RIMS Kôkyûroku Bessatsu
B90 (2022), 185–193

Counting superspecial Richelot isogenies by reduced automorphism groups

By

Katsuyuki Takashima*

Abstract

The recent cryptanalysis by Costello and Smith [10] employed the subgraphs whose vertices consist of *decomposed* principally polarized abelian varieties, hence it is important to study the subgraphs in isogeny-based cryptography. Katsura and Takashima [22] initiated the investigation of the decomposed abelian surface subgraphs in the genus-2 case. This paper surveys the work, aiming to provide a kind of handbook for applying our results to cryptography.

§ 1. Introduction

Isogenies of supersingular elliptic curves are widely studied as one candidate for post-quantum cryptography (PQC), e.g., [6, 11, 18, 4]. In particular, the supersingular isogeny-based Diffie-Hellman (SIDH) key exchange proposed by De Feo et al. [11] is elegantly designed and strongly secure in the post-quantum age, that is, it allows only exponential-time (classical and) quantum cryptanalyses [19, 9][1]. Moreover, the key encapsulation mechanism SIKE [18] that is selected as the only isogeny-based (alternate) candidates in the third round of NIST[2] PQC competition is based on the SIDH key exchange.

Note that the families of supersingular isogeny graphs in SIDH are Ramanujan [25], that is, they have an optimal expanding graph property. The Ramanujan property of the isogeny graphs is very desirable for cryptography, and the fact was originally pointed

Received December 30, 2020. Revised March 2, 2021.
2020 Mathematics Subject Classification(s): Primary 14K02; Secondary 14G50, 14H37, 14H40.
Key Words: *Richelot isogenies, superspecial abelian surfaces, reduced group of automorphisms, genus-2 isogeny cryptography.*
*Faculty of Education and Integrated Arts and Sciences, Waseda University, Tokyo 169-8050, Japan.
e-mail: `ktakashima@waseda.jp`
[1] While another isogeny-based key exchange named CSIDH [4] is versatile in applied cryptography, it allows subexponential-time quantum cryptanalyses [7, 24, 2].
[2] NIST stands for National Institute of Standards and Technology.

out by Charles et al. [6] as an advantage of the CGL hash function proposal. The mathematical and computational aspects of the graphs are closely connected with the security and efficiency of SIDH, and have been actively studied by several researchers, e.g., [8, 13, 14, 23].

Recently, several authors have extended the cryptosystems to higher genus isogenies, especially the genus-2 case [5, 29, 15, 3, 10]. Castryck, Decru, and Smith [3] showed that *superspecial* genus-2 curves and their isogeny graphs give a correct foundation for constructing genus-2 isogeny cryptography. The recent cryptanalysis by Costello and Smith [10] employed the subgraph whose vertices consist of decomposed principally polarized abelian varieties, hence it is important to study the subgraph in cryptography. Katsura and Takashima [22] initiated the investigation of the decomposed abelian surface subgraphs, especially we studied how the decomposed part connects with the non-decomposed part in the superspecial Richelot isogeny graphs. Moreover, by extending an approach by Ibukiyama, Katsura, and Oort [16], which is based on the classification of reduced automorphism groups (cf. Bolza [1] and Igusa [17]), we also count the total number of Richelot isogenies up to isomorphism. (For connectedness and the (non-)Ramanujan property of the superspecial Richelot isogeny graphs, refer to [20])

This paper surveys the work of Katsura and Takashima [22], aiming to provide a kind of handbook for applying the results to cryptography. Section 2 gives some preliminary definitions and facts on superspecial abelian surfaces and Richelot isogenies. Section 3 gives classical results on counting superspecial curves of genus 1 and 2. Section 4.1 classifies *long* reduced automorphisms which are a key ingredient in our work, and based on it, Section 4.2 determines local configuration types (LCT) of Richelot isogenies. Combining it with the superspecial curve counting in Section 3, Section 4.3 gives total numbers of superspecial Richelot isogenies up to isomorphism.

We use the following notation: For an abelian surface A, $A[n]$ denotes the group of n-torsion points of A, and $D \sim D'$ (resp. $D \approx D'$) denotes linear equivalence (resp. numerical equivalence) for divisors D and D' on A.

§ 2. Preliminaries

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.e., $E_i[p] = \{O_{E_i}\}$ for $i = 1, 2$. 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. [28]). If we do not consider polarizations, all superspecial abelian surfaces are isomorphic to each other. For a nonsingular projective curve C of genus 2 over k, we denote by $(J(C), C)$

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.

