).

We denote by $h$ the number of supersingular elliptic curves defined over $k$. Then, we know

$$h = \frac{p - 1}{12} + \frac{1 - (\frac{-3}{p})}{3} + \frac{1 - (\frac{-1}{p})}{4}$$

(cf. Igusa [6], for instance). We denote by $h_1$ the number of supersingular elliptic curves with trivial reduced automorphism group, $h_2$ the number of supersingular elliptic curves with $\text{Aut}(E_2) \cong \mathbb{Z}/4\mathbb{Z}$, $h_3$ the number of supersingular elliptic curves with $\text{Aut}(E_3) \cong \mathbb{Z}/6\mathbb{Z}$. We have $h = h_1 + h_2 + h_3$ and $h_2 = \frac{1 - (\frac{-1}{p})}{2}$ and $h_3 = \frac{1 - (\frac{-3}{p})}{2}$.

**Theorem 6.4.** The total number of non-decomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces is equal to

$$\frac{(p - 1)(p - 17)}{48} - \frac{1 - (\frac{-1}{p})}{8} + \frac{1 - (\frac{-3}{p})}{6}.$$

The total number of decomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces is equal to

$$\frac{(p - 1)(3p + 17)}{96} + (p + 6)\frac{1 - (\frac{-1}{p})}{16} + \frac{1 - (\frac{-3}{p})}{3}.$$
Proof. The total number of non-decomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces is equal to
\[
6\left\{ \frac{h_1(h_1-1)}{2} \right\} + 4h_1 + 3h_2h_1 + 2h_3h_1 + h_2 + h_3 + h_2h_3.
\]
The total number of decomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces is equal to
\[
9\left\{ \frac{h_1(h_1-1)}{2} \right\} + 7h_1 + 6h_2h_1 + 3h_3h_1 + 4h_2 + 2h_3 + 2h_2h_3.
\]
Since \(\{1 - (\frac{-1}{p})\}^2 = 2\{1 - (\frac{-1}{p})\}\) and \(\{1 - (\frac{-3}{p})\}^2 = 2\{1 - (\frac{-3}{p})\}\), the result follows from these facts. \(\square\)

Remark 6.5. Since the total number of decomposed Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus 2 is equal to the total number of non-decomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces, (6.1) and (6.2) give the same number.

7. Examples

By [5] and [9], we have the following normal forms of curves \(C\) of genus 2 with given reduced automorphism group \(\text{RA}(C)\):

1. For \(S_4 \subset \text{RA}(C)\), the normal form is \(y^2 = (x^3 - 1)(x^3 - \alpha)\).
   This curve is superspecial if and only if \(\alpha\) is a zero of the polynomial
   \[
g(z) = \sum_{l=0}^{[p/3]} \left( \frac{(p-1)/2}{(p+1)/6 + l} \right) \left( \frac{(p-1)/2}{l} \right) z^l.
   \]

2. For \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset \text{RA}(C)\), the normal form is \(y^2 = x(x^2 - 1)(x^2 - \beta)\).
   This curve is superspecial if and only if \(\beta\) is a zero of the polynomial
   \[
h(z) = \sum_{l=0}^{[p/4]} \left( \frac{(p-1)/2}{(p+1)/4 + l} \right) \left( \frac{(p-1)/2}{l} \right) z^l.
   \]

3. For \(\text{RA}(C) \cong D_{12}\), the normal form is \(y^2 = x^6 - 1\).
   This curve is superspecial if and only if \(p \equiv 5 \pmod{6}\).

4. For \(\text{RA}(C) \cong S_4\), the normal form is \(y^2 = x(x^4 - 1)\).
   This curve is superspecial if and only if \(p \equiv 5 \text{ or } 7 \pmod{8}\) (cf. Ibukiyama–Katsura–Oort [5]).

Finally, the elliptic curve \(E\) defined by \(y^2 = x(x-1)(x-\lambda)\) is supersingular if and only if \(\lambda\) is a zero of the Legendre polynomial
\[
\Phi(z) = \sum_{l=0}^{(p-1)/2} \left( \frac{(p-1)/2}{l} \right) z^l.
\]

Using these results, we construct some examples.