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. For $\sigma \in \mathrm{RA}(C)$, $\tilde{\sigma}$ is an element of $\mathrm{Aut}(C)$ such that $\tilde{\sigma} \bmod \langle\iota\rangle = \sigma$. 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 (cf. Katsura–Oort [21]). This definition does not depend on the choice of $\tilde{\sigma}$.

Let (A, D) be a principally polarized abelian surface with $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ a maximal isotropic subgroup of $A[2]$ with respect to the Weil pairing. We have a quotient homomorphism $\pi : A \longrightarrow A/G$. There exists a divisor D' on A/G s.t. $2D \sim \pi^*D'$. We see that D' is a principal polarization on A/G and that D' is either a nonsingular curve of genus 2 or $E_1' + E_2'$ with elliptic curves E_1', E_2' and $(E_1' \cdot E_2') = 1$. The correspondence from (A, D) to $(A/G, D')$ is called a Richelot isogeny since the first explicit construction was given by Richelot [26, 27]. It is called decomposed if D' consists of two elliptic curves. Otherwise, it is called non-decomposed.

Definition 2.1 (Isomorphism of Richelot isogenies)**.** Let (A, D), (A', D') and (A'', D'') 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 $\sigma^*D \approx D$ and an isomorphism $g : A' \longrightarrow A''$ with $g^*D'' \approx D'$ s.t. the following diagram commutes:

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

§ 3. Counting superspecial curves of genus $g = 1, 2$

By definition, the notion of supersingularity and superspeciality are equivalent in the genus-1 case.

The case that $g = 1$ ([12]). For supersingular elliptic curves E defined over k of characteristic $p \geq 5$, $\mathrm{Aut}(E)$ is isomorphic to

$$(1)\ \mathbb{Z}/2\mathbb{Z}, \quad (2)\ \mathbb{Z}/4\mathbb{Z}, \quad (3)\ \mathbb{Z}/6\mathbb{Z}.$$

We denote by h_l the number of supersingular elliptic curves whose $\mathrm{Aut}(E)$ are of type (l) and $h = h_1 + h_2 + h_3$. The numbers h_l's are given as follows:

(1) $h_1 = \frac{p-1}{12} - \{1 - (\frac{-1}{p})\}/4 - \{1 - (\frac{-3}{p})\}/6,$

(2) $h_2 = \{1 - (\frac{-1}{p})\}/2$, and

(3) $h_3 = \{1 - (\frac{-3}{p})\}/2$

since supersingular curves $E_2 : y^2 = x^3 - x$ for $p \equiv 3 \pmod 4$ and $E_3 : y^2 = x^3 - 1$ for $p \equiv 2 \pmod 3$ have $\mathrm{Aut}(E_2) \cong \mathbb{Z}/4\mathbb{Z}$ and $\mathrm{Aut}(E_3) \cong \mathbb{Z}/6\mathbb{Z}$. The total number h of supersingular elliptic curves over k is $h = h_1 + h_2 + h_3 = \frac{p-1}{12} + \{1-(\frac{-1}{p})\}/4 + \{1-(\frac{-3}{p})\}/3$.

The case that $g = 2$ ([17, 16]). In 1986, Ibukiyama, Katsura, and Oort [16] explicitly counted the curves of genus 2 with given reduced groups of automorphisms $\mathrm{RA}(C)$. Based on the result, in Section 4, we count the number of Richelot isogenies from a superspecial Jacobian to decomposed surfaces in terms of long reduced automorphisms.

$\mathrm{RA}(C)$ acts on the projective line $\mathbb{P}^1$ as a subgroup of $\mathrm{PGL}_2(k)$. The structure of $\mathrm{RA}(C)$ is classified as follows (cf. Igusa [17, p. 644], and Ibukiyama–Katsura–Oort [16, p. 130]):

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

We denote by n_l the number of superspecial curves of genus 2 whose reduced group of automorphisms is isomorphic to the group (l). Then, n_l's are given as follows (cf. [16, Theorem 3.3]):

(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) $n_5 = \{1 - (\frac{-2}{p})\}/2$, and

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

Here, for a prime number p and an integer a, $(\frac{a}{p})$ is the Legendre symbol. The total number n of superspecial curves of genus 2 is given by

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

§ 4. Counting superspecial Richelot isogenies up to isomorphism

§ 4.1. Long elements in $\mathrm{RA}(C)$

Table 1 counts the number of long elements of order 2 in $\mathrm{RA}(C)$. We denote the set of long elements in $\mathrm{RA}(C)$ by $\mathrm{L}(C)$, and we express the reduced automorphism $f \in \mathrm{RA}(C)$ by $f : x \mapsto f(x)$ with a suitable coordinate x of $\mathbb{A}^1 \subset \mathbb{P}^1$. Table 1 also gives the list of $f(x)$ corresponding to long elements of order 2. Here, we denote by ω a primitive cube root of unity, by i a primitive fourth root of unity, and by ζ a primitive sixth root of unity.