7.1. Examples in characteristic 13. Assume the characteristic \(p = 13\). Over \(k\) we have only one supersingular elliptic curve \(E\), and three superspecial curves \(C_1, C_2\) and \(C_3\) of genus 2 with reduced automorphism groups \(\text{RA}(C_1) \cong S_3\), \(\text{RA}(C_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\) and \(\text{RA}(C_3) = S_4\), respectively (cf. Ibukiyama–Katsura–Oort [5], Remark 3.4). In characteristic 13, we know \(h(z) = 7z^3 + 12z^2 + 12z + 7\), and the zeros are given by \(-1\) and \(-5 \pm \sqrt{6}\).
We also know \(g(z) = 2z^4 + 3z^3 + 4z^2 + 3z + 2\), and one of zeros is given by \(-4 + \sqrt{2}\). The
Legendre polynomial is given by $\Phi(z) = z^6 + 10z^5 + 4z^4 + 10z^3 + 4z^2 + 10z + 1$, and one of zeros is given by $3 - 2\sqrt{2}$. Using these facts, we know that the curves above are given by the following equations:

1. $E: y^2 = x(x - 1)(x - 3 + 2\sqrt{2})$ \quad (Aut($E$) $\cong \mathbb{Z}/2\mathbb{Z}$),
2. $C_1: y^2 = (x^3 - 1)(x^3 + 4 - \sqrt{2})$ \quad (RA($C_1$) $\cong S_3$),
3. $C_2: y^2 = x(x^2 - 1)(x^2 + 5 + 2\sqrt{6})$ \quad (RA($C_2$) $\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$),
4. $C_3: y^2 = x(x^3 - 1)$ \quad (RA($C_3$) $\cong S_4$).

Therefore, outgoing from superspecial curves of genus 2, we have, in total, $1 + 2 + 1 = 4$ decomposed Richelot isogenies up to isomorphism by Proposition 6.1. On the other hand, outgoing from the unique decomposed principally polarized abelian surface $(E \times E, E + E)$, we have 5 non-decomposed Richelot isogenies (not up to isomorphism) (cf. Castryck–Decru–Smith [1], also see, Katsura–Oort [9] and Igusa [7]). Using the method in Castryck–Decru–Smith [1], as the images of 5 non-decomposed Richelot isogenies, we have the following superspecial curves of genus 2:

(a) $C_a: y^2 = (x^2 - 1)(x^2 - 4 + 7\sqrt{2})(x^2 - 6 + 6\sqrt{2})$ \quad (RA($C_a$) $\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$),

(b) $C_b: y^2 = (x^2 - 1)(x^2 + 3 - 2\sqrt{2})(x^2 - 4 - \sqrt{2})$ \quad (RA($C_b$) $\cong S_4$),

(c) $C_c: y^2 = (x^2 - 1)(x^2 + 3 - 4\sqrt{2})(x^2 + 1 + 3\sqrt{2})$ \quad (RA($C_c$) $\cong S_3$),

(d) $C_d: y^2 = (x^2 - 1)(x^2 - 3)(x^2 + 3 - 4\sqrt{2})$ \quad (RA($C_d$) $\cong S_3$),

(e) $C_e: y^2 = (x^2 - 1)(x^2 - 6 - 6\sqrt{2})(x^2 - 2 + 2\sqrt{2})$ \quad (RA($C_e$) $\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).

We see that $C_a \cong C_e \cong C_2$, $C_c \cong C_d \cong C_1$ and $C_b \cong C_3$. As Richelot isogenies, $(E \times E, E + E) \rightarrow (J(C_a), C_e)$ is isomorphic to $(E \times E, E + E) \rightarrow (J(C_d), C_a)$, but $(E \times E, E + E) \rightarrow (J(C_a), C_a)$ is not isomorphic to $(E \times E, E + E) \rightarrow (J(C_e), C_e)$. Compare our graph with Castryck–Decru–Smith [1], Figure 1. In the graph the numbers along the edges are the multiplicities of Richelot isogenies outgoing from the nodes.
7.2. Examples in characteristic 11. Assume the characteristic $p = 11$. Over $k$ we have two supersingular elliptic curves $E_2, E_3$ and two superspecial curves $C_1, C_2$ of genus 2 with reduced automorphism groups $\text{RA}(C_1) \cong S_3$, $\text{RA}(C_2) \cong D_{12}$, respectively (cf. Ibukiyama–Katsura–Oort [5], Remark 3.4). In characteristic 11, we know 

$$h(z) = 10(z^3 + 5z^2 + 5z + 1),$$

and the roots are given by $-1, 3$ and $4$. Using this fact, we know that the curves above are given by the following equations:

1. $E_2$: $y^2 = x^3 - x$ \quad (RA($E_2$) $\cong \mathbb{Z}/2\mathbb{Z}$),
2. $E_3$: $y^2 = x^3 - 1$ \quad (RA($E_3$) $\cong \mathbb{Z}/3\mathbb{Z}$),
3. $C_1$: $y^2 = (x^3 - 1)(x^3 - 3)$ \quad (RA($C_1$) $\cong S_3$),
4. $C_2$: $y^2 = x^6 - 1$ \quad (RA($C_3$) $\cong D_{12}$).

We have three decomposed principally polarized abelian surfaces:

$$E_2 \times E_2, E_3 \times E_3, E_2 \times E_3.$$ 

Therefore, from the superspecial curves of genus 2 we have, in total, $1 + 2 = 3$ decomposed Richelot isogenies up to isomorphism by Proposition 6.1. On the other hand, from the decomposed principally polarized abelian surfaces, we have $1 + 1 + 1 = 3$ non-decomposed Richelot isogenies up to isomorphism by Proposition 6.3 (cf. Castryck–Decru–Smith [1], also see, Katsura–Oort [9] and Igusa [7]). For the decomposed principally polarized abelian surface $E_2 \times E_2$ the image of the only one non-decomposed Richelot isogeny is given by $C_2$. For the decomposed principally polarized abelian surface $E_3 \times E_3$ the image of the only one non-decomposed Richelot isogeny is also given by $C_2$. For the decomposed principally polarized abelian surface $E_2 \times E_3$ the image of the only one non-decomposed Richelot isogeny is given by $C_1$. 

![Diagram showing the relationships between the curves and isogenies](image-url)
7.3. **Examples in characteristic 7.** Assume the characteristic $p = 7$. Over $k$ we have only one supersingular elliptic curve $E_2$ and only one superspecial curves $C$ of genus 2, which has the reduced automorphism group $\text{RA}(C) \cong S_4$ (cf. Ibukiyama–Katsura–Oort [5], Remark 3.4).

They are given by the following equations:

1. $E_2$: $y^2 = x^3 - x$ \quad ($\text{Aut}(E_2) \cong \mathbb{Z}/2\mathbb{Z}$).
2. $C$: $y^2 = x(x^4 - 1)$ \quad ($\text{RA}(C) \cong S_4$).

We have only one decomposed principally polarized abelian surfaces $E_2 \times E_2$. Therefore, outgoing from the superspecial curves of genus 2 we have only one decomposed Richelot isogenies up to isomorphism. From the decomposed principally polarized abelian surface, we have also only one non-decomposed Richelot isogenies up to isomorphism (cf. Castryck–Decru–Smith [1], also see, Katsura–Oort [9] and Igusa [7]). For the decomposed principally polarized abelian surface $E_2 \times E_2$ the image of the only one non-decomposed Richelot isogeny is given by $C$.

**8. Cryptographic Application: Improving the Costello–Smith attack**

We will describe a cryptographic application of the equivalent conditions given in Proposition 4.3, which may improve the Costello–Smith attack on genus-2 isogeny problem. The implementation and further mathematical study will be given in our forthcoming paper.

**Definition 8.1.** Let $\Gamma_g(p)$ be the graph consisting of (isomorphism classes of) superspecial curves of genus $g$ (or the Jacobians) over $k$ of characteristic $p > 5$ as vertices and $(2, \ldots, 2)_g$-isogenies between them as edges. The vertex set is denoted by $V_g(p)$.

Algorithm 1 shows the attack on the genus-2 isogeny problem given in [2]. Since the key ingredient of the attack is using the decomposed subset $V_1(p) \times V_1(p)(\subset V_2(p))$ of elliptic
curve products, we can improve it using Proposition 4.3, which states the equivalence of neighboring to decomposed abelian surfaces in $\Gamma_2(p)$ and possession of involutive reduced automorphisms.