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

Table 1. Long elements in $\mathrm{RA}(C)$.

§ 4.2. Local configuration types (LCT) of Richelot isogenies

LCT of nonsingular genus-2 curves C. The number of Richelot isogenies up to isomorphism in each case and the number of elements in each isomorphism class are listed in Table 2, where, for example, the type $(1\times 6, 2\times 4)$ for non-decomposed Richelot isogenies in the case (1) (s.t., $\mathrm{RA}(C) \cong \mathbb{Z}/2\mathbb{Z}$) means that there exist 1 isomorphism class which contains 6 elements and 2 isomorphism classes which contain 4 elements. We call the above type like $(1 \times 6, 2 \times 4)$ *local configuration type (LCT)*. Moreover, in the table, let $r_{\mathrm{nd},l}$ (resp. $r_{\mathrm{nd}\to\mathrm{d},l}$) be the number of Richelot isogenies (resp. decomposed Richelot isogenies) up to isomorphism in the case (l).

(l)	$\mathrm{RA}(C)$	non-decomposed	decomposed	$r_{\mathrm{nd},l}$	$r_{\mathrm{nd}\to\mathrm{d},l}$
(0)	$\{0\}$	(1×15)	(0)	15	0
(1)	$\mathbb{Z}/2\mathbb{Z}$	$(1\times 6,\ 2\times 4)$	(1×1)	11	1
(2)	S_3	$(1\times 3,\ 3\times 3)$	(3×1)	7	1
(3)	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$	$(1\times 1,\ 2\times 4,\ 4\times 1)$	(1×2)	8	2
(4)	D_{12}	$(2\times 1,\ 3\times 1,\ 6\times 1)$	$(1\times 1,\ 3\times 1)$	5	2
(5)	S_4	$(1\times 1,\ 4\times 2)$	(6×1)	4	1
(6)	$\mathbb{Z}/5\mathbb{Z}$	(5×3)	(0)	3	0

Table 2. Local configuration types of Richelot isogenies from nonsingular genus-2 curves C and numbers $r_{\mathrm{nd},l}$, $r_{\mathrm{nd}\to\mathrm{d},l}$ for $l = 0,\dots,6$.

LCT of decomposed principally polarized abelian surfaces. Let E, E' be supersingular elliptic curves which are neither isomorphic to E_2 nor to E_3 with E_2 and E_3 defined as above. We also assume that E is not isomorphic to E'. The number of Richelot isogenies up to isomorphism outgoing from a decomposed principally polarized superspecial abelian surface in each case and the number of elements in each isomorphism class are listed in Table 3. Here, we use the same notation for local configuration types used in Table 2. Moreover, as in the table, let $r_{\mathrm{d}\to\mathrm{nd},l}$ (resp. $r_{\mathrm{d}\to\mathrm{d},l}$) be the number of non-decomposed Richelot isogenies (resp. decomposed Richelot isogenies) up to isomorphism in the case (l).

(l)	A	non-decomposed	decomposed	$r_{\mathrm{d}\to\mathrm{nd},l}$	$r_{\mathrm{d}\to\mathrm{d},l}$
(i)	$E\times E'$	(1×6)	(1×9)	6	9
(ii)	$E\times E$	$(1\times 3, 2\times 1)$	$(1\times 4, 2\times 3)$	4	7
(iii)	$E\times E_2$	(2×3)	$(1\times 3, 2\times 3)$	3	6
(iv)	$E\times E_3$	(3×2)	(3×3)	2	3
(v)	$E_2\times E_2$	(4×1)	$(1\times 1, 2\times 1, 4\times 2)$	1	4
(vi)	$E_3\times E_3$	(3×1)	$(3\times 1, 9\times 1)$	1	2
(vii)	$E_2\times E_3$	(6×1)	$(3\times 1, 6\times 1)$	1	2

Table 3. Local configuration types of Richelot isogenies from decomposed principally polarized abelian surfaces A and numbers $r_{\mathrm{d}\to\mathrm{nd},l}$, $r_{\mathrm{d}\to\mathrm{d},l}$ for $l = i,\dots,vii$.