Algorithm 1 Computing isogeny paths in $\Gamma_2(p)$ [2]

**Input**: Superspecial Jacobian $A$ and $A'$ in $\mathcal{V}_2(p) \setminus \mathcal{V}_1(p) \times \mathcal{V}_1(p)$.

**Output**: A path $\rho : A \rightarrow A'$ in $\Gamma_2(p)$.

1. Find a path $\xi$ from $A$ to some decomposed one, $E_1 \times E_2$ in $\mathcal{V}_1(p) \times \mathcal{V}_1(p)$.
2. Find a path $\xi'$ from $A'$ to some decomposed one, $E'_1 \times E'_2$ in $\mathcal{V}_1(p) \times \mathcal{V}_1(p)$.
3. Find paths $\beta_1 : E_1 \rightarrow E'_1$ and $\beta_2 : E_2 \rightarrow E'_2$ in $\Gamma_1(p)$ using elliptic curve path finding.
4. If length$(\beta_1) \neq$ length$(\beta_2)$ mod 2, then go to step 1 (or 2) and try again with another $\xi, \xi', \beta_1, \beta_2$.
5. Otherwise, construct the product path $\chi : E_1 \times E_2 \rightarrow E'_1 \times E'_2$.
6. **return** the path $\rho := \xi'^1 \circ \chi \circ \xi$ from $A$ to $A'$.

Steps 1 and 2 compute paths $\xi$ and $\xi'$ by taking $O(p)$ non-backtracking random walks of length $O(\log(p))$ which can be parallelized, so with $P$ processors we expect $O(p/P)$ steps before finding $\xi$ and $\xi'$. As in [10], we define $M$-small curves of genus $g$ and the sets of those.

**Definition 8.2.** Given $1 \leq M < p$, a curve $C$ of genus $g$ (or its Jacobian $J(C)$) is $M$-small if there exists an endomorphism $\alpha$ of $J(C)$ with $\deg \alpha \leq M$ such that $\alpha$ is not multiplication by an integer. The set of $M$-small superspecial curves of genus $g$ (or invariants for $g = 1, 2$) is denoted $\mathcal{S}_g(p, M) \subset \mathcal{V}_g(p)$.

Since non-trivial elements in $\text{RA}(C)$ give non-scalar endomorphisms of degree 1, Proposition 4.3 implies that 1-small set $\mathcal{S}_2(p, 1)$ neighbors the decomposed component. Love–Boneh [10] observed the following facts on the sets $\mathcal{S}_1(p, M)$ in the elliptic curve case.

1. The set of all $M$-small elliptic curves can be generated efficiently by finding roots of Hilbert class polynomials.
2. When $M \ll p$, the set $\mathcal{S}_1(p, M)$ of $M$-small elliptic curves partitions into $O(M)$ subsets, i.e., $\mathcal{S}_1(p, M) = \bigcup_{\Delta} \mathcal{T}_1(p, \Delta)$ indexed by fundamental discriminant $|\Delta| < 4M$.
3. Moreover, there is no isogeny of degree $O(p^{1/4-\varepsilon})$ between any two elements in distinct subsets, i.e., $\mathcal{T}_1(p, \Delta) \neq \mathcal{T}_1(p, \Delta')$.

So, we can assume similar facts in the genus-2 case, i.e., for $\mathcal{S}_2(p, M)$.

**Hypothesis 8.3.** The set of all $M$-small curves of genus 2 can be generated efficiently by finding roots of class polynomials for Igusa invariants $j := (j_1, j_2, j_3)$ (see [3, 13], for example) and partitions into $O(M)$ subsets $\{\mathcal{T}_2(p, \Delta)\}$ according to discriminants $\Delta$ of quartic CM-orders.

Figure 1 shows how the $M$-small sets $\mathcal{S}_2(p, M)$ are located in the graph $\Gamma_2(p)$ of superspecial curves of genus 2. We recall that $\mathcal{V}_2(p)$ is the vertex set of $\Gamma_2(p)$. Based on the above hypothesis, Algorithm 2 proposes an improved random walk search in Algorithm 1, i.e., steps 1 and 2 in Algorithm 1 by making use of the special graph structure as is given in Figure 1 and efficient CM testing for genus-2 curves.
A superspecial Jacobian $J_1(p) \times J_1(p)$ is adjacent to a subset $S_2(p, 1)$ which is included in $T_2(p, \Delta_1)$. There exist other $O(M)$ disjoint subsets $T_2(p, \Delta_2), \ldots, T_2(p, \Delta_N)$ such that $S_2(p, M) = T_2(p, \Delta_1) \sqcup \cdots \sqcup T_2(p, \Delta_N)$.