§ 4.3. Total numbers of superspecial Richelot isogenies up to isomorphism

Richelot isogenies from nonsingular 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 irreducible superspecial curves of genus 2, and N_{nd} =

$N_{\mathrm{nd}\to\mathrm{d}} + N_{\mathrm{nd}\to\mathrm{nd}}$ be the total number of both types of Richelot isogenies up to isomorphism.

Theorem 4.1 (Theorem 6.2 in [22])**.**

$$N_{\mathrm{nd}} = \frac{(p-1)(p+2)(p+7)}{192} - 3\{1-(\frac{-1}{p})\}/32 + \{1-(\frac{-2}{p})\}/8, \tag{4.1}$$

$$N_{\mathrm{nd}\to\mathrm{d}} = \frac{(p-1)(p+3)}{48} - \{1-(\frac{-1}{p})\}/8 + \{1-(\frac{-3}{p})\}/6. \tag{4.2}$$

Proof. Since $(r_{\mathrm{nd},0},\dots,r_{\mathrm{nd},6}) = (15,11,7,8,5,4,3)$ and $(r_{\mathrm{nd}\to\mathrm{d},0},\dots,r_{\mathrm{nd}\to\mathrm{d},6}) = (0,1,1,2,2,1,0)$ in Table 2, $N_{\mathrm{nd}} = r_{\mathrm{nd},0}\cdot n_0 + \cdots + r_{\mathrm{nd},6}\cdot n_6 = 15n_0 + 11n_1 + 7n_2 + 8n_3 + 5n_4 + 4n_5 + 3n_6 =$ RHS of (4.1) and $N_{\mathrm{nd}\to\mathrm{d}} = r_{\mathrm{nd}\to\mathrm{d},0}\cdot n_0 + \cdots + r_{\mathrm{nd}\to\mathrm{d},6}\cdot n_6 = n_1+n_2+2n_3+2n_4+n_5 =$ RHS of (4.2). Here, the numbers n_l are given in Section 3. □

Richelot isogenies from elliptic curve products. Let $N_{\mathrm{d}\to\mathrm{nd}}$ (resp. $N_{\mathrm{d}\to\mathrm{d}}$) be the total number of non-decomposed (resp. decomposed) Richelot isogenies up to isomorphism outgoing from decomposed principally polorized superspecial abelian surfaces.

Theorem 4.2 (Theorem 6.4 in [22])**.**

$$N_{\mathrm{d}\to\mathrm{nd}} = \frac{(p-1)(p+3)}{48} - \{1-(\frac{-1}{p})\}/8 + \{1-(\frac{-3}{p})\}/6, \tag{4.3}$$

$$N_{\mathrm{d}\to\mathrm{d}} = \frac{(p-1)(3p+17)}{96} + (p+6)\{1-(\frac{-1}{p})\}/16 + \{1-(\frac{-3}{p})\}/3. \tag{4.4}$$

Proof. Since $(r_{\mathrm{d}\to\mathrm{nd},i},\dots,r_{\mathrm{d}\to\mathrm{nd},vii}) = (6,4,3,2,1,1,1)$, and $(r_{\mathrm{d}\to\mathrm{d},i},\dots,r_{\mathrm{d}\to\mathrm{d},vii}) = (9,7,6,3,4,2,2)$ in Table 3, $N_{\mathrm{d}\to\mathrm{nd}} = 6\{\frac{h_1(h_1-1)}{2}\}+4h_1+3h_1h_2+2h_1h_3+h_2+h_3+h_2h_3 =$ RHS of (4.3) and $N_{\mathrm{d}\to\mathrm{d}} = 9\{\frac{h_1(h_1-1)}{2}\} + 7h_1 + 6h_1h_2 + 3h_1h_3 + 4h_2 + 2h_3 + 2h_2h_3 =$ RHS of (4.4). Here, the numbers h_l are given in Section 3. Note that the results follow from the facts $\{1-(\frac{-1}{p})\}^2 = 2\{1-(\frac{-1}{p})\}$ and $\{1-(\frac{-3}{p})\}^2 = 2\{1-(\frac{-3}{p})\}$. □

References

[1] O. Bolza. On binary sextics with linear transformations into themselves. *American Journal of Mathematics*, 10(1):47–70, 1887.

[2] X. Bonnetain and A. Schrottenloher. Quantum security analysis of CSIDH. In *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 493–522. Springer, 2020.

[3] W. Castryck, T. Decru, and B. Smith. Hash functions from superspecial genus-2 curves using Richelot isogenies. *J. Math. Crypt.*, 14(1):268–292, 2020.

[4] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. CSIDH: An efficient post-quantum commutative group action. In *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 395–427. Springer, 2018.

[5] D. Charles, E. Goren, and K. Lauter. Families of Ramanujan graphs and quaternion algebras. In *Groups and Symmetries: From Neolithic Scots to John McKay*, pages 53–80, 2009.

[6] D. Charles, K. Lauter, and E. Goren. Cryptographic hash functions from expander graphs. *J. Crypt.*, 22(1):93–113, 2009.

[7] A. M. Childs, D. Jao, and V. Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Math. Cryptol.*, 8(1):1–29, 2014.

[8] A. Costache, B. Feigon, K. E. Lauter, M. Massierer, and A. Puskás. Ramanujan graphs in cryptography. In *Research Directions in Number Theory*, pages 1–40, 2019.

[9] C. Costello, P. Longa, M. Naehrig, J. Renes, and F. Virdia. Improved classical cryptanalysis of SIKE in practice. In *PKC 2020, Part II*, volume 12111 of *LNCS*, pages 505–534. Springer, 2020.

[10] C. Costello and B. Smith. The supersingular isogeny problem in genus 2 and beyond. In *PQCrypto 2020*, volume 12100 of *LNCS*, pages 151–168. Springer, 2020.

[11] L. De Feo, D. Jao, and J. Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Crypt.*, 8(3):209–247, 2014.

[12] M. Deuring. Die Typen der Multiplicatoren-ringe elliptischer Functionenkörper. *Abh. Math. Sem. Univ. Hamburg*, 14:197–272, 1941.

[13] K. Eisenträger, S. Hallgren, K. E. Lauter, T. Morrison, and C. Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 329–368. Springer, 2018.

[14] K. Eisenträger, S. Hallgren, C. Leonardi, T. Morrison, and J. Park. Computing endomorphism rings of supersingular elliptic curves and connections to pathfinding in isogeny graphs. In *ANTS 2020*, volume 4 of *The Open Book Series*, pages 215–232. Mathematical Sciences Publishers, 2020.

[15] E. V. Flynn and Y. B. Ti. Genus two isogeny cryptography. In *PQCrypto 2019*, volume 11505 of *LNCS*, pages 286–306. Springer, 2019.

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

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

[18] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. D. Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, G. Pereira, J. Renes, V. Soukharev, and D. Urbanik. SIKE: Supersingular isogeny key encapsulation. *submission to the NIST's PQC standardization, round 3*, October 2020.

[19] S. Jaques and J. M. Schanck. Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE. In *CRYPTO 2019, Part I*, volume 11692 of *LNCS*, pages 32–61. Springer, 2019.

[20] B. W. Jordan and Y. Zaytman. Isogeny graphs of superspecial abelian varieties and generalized Brandt matrices. *ArXiv*, abs/2005.09031, 2020.

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

[22] T. Katsura and K. Takashima. Counting Richelot isogenies between superspecial abelian surfaces. In *ANTS 2020*, volume 4 of *The Open Book Series*, pages 283–300. Mathematical Sciences Publishers, 2020.

[23] J. Love and D. Boneh. Supersingular curves with small non-integer endomorphisms. In *ANTS 2020*, volume 4 of *The Open Book Series*, pages 7–22. Mathematical Sciences Publishers, 2020.

[24] C. Peikert. He gives c-sieves on the CSIDH. In *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 463–492. Springer, 2020.

[25] A. K. Pizer. Ramanujan graphs and Hecke operators. *Bull. Amer. Math. Soc.*, 23(1):127–137, 1990.

[26] F. J. Richelot. Essai sur une méthode générale pour déterminer les valeurs des intégrales ultra-elliptiques, fondée sur des transformations remarquables de ces transcendantes. *C.R. Acad. Sci. Paris*, 2:622–627, 1836.

[27] F. J. Richelot. De transformatione integralium Abelianorum primi ordinis commentatio. *J. Reine Angew. Math.*, 16:221–341, 1837.

[28] T. Shioda. Supersingular K3 surfaces. In *Algebraic Geometry, Proc. Copenhagen 1978 (K. Lϕnsted, ed.)*, volume 732 of *LNM*, pages 563–591. Springer-Verlag, 1979.

[29] 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. Springer, 2017.