Algorithm 2 Improved parallel search of a path in $\Gamma_2(p)$ between $A$ and $J_1(p) \times J_1(p)$

**Input**: A superspecial Jacobian $A$ in $\Gamma_2(p) \setminus J_1(p) \times J_1(p)$, a threshold $M$ and Igusa class polynomials $\{\tilde{H}_{1, \Delta}\}_{l=1,2,3; \Delta \leq \delta_l}$ with coefficients in $\mathbb{F}_p$ (where $\Delta$’s are discriminants of quartic CM-orders). Note that prime divisors of denominators of original (e.g., $\mathbb{Q}$-coeff.) class polynomials $H_{1, \Delta}$ are small for small $\Delta$ (i.e., order of $O(\Delta)$), and then $\tilde{H}_{1, \Delta}$ are well-defined for a cryptographically large prime $p \gg \Delta$ (see e.g., [13]).

**Output**: A path $\xi$ from $A$ to a product of elliptic curves $E_1 \times E_2$ in $J_1(p) \times J_1(p)$.

1. **From $A$, compute multiple paths in $\Gamma_2(p)$ in parallel.** In each step, check whether the Igusa invariants $j = (j_l)_{l=1,2,3}$ for the vertex satisfy the class polynomials $\{\tilde{H}_{1, \Delta}\}_{l=1,2,3; \Delta \leq \delta_l}$ or not.
2. **If some** Igusa invariant $j = (j_l)_{l=1,2,3}$ for $A' = J(C') \in J_2(p)$ on the paths satisfies class polynomials $\{\tilde{H}_{1, \Delta}\}_{l=1,2,3}$ for **some** $\Delta$, search around the vertex $A'$ intensively for meeting a product of elliptic curves $E_1 \times E_2$ in $J_1(p) \times J_1(p)$.
3. **Return** the path $\xi$ from $A$ to $E_1 \times E_2$.

**REFERENCES**

[1] W. Castryck, T. Decru, and B. Smith. Hash functions from superspecial genus-2 curves using Richelot isogenies. In *NatMic 2019: Number-Theoretic Methods in Cryptology*, 2019. To appear in *Journal of Mathematical Cryptology*.

[2] C. Costello and B. Smith. The supersingular isogeny problem in genus 2 and beyond. *IACR Cryptology ePrint Archive*, 2019:1387, 2019. To appear in *Journal of Mathematical Cryptology*.

[3] A. Enge and D. Robert. Computing class polynomials in genus 2. Technical report, DGA, April 2013.

[4] E. V. Flynn and Y. B. Ti. Genus two isogeny cryptography. In *PQCrypto 2019*, pages 286–306, 2019.

[5] T. Ibukiyama, T. Katsura, and F. Oort. Supersingular curves of genus two and class numbers. *Compositio Math.*, 57:127–152, 1986.

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

[7] J.-I. Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math.*, 72:612–649, 1960.

[8] T. Katsura and F. Oort. Families of supersingular abelian surfaces. *Compositio Math.*, 62:107–167, 1987.

[9] T. Katsura and F. Oort. Supersingular abelian varieties of dimension two or three and class numbers. *Advanced Studies in Pure Math.*, 10:253–281, 1987.

[10] J. Love and D. Boneh. Supersingular curves with small non-integer endomorphisms. *CoRR*, abs/1910.03180, 2019.
[11] D. Mumford. *Abelian Varieties*. Oxford Univ. Press, 1970.
[12] T. Shioda. Supersingular K3 surfaces. In *Algebraic Geometry, Proc. Copenhagen 1978* (K. Lønsted, ed.), Lecture Notes in Math. 732, pages 563–591. Springer-Verlag, Berlin-Heidelberg-New York, 1979.
[13] M. Streng. Computing Igusa class polynomials. *Math. Comput.*, 83(285):275–309, 2014.
[14] K. Takashima. Efficient algorithms for isogeny sequences and their cryptographic applications. In *Mathematical Modelling for Next-Generation Cryptography: CREST Crypto-Math Project*, pages 97–114. 2017.

**Graduate School of Mathematical Sciences, The University of Tokyo, Meguro-ku, Tokyo 153-8914, Japan**
*E-mail address*: tkatsura@ms.u-tokyo.ac.jp

**Information Technology R&D Center, Mitsubishi Electric, Kamakura-shi, Kanagawa 247-8501, Japan**
*E-mail address*: Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp