Finite Fields and Their Applications 103 (2025) 102579

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

Neighborhood of vertices in the isogeny graph of principally polarized superspecial abelian surfaces

Zheng Xu [a], Yi Ouyang [a,b,*], Zijian Zhou [c]

[a] *Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*
[b] *School of Mathematical Sciences, Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei 230026, Anhui, China*
[c] *College of Sciences, National University of Defense Technology, Changsha 410073, Hunan, China*

A R T I C L E I N F O

Article history:
Received 12 March 2024
Received in revised form 17 October 2024
Accepted 8 January 2025
Available online xxxx
Communicated by Gary L. Mullen

MSC:
11G20
11G15
14G15
14H52
94A60

Keywords:
Supersingular elliptic curves
Superspecial abelian surfaces
Principally polarized
Isogeny graph

A B S T R A C T

For two supersingular elliptic curves E and E' defined over $\mathbb{F}_{p^2}$, let $[E \times E']$ be the superspecial abelian surface with the principal polarization $\{0\} \times E' + E \times \{0\}$. We determine local structure of the vertices $[E \times E']$ in the (ℓ, ℓ)-isogeny graph of principally polarized superspecial abelian surfaces where either E or E' is defined over $\mathbb{F}_p$. We also present a simple new proof of the main theorem in [26].

© 2025 Elsevier Inc. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

* Corresponding author.
E-mail addresses: xuzheng1@mail.ustc.edu.cn (Z. Xu), yiouyang@ustc.edu.cn (Y. Ouyang), zhouzijian122006@163.com (Z. Zhou).

https://doi.org/10.1016/j.ffa.2025.102579
1071-5797/© 2025 Elsevier Inc. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

1. Introduction

Supersingular isogeny-based cryptography is a relatively new suggestion for post quantum cryptosystems and is based on the assumption that it is computationally hard (even for a quantum computer) to find a path in the ℓ-isogeny graph between two given vertices (equivalently to compute the endomorphism rings of supersingular elliptic curves). Known instantiations for isogeny-based cryptography include the key exchange protocols SIDH [21], CSIDH [7] and OSIDH [6], and the signature schemes GPS-sign [16] and SQI-sign [12].

As isogenies between supersingular curves found success in post quantum cryptography, it is natural to generalize the isogeny-based cryptosystem to abelian varieties of higher dimensions. Flynn-Ti [13] constructed a SIDH-like key exchange cryptosystem based on supersingular hyperelliptic curves over finite fields. In [4], Castryck-Decru-Smith constructed hash functions by Richelot isogenies between superspecial abelian varieties of dimension two as a generalization of hash functions in [5].

It is important to study the structure of these graphs, especially the neighborhoods of a fixed vertex since the security of isogeny-based cryptosystems depends the properties of the supersingular isogeny graphs.

In the supersingular elliptic curve case, the isogeny graph over $\mathbb{F}_p$ was constructed in [11]. Adj-Ahmadi-Menezes [1] described the subgraphs with trace 0 or $\pm p$. The authors (with S. Li) clarified the local structure of the isogeny graph at $\mathbb{F}_p$-vertices (i.e. whose j-invariants are inside $\mathbb{F}_p$) in [33,27,26]. As there is no effective way to describe explicitly the endomorphism rings of supersingular elliptic curves defined over $\mathbb{F}_{p^2}\backslash\mathbb{F}_p$, it is still an open problem to obtain generalized results of the local structure at these vertices for any p and ℓ.

Now let us move on to the higher dimension case, in particular the abelian surfaces case (the dimension 2 case). Ionica and Thomé [20] described the structure of the isogeny graph of ordinary abelian surfaces. Katsura and Takashima [24,25,37] obtained the number of Richelot isogenies from superspecial abelian surfaces to products of supersingular curves. Florit and Smith [14,15] classified the Richelot isogenies between superspecial abelian surfaces. In [22,23], Jordan and Zaytman summarized the relationship between matrices of maximal orders of quaternion algebras and isogenies of principally polarized superspecial abelian varieties (PPSSAV in short), defined the big and little isogeny graphs of PPSSAV and studied their structures. Moreover, the method to find a path and the concept of multiradical isogenies have been extended to the case of abelian surfaces in [8,3].

Note that the recent break of SIDH [2,29,34] is based on the fact that the secret key can be recovered by constructing an isogeny from an abelian surface with information extracted from the given torsion points. This indicates that understanding the isogeny (graph) of abelian surfaces could also be very useful in studying the supersingular isogeny cryptosystems.

For two supersingular elliptic curves E and E' defined over $\mathbb{F}_{p^2}$, let $[E \times E']$ be the superspecial abelian surface with the principal polarization $\{0\} \times E' + E \times \{0\}$. In this article, we determine local structure of the vertices $[E \times E']$ in the (ℓ, ℓ)-isogeny graph of principally polarized superspecial abelian surfaces where either E or E' is defined over $\mathbb{F}_p$. Previously, Florit and Smith [14,15] partitioned vertices in the graph into several types and computed the number of edges connecting to each type in the $(2,2)$-isogeny graph. Here we treat the general case $\ell \geq 2$ and obtain the numbers of edges connecting to any adjacent vertex rather than its type and also determine the structure of the associated isogeny kernels. We obtain our results by classifying the action of automorphism groups on the kernels of isogenies.

The paper is organized as follows. In §2 we recall basic results about principally polarized superspecial abelian varieties/surfaces and the associated (ℓ, ℓ)-isogeny graphs. We study the loops and neighborhoods of $[E \times E']$ in the cases (i) $E = E' = E_{1728}$, (ii) $E = E' = E_0$, (iii) $j(E) \in \mathbb{F}_p \backslash \{0, 1728\}$ and $j(E') \neq j(E)$, (iv) $j(E) \in \mathbb{F}_p \backslash \{0, 1728\}$ and $E' = E$ in §3-§6 respectively. We present a simple new proof of the main theorem in [26] in §7.

2. Preliminaries

Throughout this paper we assume that p is a prime number and k is a finite field of characteristic p. Let $\bar{\mathbb{F}}_p$ be an algebraic closure of k. We assume the abelian varieties are defined over $\bar{\mathbb{F}}_p$.

2.1. Principally polarized abelian varieties

We recall a few facts about principally polarized abelian varieties.

Let A be an abelian variety defined over k. Then a divisor D determines an isogeny $\lambda_D : A \to \hat{A}$, the dual abelian variety of A. If D is an ample divisor, then λ_D is a polarization on A. If moreover $\deg(\lambda_D) = 1$, then λ_D is a principal polarization of A and $\mathcal{A} = (A, D)$ is called a principally polarized abelian variety (PPAV in short).

For $m \in \mathbb{Z}_+$, let $A[m]$ be the m-torsion subgroup of A. If m is prime to p, a subgroup S of $A[m]$ is called maximal m-isotropic if it is maximal among subgroups T of $A[m]$ such that the restriction of the Weil pairing $e_m : A[m] \times A[m] \to \mu_m$ on $T \times T$ is trivial.

The following result in §23 of [31] implies that the kernel of an isogeny between principally polarized abelian varieties is a maximal isotropic subgroup:

Theorem 2.1. *Let (A, D) be a principally polarized abelian variety over $\overline{\mathbb{F}}_p$ and S be a subgroup of $A[m]$. Denote by $\phi : A \to A' = A/S$ the isogeny with kernel S. Then there exists a principally polarized divisor D' of A' such that $\phi^* D' \sim mD$ if and only if S is a maximal m-isotropic subgroup. Particularly, if S is a maximal m-isotropic subgroup of $A[m]$, then (A', D') is also a principally polarized abelian variety.*

By the above result, if φ is an isogeny between a principally polarized abelian variety (A, D) and an abelian variety A', and $\ker(\varphi)$ is a maximal m-isotropic subgroup, then A' also has a structure of principal polarization.

Suppose $p > 3$ and ℓ is a prime different from p. The following result in [13] presents the types of maximal ℓ^n-isotropic subgroups.

Proposition 2.2. *Let $\mathcal{A} = (A, D)$ be a principally polarized abelian surface. Then there are two types of maximal ℓ^n-isotropic subgroups in $A[\ell^n]$:*

(1) $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$,
(2) $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^{n-k}\mathbb{Z} \times \mathbb{Z}/\ell^k\mathbb{Z}$ *with* $0 \le k \le \lfloor \frac{n}{2} \rfloor$.

The number of maximal ℓ^n-isotropic subgroup is equal to $\ell^{2n-3}(\ell^2+1)(\ell+1)(\ell^n+\frac{\ell^{n-1}-1}{\ell-1})$.

In particular, for $n = 1$, there are $(\ell + 1)(\ell^2 + 1)$ maximal ℓ-isotropic subgroups, all of the form $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

2.2. Superspecial abelian varieties

A supersingular abelian variety A over $\bar{\mathbb{F}}_p$ is an abelian variety isogenous to a product of supersingular elliptic curves. A superspecial abelian variety A is a supersingular abelian variety that is isomorphic to a product of supersingular elliptic curves.

By definition, superspecial = supersingular in the elliptic curve case. There are many (if p is large enough) non-isomorphic supersingular elliptic curves over $\bar{\mathbb{F}}_p$. However, there is only one (up to isomorphism) superspecial abelian variety for each dimension $g > 1$ by the following famous result:

Theorem 2.3 *(Deligne, Ogus [32], Oort, Shioda [35]). Any superspecial abelian variety $A/\bar{\mathbb{F}}_p$ of dimension $g > 1$ is isomorphic to E^g, where E is an arbitrary supersingular elliptic curve over $\bar{\mathbb{F}}_p$.*

2.3. Principally polarized superspecial abelian varieties

Assigning a principal polarization to the superspecial abelian variety (when the dimension $g > 1$ is fixed), we obtain a principally polarized superspecial abelian variety (PPSSAV in short) and in particular a principally polarized superspecial abelian surface (PPSSAS in short) when $g = 2$. Different principal polarization gives different PPSSAV. For example, the product $E_1 \times E_2$ of supersingular elliptic curves, with the principal polarization divisor $\{0\} \times E_2 + +E_1 \times \{0\}$, is a PPSSAV.

For abelian surfaces, the following is well-known in [4, Proposition 2]:

Theorem 2.4. *There are two types of* PPSSAS *over $\bar{\mathbb{F}}_p$:*

(1) *Jacobian type $\mathcal{J}_p$, consisting of Jacobians of superspecial hyperelliptic curve of genus 2 with the canonical principal polarization, whose number is*

$$\#\mathcal{J}_p = \begin{cases} 0, & \text{if } p = 2, 3, \\ 1, & \text{if } p = 5, \\ \dfrac{p^3 + 24p^2 + 141p - 346}{2880}, & \text{if } p > 5. \end{cases}$$

(2) *Product type $\mathcal{E}_p$: consisting of products of two supersingular elliptic curves with the above principal polarization, whose number is*

$$\#\mathcal{E}_p = \begin{cases} 1, & \text{if } p = 2, 3, 5, \\ \frac{1}{2} S_{p^2}(S_{p^2} + 1), & \text{if } p > 5, \end{cases}$$

where S_{p^2} is the number of isomorphism classes of supersingular elliptic curves over $\bar{\mathbb{F}}_p$.

2.4. Relationship between isogenies and matrices

Let E be a fixed supersingular elliptic curve. It is well-known in §5 in [36] that $\mathcal{O} := \mathrm{End}(E)$ is a maximal order in the quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified only at p and ∞.

Suppose $g > 1$. Then E^g is a superspecial abelian variety of dimension g, equipped with the principal polarization $\{0\} \times E^{g-1} + \cdots + E^{g-1} \times \{0\}$. We have $\mathrm{End}(E^g) = M_g(\mathcal{O})$ and

$$\mathrm{Aut}(E^g) = \mathrm{GL}_g(\mathcal{O}) = \{M \in M_g(\mathcal{O}) \mid M \text{ is invertible}\}.$$

The reduced norm $\mathrm{Nrd} : \mathcal{O} \to \mathbb{Z}$ induces the reduced norm $\mathrm{Nrd} : M_g(\mathcal{O}) \to \mathbb{Z}$. Then we also have

$$\mathrm{GL}_g(\mathcal{O}) = \{M \in M_g(\mathcal{O}) \mid \mathrm{Nrd}(M) = 1\}.$$

Let A be a superspecial abelian variety of dimension g. By Theorem 2.3, E^g and A are isomorphic. Let $\iota_A : A \to E^g$ be a fixed isomorphism which induces $\iota_A : \mathrm{End}(A) \cong M_g(\mathcal{O})$. Note that another isomorphism ι'_A is uniquely determined by $\iota'_A \iota_A^{-1} \in \mathrm{GL}_g(\mathcal{O})$.

For $M \in M_g(\mathcal{O})$, let M^+ denote the conjugate transpose of M. If M is associated to the endomorphism $\alpha \in \mathrm{End}(A)$, then M^+ is the matrix associated to the Rosati involution $\alpha^\dagger$ of α.

Suppose X is a principal polarized divisor of A. The map

$$\mathrm{Pic}(A) \to \mathrm{End}(A), \quad L \mapsto \lambda_X^{-1} \circ \lambda_L$$

factors through the Néron-Severi group $\mathrm{NS}(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$. Let

$$j : \mathrm{NS}(A) \to \mathrm{End}(A) \cong M_g(\mathcal{O}); \qquad \overline{L} \to \iota_A(\lambda_X^{-1} \circ \lambda_L). \tag{1}$$

This map extends to $j : \mathrm{NS}(A) \otimes \mathbb{Q} \to \mathrm{End}(A) \otimes \mathbb{Q} \cong M_g(\mathcal{O}) \otimes \mathbb{Q}$.

Proposition 2.5. [30, Proposition 14.2] *The map j is invariant under the Rosati involution, which implies that*

$$j(\bar{L}) = j(\bar{L})^+,$$

and hence $j(\bar{L})$ is Hermitian.

The following result allows us to determine whether a divisor of an abelian variety corresponds to a (principal) polarization.

Proposition 2.6. [19, Proposition 2.8] *Let L be a divisor of an abelian variety A of dimension g. Then*

$$\frac{L^g}{g!} = \chi(L) = \mathrm{Nrd}(j(\bar{L})), \qquad \chi(L)^2 = \deg(\lambda_L),$$

and

(1) *L is associated to a polarization (i.e. L is an ample divisor) if and only if $j(\bar{L})$ is positive definite;*
(2) *L is associated to a principal polarization if and only if $j(\bar{L})$ is positive definite with reduced norm 1.*

Different choices of the isomorphism ι_A give different $j(\bar{L}) \in M_g(\mathcal{O})$, but they are related by the following result:

Proposition 2.7. [22, Proposition 31] *Let*

$$\mathcal{H} = \{H \in M_n(\mathcal{O}) \mid H \textit{ is positive-definite Hermitian of reduced norm } 1\}.$$

Two matrices H and H' in $\mathcal{H}$ correspond to the same polarized divisor if and only if they are in the same orbit under the action of $\mathrm{GL}_g(\mathcal{O})$ on the set $\mathcal{H}$:

$$\mathrm{GL}_g(\mathcal{O}) \times \mathcal{H} \to \mathcal{H}; \quad (M, H) \mapsto M^+ H M.$$

Moreover, there is a one-to-one correspondence between $\mathcal{H}/\mathrm{GL}_g(\mathcal{O})$ and the set of isomorphism classes of PPSSAS of dimension g.

Applying the above results to the case $g = 2$, we have

Proposition 2.8. [19, Corollary 2.9] *For $g = 2$ and $d \in \mathbb{Z}_+$, there is a one-to-one correspondence*

$$\begin{array}{ccc} \{\bar{L} \in \mathrm{NS}(A) \mid L > 0, L^2 = 2d\} & \to & \left\{ \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \in M_2(\mathcal{O}) \mid a, c \in \mathbb{Z}_+, ac - b\bar{b} = d \right\} \\ \bar{L} & \mapsto & j(\bar{L}). \end{array}$$

2.5. The (ℓ, ℓ)-isogeny graph of PPSSAS

From now on, suppose $p > 3$ and ℓ is a prime different from p. Suppose $g = 2$, i.e. we are dealing with abelian surfaces.

Let $\mathcal{A}_1 = (A, D_1)$ and $\mathcal{A}_2 = (A, D_2)$ be two principally polarized abelian surfaces over $\overline{\mathbb{F}}_p$. An (ℓ, ℓ)-isogeny is an isogeny $\phi : \mathcal{A}_1 \to \mathcal{A}_2$ such that $\ker(\phi) \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. For an (ℓ, ℓ) isogeny ϕ, there exists a dual isogeny $\hat{\phi} : \mathcal{A}_2 \to \mathcal{A}_1$ such that $\hat{\phi} \circ \phi = [\ell]$.

We can describe (ℓ, ℓ) isogenies using matrices in $M_2(\mathcal{O})$ in the following proposition, whose proof was given in [22, Proposition 31].

Proposition 2.9. *Let A be a superspecial abelian surface, P_1 and P_2 be two principal polarizations of A. Let $H_1 = j(\bar{P}_1)$ and $H_2 = j(\bar{P}_2)$. If $\alpha : A \to A$ is an isogeny of degree ℓ^{2m} associated to $M \in M_2(\mathcal{O})$, then $\alpha^*(P_2) = \ell^m P_1$ if and only if $M^+ H_2 M = \ell^m H_1$, and in this case, α is an isogeny from (A, P_1) to (A, P_2).*

We say two (ℓ, ℓ)-isogenies are equivalent if they have the same kernel.

Definition 2.10. The (ℓ, ℓ)-isogeny graph of principally polarized superspecial abelian surfaces, denoted as $\mathcal{G}_p = \mathcal{G}_{p,\ell}$, is the graph whose vertices set V is the set of $\overline{\mathbb{F}}_p$-isomorphism classes of PPSSAS and whose edges set E is the set of equivalence classes of (ℓ, ℓ)-isogenies.

By Theorem 2.1 and Proposition 2.2, the number of non-equivalent (ℓ, ℓ)-isogenies from a principally polarized superspecial abelian surface A to another is equal to the number of maximal ℓ-isotropic subgroups of A, which is $(\ell + 1)(\ell^2 + 1)$. Hence

Lemma 2.11. *The out-degree of every vertex in $\mathcal{G}_p$ is $(\ell + 1)(\ell^2 + 1)$.*

Definition 2.12. Let $\varphi : E_1 \times E_2 \to A_1$ be an edge in $\mathcal{G}_p$.

If $\{(P, Q), (P', Q')\}$ is an $\mathbb{F}_\ell$-basis of $\ker(\varphi)$, we call $\begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix}$ a generator matrix of $\ker(\varphi)$. The isogeny φ is called diagonal if $\ker(\varphi)$ has a diagonal generator matrix, and is called non-diagonal if otherwise.

Lemma 2.13. *Let $\varphi : E_1 \times E_2 \to A_1$ be an edge in $\mathcal{G}_p$. For $i = 1, 2$, let $K_i = \operatorname{im}(\ker(\varphi) \hookrightarrow (E_1 \times E_2)[\ell] \to E_i[\ell])$. Then the following are equivalent:*

(i) *φ is diagonal.*
(ii) $\dim K_1 = 1$.
(iii) $\dim K_2 = 1$.
(iv) *There exists some $0 \neq P \in E_1[\ell]$ such that $(P, 0) \in \ker(\varphi)$.*
(v) *There exists some $0 \neq Q \in E_2[\ell]$ such that $(0, Q) \in \ker(\varphi)$.*

In this case $\ker(\varphi) = K_1 \times K_2$.

Proof. If φ is diagonal, clearly $\dim K_1 = \dim K_2 = 1$ and $\ker(\varphi) = K_1 \times K_2$ by definition.

Suppose $\{(P, Q), (P', Q')\}$ is a basis of $\ker(\varphi)$ over $\mathbb{F}_\ell$.

If $\dim K_1 = 1$, then P and P' are linearly dependent and not both zero. We may assume $P' = aP$ and replace Q' by $Q' - aQ$, (P', Q') by $(0, Q')$, then $\ker(\varphi)$ has a basis of the form $\{(P, Q), (0, Q')\}$ and in particular $Q' \neq 0$. Since $\ker(\varphi)$ is a maximal isotropic subgroup, the trivial Weil pairing $e_\ell((P, Q), (0, Q')) = e_\ell(P, 0)e_\ell(Q, Q') = 1$ means $e(Q, Q') = 1$. Then Q and Q' must be linearly dependent too. Thus $K_2 = \langle Q' \rangle$, $\ker(\varphi) = K_1 \times K_2$ has a basis of the form $\{(P, 0), (0, Q')\}$ and φ is diagonal.

By symmetry, if $\dim K_2 = 1$, we also have $\dim K_1 = 1$, $\ker(\varphi) = K_1 \times K_2$ and φ is diagonal. Thus (i), (ii), (iii) are equivalent.

Clearly (i) $\Rightarrow$ (iv). On the other hand, we extend $(P, 0)$ to a basis $\{(P, 0), (P', Q')\}$ of $\ker(\varphi)$. Then K_2 is 1-dimensional. Hence we have (iv) $\Rightarrow$ (i). Similarly we have (i) $\Leftrightarrow$ (v). □

Corollary 2.14. *Among isogenies from $E_1 \times E_2$ in $\mathcal{G}_p$, $(\ell + 1)^2$ are diagonal and $\ell^3 - \ell$ are non-diagonal.*

Proof. There are $\ell+1$ choices for the 1-dimensional subspaces K_1 of $E_1[\ell]$ and K_2 of $E_1[\ell]$ respectively, so there are $(\ell+1)^2$ diagonal isogenies and $(\ell+1)(\ell^2+1) - (\ell+1)^2 = \ell^3 - \ell$ non-diagonal ones. □

As in [4], we can define the extension of (ℓ, ℓ)- isogenies:

Definition 2.15. Let $\mathcal{A}_i = (A, D_i)$ $(i = 0, 1, 2)$, $\varphi_1 : \mathcal{A}_0 \to \mathcal{A}_1$ and $\varphi_2 : \mathcal{A}_1 \to \mathcal{A}_2$ be vertices and edges in $\mathcal{G}_p$.

(1) The isogeny φ_2 is called a dual extension of φ_1 if $\ker(\varphi_2 \circ \varphi_1) \cong (\mathbb{Z}/\ell\mathbb{Z})^4$, in this case, $\ker(\varphi_2) = \varphi_1(A[\ell])$.
(2) The isogeny φ_2 is called a bad extension of φ_1 if $\ker(\varphi_2 \circ \varphi_1) \cong \mathbb{Z}/\ell^2\mathbb{Z} \times (\mathbb{Z}/\ell\mathbb{Z})^2$, in this case, $\ker(\varphi_2) \cap \varphi_1(A[\ell]) \cong \mathbb{Z}/\ell\mathbb{Z}$.
(3) The isogeny φ_2 is called a good extension of φ_1 if $\ker(\varphi_2 \circ \varphi_1) \cong (\mathbb{Z}/\ell^2\mathbb{Z})^2$, in this case, $\ker(\varphi_2) \cap \varphi_1(A[\ell]) = 0$.

3. Loops and neighborhoods of $[E_{1728} \times E_{1728}]$

3.1. Basic facts

For the forms of endomorphism rings of supersingular elliptic curves, we refer the reader to [28]. In this section, let $E = E_{1728}$ be the supersingular elliptic curve defined over $\mathbb{F}_p$ with j-invariant 1728 (which implies that $p \equiv 3 \bmod 4$). We know its endomorphism ring is

$$\mathcal{O} = \mathcal{O}_{1728} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2},$$

where $i^2 = -1,\ j^2 = -p,\ ij = -ji = k$. Note that the reduced norm on $\mathcal{O}$ is given by

$$\mathrm{Nrd}\left(x + yi + z\frac{1+j}{2} + w\frac{i+k}{2}\right) = \left(x + \frac{z}{2}\right)^2 + \left(y + \frac{w}{2}\right)^2 + \frac{p(z^2+w^2)}{4}. \quad (2)$$

Let $[E \times E] = [E_{1728} \times E_{1728}]$ be the superspecial abelian surface $E \times E$ with the principal polarization $\{0\} \times E + E \times \{0\}$ in the isogeny graph $\mathcal{G}_p$.

For $n \in \mathbb{Q}^\times$, let $\sigma(n) = \sigma_1(n)$ be the sum of positive divisors of n if $n \in \mathbb{Z}_+$ and $\sigma(n) = 0$ if otherwise. Recall

Lemma 3.1 *(Jacobi).* [10, §1.2] *For $n \in \mathbb{Z}_+$, the number of integer solutions of $x^2 + y^2 + z^2 + w^2 = n$ is*

$$8\sigma(n) - 32\sigma(\frac{n}{4}) = 8 \sum_{d \mid n,\ 4 \nmid d} d.$$

Particularly, there are 24 integer solutions of $x^2 + y^2 + z^2 + w^2 = 2$.

Let $G = \mathrm{Aut}(E \times E)$. By simple computation, we have

Lemma 3.2. *The group G is the following group of order 32:*

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},\quad \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \;\middle|\; a, b = \pm 1, \pm i \right\}. \quad (3)$$

We shall need the following notations in this section:

(i) If $\ell \equiv 1 \bmod 4$, let

  (a) $\lambda := x_\ell + y_\ell i \in \mathbb{Z}[i]$ such that $x_\ell^2 + y_\ell^2 = \ell$;
  (b) $L_1 := \ker(\lambda : E[\ell] \to E[\ell])$ and $L_2 := \ker(\bar{\lambda} : E[\ell] \to E[\ell])$;
  (c) $R \in L_1 \backslash \{0\}$ and $R' \in L_2 \backslash \{0\}$;

(d) $t := -x_\ell/y_\ell \in \mathbb{F}_\ell$. Hence $t^2+1=0$, and $i(R)=tR$, $i(R')=-tR'$.

(ii) Let $S = R+R' \in E[\ell]$ if $\ell \equiv 1 \bmod 4$ and S be any fixed nonzero $P \in E[\ell]$ if $\ell \equiv 3 \bmod 4$. Let $S^* = i(S)$, since R, R' are linearly independent, so are S and S^*.

(iii) Let $G = \mathrm{Aut}(E \times E)$.

(iv) For an isogeny φ starting from $E \times E$, let $G_\varphi = \{g \in G : \varphi g = \varphi\}$ be the stabilizer of φ by the G-action, and $O_\varphi = \{\varphi g : g \in G\}$ be the G-orbit of φ.

Note that L_1 and L_2 are the only 1-dimensional invariant $\mathbb{F}_\ell$-subspaces of the operator i on $E[\ell]$, with eigenvalues t and $-t$ respectively.

3.2. Kernels of (ℓ,ℓ)-isogenies from $E_{1728} \times E_{1728}$

Lemma 3.3. *The set $\{S, S^*\}$ is an $\mathbb{F}_\ell$-basis of $E[\ell]$.*

Proof. If $\ell \equiv 3 \mod 4$, we claim that $0 \neq P$ and $i(P)$ are linearly independent. Indeed, if $i(P) = cP$ for some $c \in \mathbb{F}_\ell$, then $(i-c)(P)=0$. Hence we have $\ell \mid \mathrm{Nrd}(i-c) = 1+c^2$, it means $1+c^2=0$ in $\mathbb{F}_\ell$, which is impossible.

If $\ell \equiv 1 \bmod 4$, then $S = R+R'$ and $S^* = i(R+R') = tR - tR'$. The points R and R' are linearly independent, so are S and S^*. □

Proposition 3.4. *There is a one-to-one correspondence of the set of non-diagonal (ℓ,ℓ)-isogenies from $E \times E$ and the set of generator matrices*

$$\left\{ \begin{pmatrix} S & S^* \\ aS+bS^* & cS+dS^* \end{pmatrix} : a,b,c,d \in \mathbb{F}_\ell, ad-bc=-1 \right\}.$$

Proof. Since both sets are of order $\ell(\ell^2-1) = \ell^3-\ell$, it suffices to show a non-diagonal isogeny has a generator matrix of the above form.

Let φ be a non-diagonal (ℓ,ℓ)-isogeny. Suppose $\{(P,Q),(P',Q')\}$ is a basis of $\ker(\varphi)$ over $\mathbb{F}_\ell$. Then $\{P,P'\}$, $\{Q,Q'\}$ and $\{S,S^*\}$ are all bases of $E[\ell]$ by Lemma 2.13 and Lemma 3.3. Suppose $S = a_1P+b_1P'$ and $S^* = i(S) = c_1P+d_1P'$. Let $a_1Q+b_1Q' = aS+bS^*$, $c_1Q+d_1Q' = cS+dS^*$. Then $\{(S, aS+bS^*), (S^*, cS+dS^*)\}$ is a new basis of $\ker(\varphi)$. To ensure $\ker(\varphi)$ is a maximal isotropic subgroup, we have $e_\ell(S,S^*)e_\ell(aS+bS^*, cS+dS^*) = 1$. This implies $ad-bc+1 \equiv 0 \pmod{\ell}$. □

Definition 3.5. For a non-diagonal (ℓ,ℓ)-isogeny φ from $E \times E$, we call $\{a,b,c,d\}$ given above the quadruple associated to φ.

We now describe the action of $G = \mathrm{Aut}(E \times E)$ on the isogenies explicitly. For the diagonal isogenies, by easy computation, we have

Lemma 3.6. *Suppose* $\ker(\varphi) = K_1 \times K_2$. *Then* $g\ker(\varphi) = \ker(\varphi g^{-1})$ *for each $g \in G$ is given in the following table:*

g	$g\ker(\varphi)$	g	$g\ker(\varphi)$
$\begin{pmatrix} \pm1 & 0 \\ 0 & \pm1 \end{pmatrix}$	$K_1 \times K_2$	$\begin{pmatrix} \pm1 & 0 \\ 0 & \pm i \end{pmatrix}$	$K_1 \times i(K_2)$
$\begin{pmatrix} \pm i & 0 \\ 0 & \pm1 \end{pmatrix}$	$i(K_1) \times K_2$	$\begin{pmatrix} \pm i & 0 \\ 0 & \pm i \end{pmatrix}$	$i(K_1) \times i(K_2)$
$\begin{pmatrix} 0 & \pm1 \\ \pm1 & 0 \end{pmatrix}$	$K_2 \times K_1$	$\begin{pmatrix} 0 & \pm1 \\ \pm i & 0 \end{pmatrix}$	$K_2 \times i(K_1)$
$\begin{pmatrix} 0 & \pm i \\ \pm1 & 0 \end{pmatrix}$	$i(K_2) \times K_1$	$\begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix}$	$i(K_2) \times i(K_1)$

Here and later we mean $g \in \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\}$ *for* $g = \begin{pmatrix} \pm1 & 0 \\ 0 & \pm1 \end{pmatrix}$.

Consequently, we have

Proposition 3.7. *Diagonal isogenies can be divided into the following classes, which are unions of G-orbits:*

- **(D1)** $(K_1, K_2) = (L_1, L_1)$ *or* (L_2, L_2), *where* $G_\varphi = G$ *and* $O_\varphi = \{\varphi\}$.
- **(D2)** $(K_1, K_2) = (L_1, L_2)$ *or* (L_2, L_1), *which form* 1 *orbit if* $\ell \equiv 1 \bmod 4$.
- **(D3)** *Exactly one of* K_1, K_2 *is in* $\{L_1, L_2\}$, *where* $|G_\varphi| = 8$ *and* $|O_\varphi| = 4$. *This class contains* $4(\ell-1)$ *isogenies if* $\ell \equiv 1 \bmod 4$.
- **(D4)** $K_1 \notin \{L_1, L_2\}$ *and* $K_2 \in \{K_1, i(K_1)\}$, *where* $|G_\varphi| = 8$ *and* $|O_\varphi| = 4$. *This class contains* $2(\ell-1)$ *isogenies if* $\ell \equiv 1 \bmod 4$, *and* $2(\ell+1)$ *isogenies if* $\ell \equiv 3 \bmod 4$.
- **(D5)** $K_1 \notin \{L_1, L_2\}$ *and* $K_2 \notin \{L_1, L_2, K_1, i(K_1)\}$, *where* $G_\varphi = \{\begin{pmatrix} \pm1 & 0 \\ 0 & \pm1 \end{pmatrix}\}$ *and* $|O_\varphi| = 8$. *This class contains* $(\ell-1)(\ell-3)$ *isogenies if* $\ell \equiv 1 \bmod 4$, *and* $\ell^2 - 1$ *isogenies if* $\ell \equiv 3 \bmod 4$.

For the non-diagonal isogenies, we have

Lemma 3.8. *Suppose φ is non-diagonal associated to the quadruple $\{a, b, c, d\}$. Then for each $g \in G$, the associated quadruple of $\pm\varphi g^{-1}$ is given in the following table:*

g	*quadruple*	g	*quadruple*	g	*quadruple*
$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\{-a,-b,-c,-d\}$	$\begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$	$\{d,-c,-b,a\}$	$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$	$\{-d,c,b,-a\}$
$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\{d,-b,-c,a\}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\{-d,b,c,-a\}$	$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$	$\{-a,-c,-b,-d\}$
$\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$	$\{a,c,b,d\}$	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	$\{-b,a,-d,c\}$	$\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$	$\{b,-a,d,-c\}$
$\begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}$	$\{-c,-d,a,b\}$	$\begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}$	$\{c,d,-a,-b\}$	$\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}$	$\{-c,a,-d,b\}$
$\begin{pmatrix} 0 & i \\ -1 & 0 \end{pmatrix}$	$\{c,-a,d,-b\}$	$\begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}$	$\{-b,-d,a,c\}$	$\begin{pmatrix} 0 & 1 \\ -i & 0 \end{pmatrix}$	$\{b,d,-a,-c\}$

Proof. We first show the case for $g = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$. In this case,

$$\begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} S & S^* \\ aS + bS^* & cS + dS^* \end{pmatrix} = \begin{pmatrix} S^* & -S \\ -bS + aS^* & -dS + cS^* \end{pmatrix},$$

hence $\{(S, dS - cS^*), (S^*. -bS + aS^*)\}$ is a basis for $\begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}\varphi$, thus the associated quadruple is $\{d, -c, -b, a\}$.

We then show the case for $g = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$. In this case,

$$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} S & S^* \\ aS + bS^* & cS + dS^* \end{pmatrix} = \begin{pmatrix} aS^* - bS & cS^* - dS \\ S^* & -S \end{pmatrix}.$$

Note that

$$a \begin{pmatrix} cS^* - dS \\ -S \end{pmatrix} - c \begin{pmatrix} aS^* - bS \\ S^* \end{pmatrix} = \begin{pmatrix} S \\ -aS - cS^* \end{pmatrix},$$
$$b \begin{pmatrix} cS^* - dS \\ -S \end{pmatrix} - d \begin{pmatrix} aS^* - bS \\ S^* \end{pmatrix} = \begin{pmatrix} S^* \\ -bS - dS^* \end{pmatrix},$$

hence $\{(S, -aS - cS^*), (S^*, -bS - dS^*)\}$ is a basis for $\left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)\varphi$, thus the associated quadruple is $\{-a, -c, -b, -d\}$.

All other cases are similar. □

For every g, by looking for all φ fixed by g in the above table, we get

Proposition 3.9. *Non-diagonal isogenies can be divided into the following classes, which are unions of G-orbits:*

(**N1**) $\{a, b, c, d\} = \{a, b, -b, a\}$*:*

- (i) $b = \pm a$, *where* $|G_\varphi| = 8$ *and* $|O_\varphi| = 4$,
- (ii) $a = 0$ *or* $b = 0$, *where* $|G_\varphi| = 8$ *and* $|O_\varphi| = 4$,
- (iii) *other cases of this form, where* $G_\varphi = \{\pm I_2, \pm iI_2\}$ *and* $|O_\varphi| = 8$.

This class contains $\ell - 1$ *isogenies if* $\ell \equiv 1 \bmod 4$ *and* $\ell + 1$ *isogenies if* $\ell \equiv 3 \bmod 4$.

(**N2**) $\{a, b, c, d\} = \{a, b, b, -a\}$, *where* $|G_\varphi| = 8$ *and* $|O_\varphi| = 4$. *This class contains* $\ell - 1$ *isogenies if* $\ell \equiv 1 \bmod 4$ *and* $\ell + 1$ *isogenies if* $\ell \equiv 3 \bmod 4$.

(**N3**) $\{a, b, c, d\} = \{a, b, c, -a\}$, $c \neq b$ *and* $c \neq -b$ *if* $a = 0$, *or* $\{a, b, c, d\} = \{a, b, b, d\}$, $d \neq -a$ *and* $d \neq a$ *if* $b = 0$, *where* $|G_\varphi| = 4$ *and* $|O_\varphi| = 8$. *This class contains* $2(\ell^2 - 1)$ *isogenies.*

(**N4**) *all other cases, where* $G_\varphi = \{\pm I_2\}$ *and* $|O_\varphi| = 16$. *This class contains* $(\ell - 1)(\ell^2 - \ell - 4)$ *isogenies if* $\ell \equiv 1 \bmod 4$ *and* $\ell(\ell + 1)(\ell - 3)$ *isogenies if* $\ell \equiv 3 \bmod 4$.

Proof. We only need to count the number of isogenies in each class.

First for a fixed $c \in \mathbb{F}_\ell^\times$, the equation $a^2 + b^2 = c$ has $\ell - 1$ pairs of solutions in $\mathbb{F}_\ell$ if $\ell \equiv 1 \bmod 4$ and $\ell + 1$ pairs if $\ell \equiv 3 \bmod 4$. Take $c = \pm 1$, we get the orders of Classes **N1** and **N2**.

For Class **N3**, we need to find the solutions of $a^2 + bc = 1 (b \neq c, b \neq -c$ if $a = 0)$ and $b^2 - ad = 1 (a \neq -d, a \neq d$ if $b = 0)$. Consider the first one:

(1) if $a = \pm 1$, then we can take either $b = 0$ or $c = 0$, there are $4\ell - 2$ solutions of this type;
(2) if $a \neq \pm 1$, then $1 - a^2 \neq 0$, there are $\ell - 1$ pairs of b, c such that $bc = 1 - a^2$, so there are $(\ell - 2)(\ell - 1)$ solutions of this type;
(3) we need to exclude the $b = c$ case, which counts for $\ell - 1$ solutions if $\ell \equiv 1 \bmod 4$ and $\ell + 1$ solutions if $\ell \equiv 3 \bmod 4$;
(4) we also need to exclude the $\{0, b, -b, 0\}$ case, then $b^2 = -1$, which has two solutions if $\ell \equiv 1 \bmod 4$ and none if $\ell \equiv 3 \bmod 4$;
(5) in conclusion, it has $\ell^2 - 1$ solutions.

Similarly the number of solutions for the second one is also $\ell^2 - 1$. Moreover, these two sets are disjoint, so Class **N3** has $2(\ell^2 - 1)$ elements.

Class **N4** follows from results for Classes **N1-N3** and Corollary 2.14 that the number of non-diagonal isogenies is $\ell^3 - \ell$. □

3.3. Loops at $[E_{1728} \times E_{1728}]$

Theorem 3.10. *Suppose* $p > 4\ell$.

(1) *If* $\ell \equiv 1 \bmod 4$, *then the set of loops of* $E \times E$ *is the union of Classes* $\mathbf{D1}, \mathbf{D2}$ *and* $\mathbf{N1}$.

(2) *If* $\ell \equiv 3 \bmod 4$, *then the set of loops of* $E \times E$ *is Class* $\mathbf{N1}$.

(3) *If* $\ell = 2$, *then* $E \times E$ *has* 3 *loops.*

Proof. Note that the principal polarized divisor $E \times \{0\} + \{0\} \times E$ corresponds to the identity matrix $I \in M_2(\mathcal{O})$. To determine the loops at $E \times E$ in the isogeny graph $\mathcal{G}_p$, it is equivalent to determine matrices $M \in M_2(\mathcal{O})$ such that $M^+M = \ell I$. Moreover, if M corresponds to φ, then $\ker \varphi = \{(P, Q) \in E \times E : M(P, Q)^T = 0\}$. Thus gM, where $g \in G$ given in Equation (3), determines the same loop as M does.
Now we prove cases (1) and (2). First assume ℓ is odd. Write

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad (a, b, c, d \in \mathcal{O}).$$

The equation $M^+M = \ell I$ implies

$$\mathrm{Nrd}(a) + \mathrm{Nrd}(b) = \ell, \quad \mathrm{Nrd}(c) + \mathrm{Nrd}(d) = \ell. \tag{4}$$

Denote $a = a_1 + a_2 i + a_3 \frac{1+j}{2} + a_4 \frac{i+k}{2}$. If a_3 and a_4 are not both zero, by Equation (2), then $\mathrm{Nrd}(a) \geq \frac{p}{4} > \ell$ since by assumption $p > 4\ell$, which contradicts Equation (4). Hence $a \in \mathbb{Z}[i]$. Similarly we have

$$a, b, c, d \in \mathbb{Z}[i].$$

Comparing the coefficients, we get

$$a\bar{a} + b\bar{b} = c\bar{c} + d\bar{d} = \ell, \quad \bar{a}c + \bar{b}d = 0. \tag{5}$$

Hence, the vector (c, d) is orthogonal to $(\bar{a}, \bar{b})$. Note that $(-\bar{b}, \bar{a})$ is also orthogonal to $(\bar{a}, \bar{b})$, we have $(c, d) = u(-\bar{b}, \bar{a})$ for some $u \in \mathbb{R}(i)$. By the identity $a\bar{a}+b\bar{b} = c\bar{c}+d\bar{d} = \ell$, we have $u \in \{\pm 1, \pm i\}$.

In this case, up to $g \in G$ we may assume $a = \bar{d}$, $b = -\bar{c}$, then

$$M = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}. \tag{6}$$

Write $a = a_1 + a_2 i$, $b = b_1 + b_2 i$. The equation $a\bar{a} + b\bar{b} = \ell$ implies

$${a_1}^2 + {a_2}^2 + {b_1}^2 + {b_2}^2 = \ell.$$

Now we reason by cases:

(i) If one of a, b is 0, up to an element $g \in G$, we may assume $b = 0$, then $c = 0$ and $a\bar{a} = d\bar{d} = \ell$, which can only happen if $\ell \equiv 1 \bmod 4$. In this case, M is one of the following matrices

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \begin{pmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{pmatrix}, \begin{pmatrix} \bar{\lambda} & 0 \\ 0 & \lambda \end{pmatrix}, \begin{pmatrix} \bar{\lambda} & 0 \\ 0 & \bar{\lambda} \end{pmatrix},$$

which correspond to the 4 isogenies in Classes **D1** and **D2**.
(ii) If $ab \neq 0$, by Lemma 3.1, the equation above has $8(\ell + 1)$ solutions if $\ell \equiv 3 \bmod 4$ and $8(\ell - 1)$ solutions if $\ell \equiv 1 \bmod 4$. Now if M is of the form Equation (6), then gM is also of this form exactly when

$$g \in \left\{ \pm I_2,\ \pm\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}.$$

Thus the number of non-diagonal loops is $\ell + 1$ if $\ell \equiv 3 \bmod 4$ and $\ell - 1$ if $\ell \equiv 1 \bmod 4$.

Finally let us compute the kernels in this case. Suppose M corresponds to the loop φ, then $(P, Q) \in \ker \varphi$ means $M(P, Q)^T = 0$. If $0 \neq P \in E[\ell]$, then $aP \neq 0$, otherwise $a\bar{a}P = 0$ and hence $P = 0$ as $\ell \nmid a\bar{a}$. So $(P, 0) \notin \ker \varphi$. Thus $\ker \varphi$ is non-diagonal. By Proposition 3.4, suppose $\ker \varphi$ is associated with $\{u, v, w, t\}$ with $ut - vw = -1$. Then

$$\begin{pmatrix} a & bi \\ \bar{b}i & \bar{a} \end{pmatrix} \begin{pmatrix} S & S^* \\ uS + vS^* & wS + tS^* \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Hence $(a + ubi - vb)(S) = (ai + wbi - tb)(S) = 0$. This implies $b(-u - vi - wi + t)(S) = 0$. Again by $\ell \nmid b\bar{b}$, we have $(-u - vi - wi + t)(S) = 0$. Since $\{S, i(S) = S^*\}$ is a basis of $E[\ell]$, we have $t = u$ and $w = -v$ in $\mathbb{F}_\ell$. In fact,

$$(u,v)=\left(\frac{a_1b_2-a_2b_1}{b_1^2+b_2^2},\frac{a_1b_1+a_2b_2}{b_1^2+b_2^2}\right).$$

Thus the loops here are exactly those contained in Class **N1**.

For case (3), we put $\ell=2$. By calculation there are 3 loops which correspond to the three matrices

$$\begin{pmatrix}1&1\\-1&1\end{pmatrix},\quad\begin{pmatrix}1&i\\i&1\end{pmatrix},\quad\begin{pmatrix}1+i&0\\0&1+i\end{pmatrix}.\quad\square$$

3.4. Neighbors of $[E_{1728}\times E_{1728}]$

In this subsection, we want to prove Theorems 3.16 and 3.17, for which we need more results about loops.

If $\ell\equiv 1 \bmod 4$, we denote the loops $\lambda\times\lambda$ and $\bar\lambda\times\bar\lambda$ on $E\times E$ by $[\lambda]$ and $[\bar\lambda]$ respectively. Hence

$$\ker[\lambda]=L_1\times L_1,\quad \ker[\bar\lambda]=L_2\times L_2.$$

Lemma 3.11. *Suppose* $\ell\equiv 1 \bmod 4$ *and* $p>4\ell$. *For a loop* $\alpha\neq[\lambda]$, $[\bar\lambda]$ *of* $E\times E$ *of degree* ℓ^2, *let*

$$L_i^\alpha=(L_i\times L_i)\cap\ker\alpha\quad(i=1,2).$$

Then $\alpha\mapsto L_i^\alpha$ *gives a one-to-one correspondence*

$$\{\textit{degree } \ell^2 \textit{ loops } \neq[\lambda] \textit{ or } [\bar\lambda]\}\leftrightarrow\{1\textit{-dimensional subspaces of } L_i\times L_i\}.$$

Consequently, $\ker\alpha=L_1^\alpha\times L_2^\alpha$, *and if* $L_1^\alpha=\{(P,kP):P\in L_1\}$ *for some* $k\neq 0$, *then* $L_2^\alpha=\{(-kQ,Q):Q\in L_2\}$.

Proof. We prove the one-to-one correspondence for $\alpha\leftrightarrow L_1^\alpha$. The case for $\alpha\leftrightarrow L_2^\alpha$ is parallel.

If $\ker\alpha=L_1\times L_2$ or $L_2\times L_1$, clearly $L_1^\alpha=L_1\times\{0\}$ or $\{0\}\times L_1$ which is 1-dimensional. Conversely these two lines correspond to these two diagonal kernels.

If α is non-diagonal, suppose it is associated to the quadruple $(u,v,-v,u)$ such that $u^2+v^2=-1$ (since $\ker(\alpha)\in(\mathbf{N1})$), then $(R,(u+vt)R)\in\ker\alpha\cap(L_1\times L_1)$ which must be one dimensional, where R and t are defined as in section 3.1.

On the other hand, we may assume the 1-dimensional subspace is generated by (R,kR) for some $k\neq 0$. By Theorem 3.10, we need to find a unique quadruple $(u,v,-v,u)$ such that $u^2+v^2=-1$ and $(R,kR)\in\langle(S,uS+vS^*),(S^*,-vS+uS^*)\rangle$. Note that $iR=tR$, $iR'=-tR'$, $S=R+R'$ and $S^*=tR-tR'$, where $t^2=-1$. Then

$$\begin{pmatrix} R \\ uR + vtR \end{pmatrix} = \frac{1}{2}\begin{pmatrix} S \\ uS + vS^* \end{pmatrix} - \frac{t}{2}\begin{pmatrix} S^* \\ -vS + uS^* \end{pmatrix}.$$

By Lemma 2.13, a non-diagonal kernel can not contain two elements of the form $(R, *)$, hence $u + vt = k$. Then $u^2 + v^2 = (u + vt)(u - vt) = -1$ and hence $u - vt = -k^{-1}$. There is a unique $(u, v) = (\frac{k-k^{-1}}{2}, \frac{k+k^{-1}}{2t})$ satisfying these conditions. We also see L_2^α in this case is the 1-dimensional subspace generated by $(R', -k^{-1}R')$ or equivalently by $(-kR', R')$. $\square$

Proposition 3.12. *Suppose $p > 4\ell^2$. Every loop φ of $E \times E$ of degree ℓ^4 corresponds to a matrix of the following form:*

(I) *ℓI_2. In this case $\ker\varphi \cong (\mathbb{Z}/\ell\mathbb{Z})^4$.*

(II) *$\begin{pmatrix} a & bi \\ \bar{b}i & \bar{a} \end{pmatrix}$, where $a, b \in \mathbb{Z}[i]$, $a\bar{a} + b\bar{b} = \ell^2$ and $ab \neq 0$. In this case $\ker(\varphi) \cong (\mathbb{Z}/\ell^2\mathbb{Z})^2$.*

(III) *$\lambda\begin{pmatrix} a & bi \\ \bar{b}i & \bar{a} \end{pmatrix}$ or $\bar{\lambda}\begin{pmatrix} a & bi \\ \bar{b}i & \bar{a} \end{pmatrix}$, where $a, b \in \mathbb{Z}[i]$ and $a\bar{a} + b\bar{b} = \ell$. In this case $\ker\varphi \cong (\mathbb{Z}/\ell\mathbb{Z})^2 \times \mathbb{Z}/\ell^2\mathbb{Z}$ which occurs only if $\ell \equiv 1 \bmod 4$.*

As a consequence, every loop of degree ℓ^4 can be factorized as the product of two loops of degree ℓ^2. Moreover, loops in Case II are uniquely factorized as the composition of two edges of degree ℓ^2.

Proof. Suppose M corresponds to φ. Then $M^+M = \ell^4 I$. If $p > 4\ell^2$, by following the same argument in the proof of Theorem 3.10, we can deduce that $M \in M_2(\mathbb{Z}[i])$ has the form of I, II or III.

Clearly a loop φ in Case I is the composition of α and $\hat{\alpha}$ where α is a loop of degree ℓ^2. It is also clear $\ker(\alpha) \cong (\mathbb{Z}/\ell\mathbb{Z})^4$.

A loop in Case III is the extension of $[\lambda]$ or $[\bar{\lambda}]$ of a non-diagonal loop α of degree ℓ^2. By Lemma 3.11, $L_1^\alpha \cong L_2^\alpha \cong \mathbb{Z}/\ell\mathbb{Z}$, thus this extension is bad and $\ker\varphi = \mathbb{Z}/\ell^2\mathbb{Z} \times (\mathbb{Z}/\ell\mathbb{Z})^2$.

Now let $\varphi = \alpha \circ \beta$ be a loop of degree ℓ^4 where α, β are two loops of degree ℓ^2 such that $\alpha, \beta \notin \{[\lambda], [\bar{\lambda}]\}$ and $\beta \neq \hat{\alpha}$.

We first claim that α is a good extension of β. If not, then α is a bad extension of β. Hence $\beta((E \times E)[\ell]) \cap \ker(\alpha) \cong \mathbb{Z}/\ell\mathbb{Z}$ is an $\mathbb{F}_\ell$-line generated by some $(P, Q) \in (E \times E)[\ell]$. Since $i \circ \beta = \beta \circ i$, we have

$$(i(P), i(Q)) \in i \circ \beta((E \times E)[\ell]) = \beta \circ i((E \times E)[\ell]) = \beta((E \times E)[\ell]).$$

Similarly, by $i \circ \alpha = \alpha \circ i$, we have $(i(P), i(Q)) \in \ker(\alpha)$. Hence $(i(P), i(Q)) = c(P, Q)$ for some $c \in \mathbb{F}_\ell$. This is impossible if $\ell \equiv 3 \bmod 4$. If $\ell \equiv 1 \bmod 4$, then both of P and Q are in either L_1 or L_2. Since $\beta((E \times E)[\ell]) \subseteq \ker(\hat{\beta})$, we have $(P, Q) \in \ker(\hat{\beta}) \cap \ker(\alpha)$. However, by Lemma 3.11, there is only one loop of degree ℓ^2 not of the form $[\lambda]$ whose kernel contains (P, Q), thus $\hat{\beta} = \alpha$, which is a contradiction.

We then show the factorization of φ as $\alpha \circ \beta$, where α and β are two edges of degree ℓ^2, is unique. Indeed, $\ker(\varphi) \cong (\mathbb{Z}/\ell^2\mathbb{Z})^2$ has a unique subgroup which is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$. This subgroup must be $\ker(\beta)$. Thus β is unique and so is α.

In conclusion, loops which is the composition of two loops $\neq [\lambda]$, $[\bar{\lambda}]$ and without backtracking are all in Case II, with kernels $\cong (\mathbb{Z}/\ell^2\mathbb{Z})^2$, and the number of such loops is $(\ell+1)\ell$. However, following the proof of Theorem 3.10, the number of loops of degree ℓ^4 in Case II is $\sigma(\ell^2) - 1 = \ell^2 + \ell$. Thus loops of degree ℓ^4 in Case II are all products of loops of degree ℓ^2. $\square$

Definition 3.13. Let α be an (ℓ, ℓ)-isogeny from $E \times E$. If

$$\dim(\ker(\alpha) \cap (L_i \times L_i)) = 1$$

for $i = 1$ (resp. $i = 2$), we call α an λ-isogeny (resp $\bar{\lambda}$-isogeny).

Lemma 3.14. *Suppose $p > 4\ell^2$ and $\ell \equiv 1 \pmod 4$.*

If α and β are two edges from $E \times E$ to a vertex $V \neq E \times E$ such that the loop $\varphi = \hat{\alpha} \circ \beta$ has a factor of $[\lambda]$ or $[\bar{\lambda}]$. Then

(1) *α and β are not in the same G-orbit.*
(2) *If $\varphi = \tau \circ [\lambda]$, then $\hat{\varphi} = \hat{\beta} \circ \alpha = \hat{\tau} \circ [\bar{\lambda}]$.*
(3) *If $\varphi = \tau \circ [\lambda]$, then*

$$\ker(\beta) \cap (L_1 \times L_1) = L_1^{\tau}, \quad \ker(\alpha) \cap (L_2 \times L_2) = L_2^{\hat{\tau}}. \tag{7}$$

Hence τ, α (resp. τ, β) and φ are uniquely determined by β (resp. α).

On the other hand, if an edge $\beta : E \times E \to V$ is an λ-isogeny (resp $\bar{\lambda}$-isogeny), then there exists $\alpha : E \times E \to V$ such that $\varphi = \hat{\alpha} \circ \beta = \tau \circ [\lambda]$ (resp. $\varphi = \hat{\alpha} \circ \beta = \tau \circ [\bar{\lambda}]$) for some loop τ.

Proof. (1) is easy, since if $\alpha = \beta g$ for $g \in G$, then $\hat{\beta} \circ \alpha = \ell g$ belongs to Case (I) in Proposition 3.12. (2) follows from the fact that $[\lambda]$ commutes with τ.

For (3), we only need to study $\ker(\beta)$. Note that

(a) φ belongs to Case (III) in Proposition 3.12, thus $\ker(\varphi) \cong (\mathbb{Z}/\ell\mathbb{Z})^2 \times \mathbb{Z}/\ell^2\mathbb{Z}$;
(b) $L_2^{\tau} = (L_2 \times L_2) \cap \ker(\tau) \subseteq \ker(\varphi)$;
(c) $L_1 \times L_1 = \ker[\lambda] \subseteq \ker(\varphi)$.

Thus the ℓ-part of $\ker(\varphi)$, which contains $\ker(\beta)$, is generated by $L_1 \times \{0\} = \langle (R, 0) \rangle$, $\{0\} \times L_1 = \langle (0, R) \rangle$ and L_2^{τ}.

Now we consider cases:

(i) If $L_2^\tau = L_2 \times \{0\} = \langle (R', 0) \rangle$, then $L_1^\tau = \{0\} \times L_1$. By computation, $\ker(\beta) = \langle (U, 0), (0, R) \rangle$ where $U \in E[\ell]$, $U \notin L_1 \cup L_2$. Thus

$$\ker(\beta) \cap (L_1 \times L_1) = L_1^\tau, \quad \ker(\beta) \cap (L_2 \times L_2) = 0.$$

(ii) If $L_2^\tau = \{0\} \times L_2 = \langle (0, R') \rangle$, then $L_1^\tau = L_1 \times \{0\}$. The proof is similar to (i).

(iii) If $L_2^\tau = \langle (R', aR') \rangle$ for some $a \neq 0$, by Lemma 3.11, then $L_1^\tau = \langle (R, -a^{-1}R) \rangle$. In this case $\langle (R, 0), (0, R), (R', aR') \rangle \supset \ker(\beta)$. We assume $\ker(\beta) = \langle (R, cR), (R', bR + aR') \rangle$. By computing the Weil pairing, we get $c = -a^{-1}$ and $\ker(\beta) \cap (L_1 \times L_1) = L_1^\tau$ and $\ker(\beta) \cap (L_2 \times L_2) = 0$.

This finishes the proof of (3).

Now suppose β is an λ-isogeny, we let τ be the loop such that $L_1^\tau = L$. Checking the argument above we see that $\ker(\beta) \subset \ker(\tau \circ [\lambda])$, so $\varphi = \tau \circ [\lambda]$ factors through β. □

Lemma 3.15. *Suppose $\ell \equiv 1 \bmod 4$ and $p > 4\ell^2$.*

(1) *The diagonal non-loop λ-isogenies and $\bar{\lambda}$-isogenies are exactly those in Class* **D3**, *whose number is $4(\ell - 1)$.*

(2) *The quadruples $\{a, b, c, d\}$ associated to non-diagonal non-loop λ-isogenies are parameterized by*

$$a = k - k^{-1} - d, \ b = dt - kt, \ c = dt + k^{-1}t, \tag{8}$$

where $k \in \mathbb{F}_\ell^\times, d \in \mathbb{F}_\ell, k - k^{-1} \neq 2d$. If $k = \pm 1$ and $d \neq 0$ or $d \neq k = \pm t$, then the isogenies belong to Class **N3**, *other cases belong to Class* **N4**. *The number of λ-isogenies and $\bar{\lambda}$-isogenies is $2(\ell - 1)^2$, of which $8(\ell - 1)$ are in Class* **N3** *and $2(\ell - 1)(\ell - 5)$ in Class* **N4**.

Proof. (1) is easy. For (2), if $\ker(\beta)$ contains an element (R, uR) for some $u \neq 0$, then $(R, uR) = \frac{1}{2}[(S, aS + bS^*) - t(S^*, cS + dS^*)]$, which means

$$ad = bc - 1, \ a - d = bt + ct.$$

Hence $(a + d)^2 = (a - d)^2 + 4ad = -(b + c)^2 + 4bc - 4 = -(b - c)^2 - 4$, and

$$(a + d)^2 + (b - c)^2 = (a + d + bt - ct)(a + d - bt + ct) = -4.$$

Plug in $a = d + bt + ct$, we get

$$d + bt = k, \ d + ct = -k^{-1}.$$

This gives the parametrization. However, we need to exclude the loop case, which means $a = d$ or equivalently $k - k^{-1} = 2d$. □

Theorem 3.16. *Suppose $p > 4\ell^2$. Let V be a vertex adjacent to $E \times E$.*

(1) *If there exists one λ-isogeny (resp. $\bar{\lambda}$-isogeny) $\beta : E \times E \to V$, then all isogenies from $E \times E$ to V are λ-isogenies (resp. $\bar{\lambda}$-isogenies) and they form two G-orbits.*
(2) *For all other cases, (ℓ, ℓ)-isogenies from $E \times E$ to V form a single G-orbit.*

Proof. Suppose α, β are two edges from $E \times E$ to V, then $\varphi = \hat{\alpha} \circ \beta$ is a loop of degree ℓ^4. Moreover, by the unique factorization of loops of Case II in Proposition 3.12, φ doesn't belong to this case. By Lemma 3.14, φ belongs to Case III only if β is an λ-isogeny or an $\bar{\lambda}$-isogeny. For all other cases, φ must be in Case I and α and β are in the same G-orbit.

Now suppose φ belongs to Case III, then by Lemma 3.14, α and β are in two different G-orbits. Moreover $\hat{g_1}\beta g_2$ for all $g_1, g_2 \in G$ are in Case III, which in turn means that αg_1 and βg_2 are λ-isogenies or an $\bar{\lambda}$-isogenies.

We only need to show there is no other G-orbit. If not, suppose α' is an edge from $E \times E$ to V not in αG and βG. Then both $\varphi = \hat{\alpha} \circ \beta$ and $\varphi' = \hat{\alpha'} \circ \beta$ factor through $[\lambda]$ or $[\bar{\lambda}]$, however, there is only one such φ by Lemma 3.14. □

Theorem 3.17. *Suppose $p > 4\ell^2$. Consider the neighborhood of $[E_{1728} \times E_{1728}]$.*

(1) *If $\ell \equiv 1 \bmod 4$, the neighborhood is given by the following table:*

#Vertices	*Multi-Edges*	*Edge Type*	*#Vertices*	*Multi-Edges*	*Edge Type*
$\frac{\ell-1}{2}$	*8*	**D3**	$\frac{(\ell-1)(\ell-3)}{4}$	*8*	**N3**-*1*
$\frac{\ell-1}{2}$	*4*	**D4**	$\frac{\ell-1}{2}$	*16*	**N3**-*2*
$\frac{(\ell-1)(\ell-3)}{8}$	*8*	**D5**	$\frac{(\ell-1)(\ell^2-3\ell+6)}{16}$	*16*	**N4**-*1*
$\frac{\ell-1}{4}$	*4*	**N2**	$\frac{(\ell-1)(\ell-5)}{16}$	*32*	**N4**-*2*

(2) *If $\ell \equiv 3 \bmod 4$, the neighborhood is given by the following table:*

#Vertices	*Multi-Edges*	*Edge Type*	*#Vertices*	*Multi-Edges*	*Edge Type*
$\frac{\ell+1}{2}$	*4*	**D4**	$\frac{\ell+1}{4}$	*4*	**N2**
$\frac{\ell^2-1}{8}$	*8*	**D5**	$\frac{\ell^2-1}{4}$	*8*	**N3**
			$\frac{\ell(\ell+1)(\ell-3)}{16}$	*16*	**N4**

(3) *If $\ell = 2$, there are 3 vertices adjacent to $[E_{1728} \times E_{1728}]$, each connecting with 4 edges, 2 vertices with diagonal and 1 with non-diagonal kernels.*

Proof. For ℓ odd, this is a consequence of Proposition 3.7, Proposition 3.9, Lemma 3.15 and Theorem 3.16.

Now we consider the case $\ell = 2$. Suppose $P \in E[2]$ such that $P \neq i(P)$. Then $E[2] = \{O, P, Q = i(P), S = P+Q\}$. Moreover $i(S) = S$. Let $K_1 = \{O, P\}$, $K_2 = \{O, Q\}$ and $L = \{O, S\}$. Then the only diagonal loop kernel is $L \times L$. The other 8 diagonal isogenies form two G-orbits:

$$\{K_1 \times K_1, K_1 \times K_2, K_2 \times K_1, K_2 \times K_2\},\ \{L \times K_1, L \times K_2, K_1 \times L, K_2 \times L\}.$$

The kernels of the 2 non-diagonal loops are $\langle (P,P),(Q,Q)\rangle$ and $\langle (P,Q),(Q,P)\rangle$. The other 4 non-diagonal isogenies belong to one orbit. $\square$

4. Loops and neighborhoods of $[E_0 \times E_0]$

In this section, let E_0 be the supersingular elliptic curve defined over $\mathbb{F}_p$ with j-invariant 0 (which implies that $p \equiv 2 \bmod 3$). We know its endomorphism ring is

$$\mathcal{O}_0 = \mathbb{Z} + \mathbb{Z}\frac{1+i}{2} + \mathbb{Z}\frac{i+k}{3} + \mathbb{Z}\frac{j+k}{2},\ (i^2 = -3,\ j^2 = -p,\ ij = -ji = k).$$

Note that the reduced norm is given by

$$\begin{aligned} &\mathrm{Nrd}\left(x + y\frac{1+i}{2} + z\frac{i+k}{3} + w\frac{j+k}{2}\right) \\ &= \left(x + \frac{y}{2}\right)^2 + 3\left(\frac{y}{2} + \frac{z}{3}\right)^2 + \frac{p(z^2 + 3zw + 3w^2)}{3}. \end{aligned} \tag{9}$$

Let $[E_0 \times E_0]$ be the superspecial abelian surface $E_0 \times E_0$ with the principal polarization $\{0\} \times E_0 + E_0 \times \{0\}$ in the isogeny graph $\mathcal{G}_p$.

Now results hereafter in this section are parallel to those in the previous section, whose proofs are almost identical and will be omitted.

Lemma 4.1. [17, Theorem 13] *The number of integer solutions of Diophantine equation*

$$x^2 + xy + y^2 + z^2 + zw + w^2 = n$$

is $12\sigma(n) - 36\sigma(\frac{n}{3})$.

Let $G = \mathrm{Aut}(E_0 \times E_0)$. By simple computation, we have

Lemma 4.2. *The group G is the following group of order 72:*

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},\quad \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \;\middle|\; a, b = \pm 1, \pm\frac{1+i}{2}, \pm\frac{1-i}{2} \right\}. \tag{10}$$

We shall need the following notation in this section:

(i) If $\ell \equiv 1 \bmod 3$, let

(a) $\lambda := x_\ell + y_\ell \frac{1+i}{2} \in \mathbb{Z}[\frac{1+i}{2}]$ such that $x_\ell^2 + x_\ell y_\ell + y_\ell^2 = \ell$;
(b) $L_1 := \ker(\lambda : E_0[\ell] \to E_0[\ell])$ and $L_2 := \ker(\bar{\lambda} : E_0[\ell] \to E_0[\ell])$;

(c) $R \in L_1 \backslash \{0\}$ and $R' \in L_2 \backslash \{0\}$;
(d) $t := -x_\ell / y_\ell \in \mathbb{F}_\ell$. Note that $t^2 - t + 1 = 0$.

(ii) Let $S = R + R' \in E_0[\ell]$ if $\ell \equiv 1 \bmod 3$ and $S = P$ be a fixed nonzero $P \in E_0[\ell]$ if $\ell \equiv 2 \bmod 3$. Let $S^* = \frac{1+i}{2}(S)$.
(iii) Let $G = \mathrm{Aut}(E_0 \times E_0)$.
(iv) For an isogeny φ starting from $E_0 \times E_0$, let $G_\varphi = \{g \in G : \varphi g = \varphi\}$ be the stabilizer of φ by the G-action, and $O_\varphi = \{\varphi g : g \in G\}$ be the G-orbit of φ.

Note that L_1 and L_2 are the only 1-dimensional invariant $\mathbb{F}_\ell$-subspaces of the operator $\frac{1+i}{2}$ on $E_0[\ell]$, with eigenvalues t and $-t$ respectively; similarly, L_1 and L_2 are the only 1-dimensional invariant $\mathbb{F}_\ell$-subspaces of the operator $\frac{1-i}{2}$ on $E_0[\ell]$, with eigenvalues $1-t$ and $1+t$ respectively.

4.1. Kernels of (ℓ, ℓ)-isogenies from $E_0 \times E_0$

Lemma 4.3. *The set $\{S, S^*\}$ is an $\mathbb{F}_\ell$-basis of $E_0[\ell]$.*

Proposition 4.4. *There is a one-to-one correspondence of the set of non-diagonal (ℓ, ℓ)-isogenies from $E_0 \times E_0$ and the set of generator matrices*

$$\left\{ \begin{pmatrix} S & S^* \\ aS + bS^* & cS + dS^* \end{pmatrix} : a, b, c, d \in \mathbb{F}_\ell, ad - bc = -1 \right\}.$$

Definition 4.5. For a non-diagonal (ℓ, ℓ)-isogeny φ from $E_0 \times E_0$, we call $\{a, b, c, d\}$ given above the quadruple associated to φ.

We now describe the action of $G = \mathrm{Aut}(E_0 \times E_0)$ on the isogenies explicitly. For the diagonal isogenies, we have

Proposition 4.6. *Suppose* $\ker(\varphi) = K_1 \times K_2$. *Diagonal isogenies can be divided into the following classes, which are unions of G-orbits:*

(D1) $(K_1, K_2) = (L_1, L_1)$ *or* (L_2, L_2), *where* $G_\varphi = G$ *and* $O_\varphi = \{\varphi\}$.
(D2) $(K_1, K_2) = (L_1, L_2)$ *or* (L_2, L_1), *which form* 1 *orbit if* $\ell \equiv 1 \bmod 3$.
(D3) *Exactly one of* K_1, K_2 *is in* $\{L_1, L_2\}$, *where* $|G_\varphi| = 12$ *and* $|O_\varphi| = 6$. *This class contains* $4(\ell - 1)$ *isogenies if* $\ell \equiv 1 \bmod 3$.
(D4) $K_1 \notin \{L_1, L_2\}$ *and* $K_2 \in \{K_1, \frac{1+i}{2}(K_1), \frac{1-i}{2}(K_1)\}$, *where* $|G_\varphi| = 8$ *and* $|O_\varphi| = 9$. *This class contains* $3(\ell - 1)$ *isogenies if* $\ell \equiv 1 \bmod 3$, *and* $3(\ell + 1)$ *isogenies if* $\ell \equiv 2 \bmod 3$.
(D5) $K_1 \notin \{L_1, L_2\}$ *and* $K_2 \notin \{L_1, L_2, K_1, \frac{1+i}{2}(K_1), \frac{1-i}{2}(K_1)\}$, *where* $G_\varphi = \{\left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right)\}$ *and* $|O_\varphi| = 18$. *This class contains* $(\ell - 1)(\ell - 4)$ *isogenies if* $\ell \equiv 1 \bmod 3$, *and* $\ell^2 - \ell - 2$ *isogenies if* $\ell \equiv 2 \bmod 3$.

For the non-diagonal isogenies, we have

Proposition 4.7. *Non-diagonal isogenies can be divided into the following classes, which are unions of G-orbits:*

- **(N1)** $\{a, b, c, d\} = \{a, b, -b, a + b\}$*: This class contains* $\ell - 1$ *isogenies if* $\ell \equiv 1 \bmod 3$ *and* $\ell + 1$ *isogenies if* $\ell \equiv 2 \bmod 3$.
- **(N2)** $\{a, b, c, d\} = \{a, b, a + b, -a\}$*, where* $|G_\varphi| = 12$ *and* $|O_\varphi| = 6$*. This class contains* $\ell - 1$ *isogenies if* $\ell \equiv 1 \bmod 3$ *and* $\ell + 1$ *isogenies if* $\ell \equiv 2 \bmod 3$.
- **(N3)** *if* $3d^2 \neq -1$*,* $\{a, b, c, d\} = \{a, b, c, -a\}$*,* $c \neq a + b$*, or* $\{a, b, c, d\} = \{a, b, a + b, d\}$*,* $d \neq -a$*, or* $\{a, b, c, d\} = \{a, b, c, b - c\}$*,* $d \neq -a$ *where* $|G_\varphi| = 4$ *and* $|O_\varphi| = 18$*. This class contains* $3(\ell^2 - 1)$ *isogenies.*
- **(N4)** *all other cases, where* $G_\varphi = \{\pm I_2\}$ *and* $|O_\varphi| = 36$*. This class contains* $\ell^3 - 3\ell^2 - 3\ell + 5$ *isogenies if* $\ell \equiv 1 \bmod 3$ *and* $\ell^3 - 3\ell^2 - 3\ell + 1$ *isogenies if* $\ell \equiv 2 \bmod 3$.

4.2. Loops at $[E_0 \times E_0]$

Theorem 4.8. *Suppose* $p > 3\ell$.

(1) *If* $\ell \equiv 1 \bmod 3$*, then the set of loops of* $E_0 \times E_0$ *is the union of Classes* **D1**, **D2** *and* **N1**.

(2) *If* $\ell \equiv 2 \bmod 3$*, then the set of loops of* $E_0 \times E_0$ *is Class* **N1**.

(3) *If* $\ell = 3$*, then* $E_0 \times E_0$ *has 1 loop.*

4.3. Neighbors of $[E_0 \times E_0]$

If $\ell \equiv 1 \bmod 3$, we denote the loops $\lambda \times \lambda$ and $\bar{\lambda} \times \bar{\lambda}$ on $E_0 \times E_0$ by $[\lambda]$ and $[\bar{\lambda}]$ respectively. Hence

$$\ker[\lambda] = L_1 \times L_1, \quad \ker[\bar{\lambda}] = L_2 \times L_2.$$

Lemma 4.9. *Suppose* $\ell \equiv 1 \bmod 3$ *and* $p > 3\ell$*. For a loop* $\alpha \neq [\lambda]$, $[\bar{\lambda}]$ *of* $E_0 \times E_0$ *of degree* ℓ^2*, let*

$$L_i^\alpha = (L_i \times L_i) \cap \ker \alpha \quad (i = 1, 2).$$

Then $\alpha \mapsto L_i^\alpha$ *gives a one-to-one correspondence*

$$\{\textit{degree } \ell^2 \textit{ loops } \neq [\lambda] \textit{ or } [\bar{\lambda}]\} \leftrightarrow \{1\textit{-dimensional subspaces of } L_i \times L_i\}.$$

Consequently, $\ker \alpha = L_1^\alpha \times L_2^\alpha$*, and if* $L_1^\alpha = \{(P, kP) : P \in L_1\}$ *for some* $k \neq 0$*, then* $L_2^\alpha = \{(-kQ, Q) : Q \in L_2\}$.

Proposition 4.10. *Suppose $p > 3\ell^2$. Every loop φ of $E_0 \times E_0$ of degree ℓ^4 corresponds to a matrix of the following form:*

(I) ℓI_2. *In this case* $\ker\varphi \cong (\mathbb{Z}/\ell\mathbb{Z})^4$.

(II) $\begin{pmatrix} a & b\frac{1+i}{2} \\ \bar{b}\frac{-1+i}{2} & \bar{a} \end{pmatrix}$, *where* $a, b \in \mathbb{Z}[\frac{1+i}{2}]$, $a\bar{a} + b\bar{b} = \ell^2$ *and* $ab \neq 0$. *In this case* $\ker\varphi \cong (\mathbb{Z}/\ell^2\mathbb{Z})^2$.

(III) $\lambda \begin{pmatrix} a & b\frac{1+i}{2} \\ \bar{b}\frac{-1+i}{2} & \bar{a} \end{pmatrix}$ *or* $\bar{\lambda} \begin{pmatrix} a & b\frac{1+i}{2} \\ \bar{b}\frac{-1+i}{2} & \bar{a} \end{pmatrix}$, *where* $a, b \in \mathbb{Z}[\frac{1+i}{2}]$ *and* $a\bar{a} + b\bar{b} = \ell$. *In this case* $\ker\varphi \cong (\mathbb{Z}/\ell\mathbb{Z})^2 \times \mathbb{Z}/\ell^2\mathbb{Z}$ *which occurs only if* $\ell \equiv 1 \bmod 3$.

As a consequence, every loop of degree ℓ^4 can be factorized as the product of two loops of degree ℓ^2. Moreover, loops in Case II are uniquely factorized as the composition of two edges of degree ℓ^2.

Definition 4.11. Let α be an (ℓ, ℓ)-isogeny from $E_0 \times E_0$. If

$$\dim(\ker(\alpha) \cap (L_i \times L_i)) = 1$$

for $i = 1$ (resp. $i = 2$), we call α an λ-isogeny (resp $\bar{\lambda}$-isogeny).

Lemma 4.12. *Suppose $p > 3\ell^2$ and $\ell \equiv 1 \pmod 3$.*

If α and β are two edges from $E_0 \times E_0$ to a vertex $V \neq E_0 \times E_0$ such that the loop $\varphi = \hat{\alpha} \circ \beta$ has a factor of $[\lambda]$ or $[\bar{\lambda}]$. Then

(1) *α and β are not in the same G-orbit.*
(2) *If $\varphi = \tau \circ [\lambda]$, then $\hat{\varphi} = \hat{\beta} \circ \alpha = \hat{\tau} \circ [\bar{\lambda}]$.*
(3) *If $\varphi = \tau \circ [\lambda]$, then*

$$\ker(\beta) \cap (L_1 \times L_1) = L_1^{\tau}, \quad \ker(\alpha) \cap (L_2 \times L_2) = L_2^{\hat{\tau}}. \tag{11}$$

Hence τ, α (resp. τ, β) and φ are uniquely determined by β (resp. α).

On the other hand, if an edge $\beta : E_0 \times E_0 \to V$ of degree ℓ^2 is an λ-isogeny (resp $\bar{\lambda}$-isogeny), then there exists $\alpha : E_0 \times E_0 \to V$ such that $\varphi = \hat{\alpha} \circ \beta = \tau \circ [\lambda]$ (resp. $\varphi = \hat{\alpha} \circ \beta = \tau \circ [\bar{\lambda}]$) for some loop τ.

Lemma 4.13. *Suppose $\ell \equiv 1 \bmod 3$ and $p > 3\ell^2$.*

(1) *The diagonal non-loop λ-isogenies and $\bar{\lambda}$-isogenies are exactly those in Class* **D3**, *whose number is $4(\ell - 1)$.*
(2) *The quadruples $\{a, b, c, d\}$ associated to non-diagonal non-loop λ-isogenies belong to Class* **N3** *and* **N4**. *The number of λ-isogenies and $\bar{\lambda}$-isogenies is $2(\ell - 1)^2$, of which $12(\ell - 1)$ are in Class* **N3** *and $2(\ell - 1)(\ell - 7)$ in Class* **N4**.

Theorem 4.14. *Suppose $p > 3\ell^2$. Let V be a vertex adjacent to $E_0 \times E_0$.*

(1) *If there exists one λ-isogeny (resp. $\bar{\lambda}$-isogeny) $\beta : E_0 \times E_0 \to V$, then all isogenies from $E_0 \times E_0$ to V are λ-isogenies (resp. $\bar{\lambda}$-isogenies) and they form two G-orbits.*
(2) *For all other cases, (ℓ, ℓ)-isogenies from $E_0 \times E_0$ to V form a single G-orbit.*

Theorem 4.15. *Suppose $p > 3\ell^2$. Consider the neighborhood of $[E_0 \times E_0]$.*
(1) *If $\ell \equiv 1 \bmod 3$, the neighborhood is given by the following table:*

#Vertices	*Multi-Edges*	*Edge Type*	*#Vertices*	*Multi-Edges*	*Edge Type*
$\frac{\ell-1}{3}$	*12*	**D3**	$\frac{(\ell-1)(\ell-3)}{6}$	*18*	**N3**-*1*
$\frac{\ell-1}{3}$	*9*	**D4**	$\frac{\ell-1}{3}$	*36*	**N3**-*2*
$\frac{(\ell-1)(\ell-4)}{18}$	*18*	**D5**	$\frac{(\ell-1)(\ell^2-4\ell+9)}{36}$	*36*	**N4**-*1*
$\frac{\ell-1}{6}$	*6*	**N2**	$\frac{(\ell-1)(\ell-7)}{36}$	*72*	**N4**-*2*

(2) *If $\ell \equiv 2 \bmod 3$, the neighborhood is given by the following table:*

#Vertices	*Multi-Edges*	*Edge Type*	*#Vertices*	*Multi-Edges*	*Edge Type*
$\frac{\ell+1}{3}$	*9*	**D4**	$\frac{\ell+1}{6}$	*6*	**N2**
$\frac{\ell^2-\ell-2}{18}$	*18*	**D5**	$\frac{\ell^2-1}{6}$	*18*	**N3**
			$\frac{\ell^3-3\ell^2-3\ell+1}{36}$	*36*	**N4**

(3) *if $\ell = 2$, then there is one vertex adjacent to $[E_0 \times E_0]$ with diagonal kernel, and each connecting $[E_0 \times E_0]$ with 9 edges. There is one vertex adjacent to $[E_0 \times E_0]$ with nondiagonal kernel, and each connecting $[E_0 \times E_0]$ with 3 edges, other three isogenies are loops.*

(4) *if $\ell = 3$, then there are two vertices adjacent to $[E_0 \times E_0]$ with diagonal kernel, and connecting $[E_0 \times E_0]$ with 6 and 9 edges. There are three vertices adjacent to $[E_0 \times E_0]$ with nondiagonal kernel, and each connecting $[E_0 \times E_0]$ with 8 edges, the last isogeny is a loop.*

5. Loops and neighborhoods of $[E \times E']$ for $j(E) \in \mathbb{F}_p \backslash \{0, 1728\}$

In this section, we assume E has j-invariant in $\mathbb{F}_p \backslash \{0, 1728\}$ and $j(E') \in \mathbb{F}_{p^2} \backslash \{0, 1728, j(E)\}$. Let π be the Frobenius map of E. We know that $\mathrm{End}(E)$ has the form (see for example [18]):

(1) If $\frac{1+\pi}{2} \notin \mathrm{End}(E)$, then there exists a prime q satisfying $(\frac{p}{q}) = -1$ and $q \equiv 3 \pmod 8$, such that

$$\mathrm{End}(E) = \mathcal{O}(q) := \mathbb{Z} + \mathbb{Z}\frac{1+i}{2} + \mathbb{Z}\frac{j-k}{2} + \mathbb{Z}\frac{ri-k}{q},$$

where $r^2 \equiv -p \pmod{q}$, $i^2 = -q$, $j^2 = -p$, $ij = -ji = k$. The reduced norm of $\mathcal{O}(q)$ is given by

$$\begin{aligned} &\mathrm{Nrd}\left(x + y\frac{1+i}{2} + z\frac{j-k}{2} + w\frac{ri-k}{q}\right) \\ &= \left(x+\frac{y}{2}\right)^2 + q\left(\frac{y}{2}+\frac{rw}{q}\right)^2 + \frac{pz^2}{4} + pq\left(\frac{z}{2}+\frac{w}{q}\right)^2. \end{aligned} \tag{12}$$

(2) If $\frac{1+\pi}{2} \in \mathrm{End}(E)$, then there exists a prime q satisfying $(\frac{p}{q}) = -1$ and $q \equiv 3 \pmod{8}$, such that

$$\mathrm{End}(E) = \mathcal{O}'(q) := \mathbb{Z} + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}i + \mathbb{Z}\frac{r'i-k}{2q},$$

where ${r'}^2 \equiv -p \pmod{4q}$, $i^2 = -q$, $j^2 = -p$, $ij = -ji = k$. The reduced norm on $\mathcal{O}(q)$ is given by

$$\begin{aligned} &\mathrm{Nrd}\left(x + yi + z\frac{1+j}{2} + w\frac{r'i-k}{2q}\right) \\ &= \left(x+\frac{z}{2}\right)^2 + q\left(y+\frac{r'w}{2q}\right)^2 + \frac{p(qz^2+w^2)}{4q}. \end{aligned} \tag{13}$$

5.1. Kernels of (ℓ,ℓ)-isogenies from $E \times E'$

Note that E, E' are not isomorphic, we have

$$G = \mathrm{Aut}(E \times E') = \{1, [-1]\times 1, 1\times[-1], [-1]\times[-1]\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Consequently, we have

Proposition 5.1. *Let φ be an (ℓ,ℓ) isogeny from $E \times E'$.*

(1) *If $\ker\varphi$ is diagonal (type* (**D**)*), then $G_\varphi = G$ and $O_\varphi = \{\varphi\}$.*
(2) *If $\ker\varphi$ is nondiagonal (type* (**N**)*), then $G_\varphi = \{1, [-1]\times[-1]\}$ and $|O_\varphi| = 2$.*

Proof. (1) If $\ker(\varphi)$ is diagonal, we can assume $\ker(\varphi)$ is generated by $(P,0)$ and $(Q,0)$. By acting G on $\langle(P,0),(0,Q)$, we have $G_\varphi = G$.

(2) If $\ker(\varphi)$ is nondiagonal, we can assume $\ker(\varphi)$ is generated by (P,Q) and (P',Q'), where P and P' are linearly independent. By computing the action of G on $\langle(P,Q),(P',Q')\rangle$, we have $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\langle(P,Q),(P',Q')\rangle = \langle(P,-Q),(P',-Q')\rangle \neq \langle(P,Q),(P',Q')\rangle$. Hence $G_\varphi = \{1,[-1]\times[-1]\}$. □

5.2. Loops at $[E \times E']$

Theorem 5.2. *For $d \in \mathbb{Z}_+$, let $\mathrm{Iso}_d(E, E') := \{\sigma : E \to E' \mid \deg(\sigma) = d\}$. Suppose either $\mathrm{End}(E) = \mathcal{O}(q)$ and $p > q\ell^2 > 4\ell^4$, or $\mathrm{End}(E) = \mathcal{O}'(q)$ and $p > 4q\ell^2 > 4\ell^4$.*

(1) *If there exists d such that $\ell - d = \square > 0$ (where $\square$ denotes a square of an integer) and $\mathrm{Iso}_d(E, E') \neq \emptyset$, then there are exactly two loops of $E \times E'$, whose kernels are nondiagonal.*
(2) *If there is an isogeny from E to E' of degree ℓ, then there is only one loop of $E \times E'$, whose kernel is diagonal.*
(3) *If $\mathrm{Iso}_d(E, E') = \emptyset$ for all d such that $\ell - d = \square$, then there is no loop of $E \times E'$.*

Proof. As seen in [29, §2], a loop of $E \times E'$ has the form:

$$\begin{pmatrix} \varphi_1 & -\varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix}$$

where $\varphi_1 : E \to E$, $\varphi_2 : E' \to E$, $\varphi_3 : E \to E'$, $\varphi_4 : E' \to E'$, and

$$\begin{pmatrix} \widehat{\varphi_1} & \widehat{\varphi_3} \\ -\widehat{\varphi_2} & \widehat{\varphi_4} \end{pmatrix} \begin{pmatrix} \varphi_1 & -\varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix} = \begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix}.$$

By computation, we have

$$\begin{aligned} &\deg(\varphi_1) = \deg(\varphi_4), \quad \deg(\varphi_2) = \deg(\varphi_3), \\ &\deg(\varphi_1) + \deg(\varphi_2) = \ell, \quad \widehat{\varphi_2} \circ \varphi_1 = \widehat{\varphi_4} \circ \varphi_3. \end{aligned} \tag{14}$$

We now show the case $\mathrm{End}(E) = \mathcal{O}(q)$, the case $\mathrm{End}(E) = \mathcal{O}'(q)$ follows by the same argument.

Under the assumption $p > q\ell^2 > 4\ell^4$, loops of E of degree $\leq \ell$ are all inside $\mathbb{Z}$. This means $\varphi_1 = [a]$ for some $a \in \mathbb{Z}$. By Equation (14), we have $\gcd(\deg(\varphi_1), \deg(\varphi_2)) = 1$, and $E[a] \subseteq \ker(\widehat{\varphi_2} \circ \varphi_1)$. Thus $E[a] \subseteq \ker(\widehat{\varphi_4} \circ \varphi_3)$, which implies that $\ker(\widehat{\varphi_4}) \cong (\mathbb{Z}/a\mathbb{Z})^2$. Hence $\varphi_4 = [a]$, $\varphi_2 = \widehat{\varphi_3}$ and $a^2 + \deg(\varphi_2) = \ell$. Thus if $\begin{pmatrix} \varphi_1 & -\varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix}$ is a loop of $E \times E'$, $\varphi_2 : E \to E'$ must be an isogeny such that $\ell - \deg(\varphi_2) = \square$. This gives the proof of (3).

To see (1), if there is an isogeny φ from E to E' of degree $d < \ell$ such that $\ell - d = a^2$, then there are two loops of $E \times E'$:

$$\begin{pmatrix} a & -\widehat{\varphi} \\ \varphi & a \end{pmatrix}, \quad \begin{pmatrix} a & \widehat{\varphi} \\ -\varphi & a \end{pmatrix}.$$

The kernels of these two loops are:

$$\langle([a]P,-\varphi(P)),([a]Q,-\varphi(Q))\rangle;\quad \langle([a]P,\varphi(P)),([a]Q,\varphi(Q))\rangle$$

where $E[\ell]=\langle P,Q\rangle$. It is easy to see these two kernels are nondiagonal and in the same orbit of $G=\mathrm{Aut}(E\times E')$.

We show that φ is the unique isogeny from E to E' such that $\deg(\varphi)\le\ell$ and $\ell-\deg(\varphi)=\square$. If there is another isogeny φ' from E to E' of degree $d'\le\ell$ such that $\ell-d'=b^2$, then $\widehat{\varphi'}\circ\varphi$ is a loop of E of degree dd'. By the assumption $p>q\ell^2>4\ell^4$, we have $\widehat{\varphi'}\circ\varphi=[x]$ with $x\in\mathbb{Z}$. Hence $[\deg(\varphi')]\varphi=[x]\varphi'$. Comparing the degrees on both sides, we find that there exist coprime integers t_1 and t_2 such that $t_1^2d'=t_2^2d$, which means $\delta=d/t_1^2=d'/t_2^2\in\mathbb{Z}_+$. By the relation $\ell=d+a^2=d'+b^2$, we have

$$\ell=t_1^2\delta+a^2=t_2^2\delta+b^2.$$

Thus ℓ splits into principal prime ideals in the imaginary quadratic field $\mathbb{Q}(\sqrt{-\delta})$. By unique factorization, we must have $d=d'$ and $\varphi=\varphi'$.

To see (2), if there is an isogeny φ from E to E' of degree ℓ, then there is one loop $\begin{pmatrix}0 & -\widehat{\varphi}\\ \varphi & 0\end{pmatrix}$ of $E\times E'$, whose kernel is diagonal. $\square$

5.3. Neighbors of $[E\times E']$

Theorem 5.3. *Suppose either* $\mathrm{End}(E)=\mathcal{O}(q)$ *and* $p>q\ell^2>4\ell^4$ *or* $\mathrm{End}(E)=\mathcal{O}'(q)$ *and* $p>4q\ell^2>4\ell^4$.

(1) *If there is an isogeny from E to E' of degree d such that $\ell-d=\square>0$, then the neighborhood of $[E\times E']$ is given by the following table:*

#Vertices	*Multi-Edges*	*Edge Type*	*#Vertices*	*Multi-Edges*	*Edge Type*
$(\ell+1)^2$	*1*	**D**	$\frac{\ell^3-\ell-2}{2}$	*2*	**N**

(2) *If there is an isogeny from E to E' of degree ℓ, then the neighborhood is given by the following table:*

#Vertices	*Multi-Edges*	*Edge Type*	*#Vertices*	*Multi-Edges*	*Edge Type*
$\ell^2+2\ell$	*1*	**D**	$\frac{\ell^3-\ell}{2}$	*2*	**N**

(3) *If there is no isogeny from E to E' of degree d such that $\ell-d=\square$, then the neighborhood is given by the following table:*

#Vertices	*Multi-Edges*	*Edge Type*	*#Vertices*	*Multi-Edges*	*Edge Type*
$(\ell+1)^2$	*1*	**D**	$\frac{\ell^3-\ell}{2}$	*2*	**N**

Proof. We claim that two (ℓ,ℓ)-isogenies α,β from $[E\times E']$ to the same vertex are in the same G-orbit under the assumption of the theorem.

Indeed, in this situation $\widehat{\beta}\circ\alpha$ is a loop of $[E\times E']$. Write

$$\widehat{\beta}\circ\alpha=\begin{pmatrix}\varphi_1 & -\varphi_2\\ \varphi_3 & \varphi_4\end{pmatrix}$$

where $\varphi_1:E\to E$, $\varphi_2:E'\to E$, $\varphi_3:E\to E'$ and $\varphi_4:E'\to E'$ are isogenies of elliptic curves. Under the assumption $p>q\ell^2>4\ell^4$ for $\mathrm{End}(E)=\mathcal{O}(q)$ or $p>4q\ell^2>4\ell^4$ for $\mathrm{End}(E)=\mathcal{O}'(q)$, loops of E with degree $\leq\ell^2$ are all inside $\mathbb{Z}$. Suppose $\varphi_1=[a]$ for some $a\in\mathbb{Z}$. Following the proof of Theorem 5.2 (1), we have

$$\varphi_1=\varphi_4=[a],\ \ \varphi_2=\widehat{\varphi_3}\text{ and }a^2+\deg(\varphi_2)=\ell^2.$$

We now denote φ_3 by φ. Then

$$\ker(\widehat{\beta}\circ\alpha)=\langle([a]P,-\varphi(P)),([a]Q,-\varphi(Q))\rangle\cong\left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^2$$

where $E[\ell^2]=\langle P,Q\rangle$, thus β is a good extension of α. Hence,

$$\ker(\alpha)=\ker(\widehat{\beta}\circ\alpha)\cap(E\times E')[\ell]=\langle([a\ell]P,-\varphi([\ell]P)),([a\ell]Q,-\varphi([\ell]Q))\rangle.$$

Similarly

$$\ker(\beta)=\ker(\widehat{\alpha}\circ\beta)\cap(E\times E')[\ell]=\langle([a\ell]P,\varphi([\ell]P)),([a\ell]Q,\varphi([\ell]Q))\rangle.$$

This implies that α,β are in the same orbit.

By the above claim and Proposition 5.1, an adjacent vertex connects to $E\times E'$ by either two edges whose kernels are nondiagonal or only one edge whose kernel is diagonal. Now the theorem follows from Corollary 2.14 and Theorem 5.2. $\square$

6. Loops and neighborhoods of $[E\times E]$ for $j(E)\in\mathbb{F}_p\backslash\{0,1728\}$

In this section, we assume E is a supersingular elliptic curve over $\mathbb{F}_p$ such that $j(E)\neq 0,\ 1728$. The maximal orders $\mathcal{O}(q)$ and $\mathcal{O}'(q)$ are defined as in §5. Results in this section are parallel to results in §5, with almost identical proof which will be omitted.

6.1. *Kernels of (ℓ,ℓ)-isogenies from $E\times E$*

Note that E is a supersingular elliptic curve over $\mathbb{F}_{p^2}$, we have

$$G:=\mathrm{Aut}(E\times E)=\{[\pm1]\times[\pm1]\}\times\left\{1,\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}\cong(\mathbb{Z}/2\mathbb{Z})^3.$$

Consequently, we have

Proposition 6.1. *The (ℓ,ℓ) isogenies from $E\times E$ can be divided into the following classes, which are unions of G-orbits:*

- (**D**1) $\ker(\varphi)=K_1\times K_2$, *where* $K_1=K_2\subseteq E[\ell]$ *has order* ℓ. *In this case,* $G_\varphi=G$ *and* $O_\varphi=\{\varphi\}$. *This class contains* $\ell+1$ *isogenies.*
- (**D**2) $\ker(\varphi)=K_1\times K_2$, *where* $K_1\neq K_2\subseteq E[\ell]$ *has order* ℓ. *In this case,* $|G_\varphi|=4$ *and* $|O_\varphi|=2$. *This class contains* $\ell(\ell+1)$ *isogenies.*
- (**N**1) *if* $\ell\equiv 1 \pmod 4$, *and* $\ell=a^2+b^2$, $t=-\frac{a}{b}$ *in* $\mathbb{Z}/\ell\mathbb{Z}$, $\ker(\varphi)=\langle (P,tP),(Q,tQ)\rangle$ *or* $\langle (P,-tP),(Q,-tQ)\rangle$, $\langle P,Q\rangle=E[\ell]$. *In this case, the isogeny* φ *corresponds to one of the following two loops of* $[E\times E]$*:*

$$\begin{pmatrix} a & b\\ -b & a\end{pmatrix},\quad \begin{pmatrix} a & b\\ b & -a\end{pmatrix}.$$

- (**N**2) $\ker(\varphi)=\langle (P,aP+bQ),(Q,cP+dQ)\rangle$, *where* $ad-bc=-1$, $a+d=0$, $\langle P,Q\rangle=E[\ell]$. *In this case,* $G_\varphi=\{1,[-1]\times[-1]\}\times\left\{1,\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}$ *and* $|O_\varphi|=2$. *This class contains* $\ell(\ell+1)$ *isogenies.*
- (**N**3) $\ker(\varphi)=\langle (P,aP+bQ),(Q,cP+dQ)\rangle$, *where* $ad-bc=-1$, $a+d\neq 0$, $\langle P,Q\rangle=E[\ell]$. *In this case,* $G_\varphi=\{1,[-1]\times[-1]\}$ *and* $|O_\varphi|=4$. *This class contains* $\ell^3-\ell^2-2\ell-2$ *isogenies if* $\ell\equiv 1\pmod 4$, *and* $\ell^3-\ell^2-2\ell$ *isogenies if* $\ell\equiv 3\pmod 4$.

6.2. Local structure of $[E\times E]$

Theorem 6.2. *Suppose either* $\mathrm{End}(E)=\mathcal{O}(q)$ *and* $p>q\ell>4\ell^2$ *or* $\mathrm{End}(E)=\mathcal{O}'(q)$ *and* $p>4q\ell>4\ell^2$.

1. *If* $\ell\equiv 1\pmod 4$, *then there are exactly two loops of* $E\times E$, *whose kernels are in* (**N**1).
2. *If* $\ell\equiv 3\pmod 4$, *then there is no loop of* $E\times E$.

Theorem 6.3. *Suppose either* $\mathrm{End}(E)=\mathcal{O}(q)$ *and* $p>q\ell^2>4\ell^4$ *or* $\mathrm{End}(E)=\mathcal{O}'(q)$ *and* $p>4q\ell^2>4\ell^4$.

(1) *If* $\ell\equiv 1\pmod 4$, *the neighborhood of* $[E\times E]$ *is given by the following table:*

#Vertices	*Multi-Edges*	*Edge Type*	*#Vertices*	*Multi-Edges*	*Edge Type*
$\ell+1$	*1*	**D**1	$\frac{\ell^2+\ell}{2}$	*2*	**N**2
$\frac{(\ell+1)\ell}{2}$	*2*	**D**2	$\frac{\ell^3-\ell^2-2\ell-2}{4}$	*4*	**N**3

(2) *If* $\ell\equiv 3\pmod 4$, *the neighborhood of is given by the following table:*

#Vertices	*Multi-Edges*	*Edge Type*	*#Vertices*	*Multi-Edges*	*Edge Type*
$\ell+1$	*1*	**D1**	$\frac{\ell^2+\ell}{2}$	*2*	**N2**
$\frac{(\ell+1)\ell}{2}$	*2*	**D2**	$\frac{\ell^3-\ell^2-2\ell}{4}$	*4*	**N3**

7. A simple proof of main theorem in [26]

In this section, we give an alternative proof of the following theorem in [26] without using Deuring's correspondence in [9]. Our new proof is similar to the proof of Proposition 3.12.

Theorem 7.1. *Suppose $\ell > 3$. Consider the ℓ-isogeny graph $\mathcal{G}_\ell(\mathbb{F}_{p^2}, -2p)$ of supersingular elliptic curves over $\mathbb{F}_{p^2}$ of trace $-2p$.*

(1) *If $p \equiv 3 \bmod 4$ and $p > 4\ell^2$, there are $\frac{1}{2}\big(\ell - (-1)^{\frac{\ell-1}{2}}\big)$ vertices adjacent to $[E_{1728}]$ in the graph, each connecting $[E_{1728}]$ with 2 edges. Moreover, $1 + (\frac{\ell}{p})$ of the vertices are of j-invariants in $\mathbb{F}_p - \{1728\}$.*

(2) *If $p \equiv 2 \bmod 3$ and $p > 3\ell^2$, there are $\frac{1}{3}(\ell - (\frac{\ell}{3}))$ vertices adjacent to $[E_0]$ in the graph, each connecting $[E_0]$ with 3 edges. Moreover, $1 + (\frac{-p}{\ell})$ of the vertices are of j-invariants in $\mathbb{F}_p^*$.*

Proof. We will show the case E_{1728}, the case E_0 follows by a parallel argument.

Suppose $p \equiv 3 \pmod 4$. Then $\mathrm{Aut}(E_{1728}) = \{\pm 1, \pm i\}$ where $i^2 = -1$. Suppose ℓ is another prime. If $p > 4\ell^2$, then elements in $\mathcal{O}$ of reduced norm ℓ^2 are actually inside $\mathbb{Z}[i]$. Thus loops from E_{1728} of degree ℓ^2 lie in $\mathbb{Z}[i]$.

If $\ell \equiv 3 \pmod 4$, the only elements in $\mathbb{Z}[i]$ of reduced norm ℓ^2 are $\sigma\ell$ where $\sigma \in \mathrm{Aut}(E_{1728})$, so ℓ is only one loop of degree ℓ^2. If there are two different isogenies φ, ψ from E_{1728} of degree ℓ to the same adjacent vertex, then $\widehat{\psi} \circ \varphi$ is a loop from E_{1728}, which is ℓ. Hence $\varphi = \psi \circ \sigma$ with $\sigma \in \mathrm{Aut}(E_{1728})$. Since φ, ψ are not loops, we have $\ker(\psi) = i(\ker(\varphi)) \neq \ker(\varphi)$. It means an adjacent vertex connects E_{1728} with two edges.

If $\ell \equiv 1 \pmod 4$, let $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = \ell$. Then elements of reduced norm ℓ in $\mathbb{Z}[i]$ are $\sigma(x \pm yi)$ where $\sigma \in \mathrm{Aut}(E_{1728})$, so the loops with degree ℓ from E_{1728} are $x \pm yi$. Elements of reduced norm ℓ^2 are $\sigma(x \pm yi)^2$ and $\sigma\ell$, corresponding to the three loops $(x \pm yi)^2$ and ℓ of degree ℓ^2 on E_{1728}. Furthermore, the first two loops are compositions of a loop of degree ℓ with itself. Hence if there are two different isogenies φ, ψ from E_{1728} with degree ℓ to the same adjacent vertex, then $\widehat{\psi} \circ \varphi$ is a loop of E_{1728}. Since $(x \pm yi)^2 \neq \ell$, we have $\ker((x \pm yi)^2)$ is cyclic (i.e. $\ker((x \pm yi)^2) \cong \mathbb{Z}/\ell^2\mathbb{Z}$). If $\widehat{\psi} \circ \varphi = (x + yi)^2$ or $(x - yi)^2$, then $\ker(\varphi) = \ker(x + yi)$ or $\ker(x - yi)$ which means φ is a loop. Hence we have $\widehat{\psi} \circ \varphi$ is not equal to $(x + yi)^2$ or $(x - yi)^2$. This implies the loop is ℓ, and $\varphi = \psi \circ \sigma$ where $\sigma \in \mathrm{Aut}(E_{1728})$. Since φ, ψ are not loops, we have $\ker(\psi) = i(\ker(\varphi)) \neq \ker(\varphi)$. It means an adjacent vertex connects E_{1728} with two edges. $\square$

Acknowledgment

Zheng Xu and Yi Ouyang were supported by Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0302902), NSFC (Grant No. 12371013), Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200). Zijian Zhou was supported by NSFC (Grant No. 62202475).

Data availability

No data was used for the research described in the article.

References

[1] G. Adj, O. Ahmadi, A. Menezes, On isogeny graphs of supersingular elliptic curves over finite fields, Finite Fields Appl. 55 (2019) 268–283.

[2] W. Castryck, T. Decru, An efficient key recovery attack on SIDH, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer Nature Switzerland, Cham, 2023, pp. 423–447.

[3] W. Castryck, T. Decru, Multiradical isogenies, in: Proceedings of AGC2T18, in: Contemporary Mathematics, vol. 779, 2022, pp. 57–89.

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

[5] D. Charles, K. Lauter, E. Goren, Cryptographic hash functions from expander graphs, J. Cryptol. 22 (1) (2009).

[6] L. Colò, D. Kohel, Orienting supersingular isogeny graphs, J. Math. Cryptol. 14 (1) (2020) 414–437.

[7] W. Castryck, T. Lange, C. Martindale, et al., CSIDH: an efficient post-quantum commutative group action, in: Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III 24, Springer International Publishing, 2018, pp. 395–427.

[8] C. Costello, B. Smith, The supersingular isogeny problem in genus 2 and beyond, in: Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings, Springer International Publishing, Cham, 2020, pp. 151–168.

[9] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Semin. Univ. Hamb. 14 (1941) 197–272.

[10] F.A. Diamond, First Course in Modular Forms, Graduate Texts in Mathematics, Springer-Verlag, 2005, p. 436.

[11] C. Delfs, S. Galbraith, Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$, Des. Codes Cryptogr. 78 (2016) 425–440.

[12] L. De Feo, D. Kohel, A. Leroux, et al., SQISign: compact post-quantum signatures from quaternions and isogenies, in: Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part I 26, Springer International Publishing, 2020, pp. 64–93.

[13] E.V. Flynn, Y.B. Ti, Genus two isogeny cryptography, in: Post-Quantum Cryptography: 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019 Revised Selected Papers 10, Springer International Publishing, 2019, pp. 286–306.

[14] E. Florit, B. Smith, Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph, in: Arithmetic, Geometry, Cryptography, and Coding Theory, American Mathematical Society, 2021, 2021, p. 779.

[15] E. Florit, B. Smith, An atlas of the Richelot isogeny graph. Theory and applications of supersingular curves and supersingular Abelian varieties, https://arxiv.org/abs/2101.00917, 2022.

[16] S.D. Galbraith, C. Petit, J. Silva, Identification protocols and signature schemes based on supersingular isogeny problems, in: Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I 23, Springer International Publishing, 2017, pp. 3–33.

[17] J.G. Huard, Elementary Evaluation of Certain Convolution Sums Involving Divisor Functions, Number Theory for the Millennium, II, AK Peters, 2002.
[18] T. Ibukiyama, On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings, Nagoya Math. J. 88 (1982) 181–195.
[19] T. Ibukiyama, T. Katsura, F. Oort, Supersingular curves of genus two and class numbers, Compos. Math. 57 (2) (1986) 127–152.
[20] S. Ionica, E. Thomé, Isogeny graphs with maximal real multiplication, J. Number Theory 207 (2020) 385–422.
[21] D. Jao, De Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, in: B.-Y. Yang (Ed.), PQCrypto 2011, in: LNCS, vol. 7071, Springer, 2011, pp. 19–34.
[22] B.W. Jordan, Y. Zaytman, Isogeny graphs of superspecial abelian varieties and Brandt matrices, arXiv preprint, arXiv:2005.09031, 2020.
[23] B.W. Jordan, Y. Zaytman, Isogeny complexes of superspecial abelian varieties, arXiv preprint, arXiv:2205.07383, 2022.
[24] T. Katsura, K. Takashima, Counting Richelot Isogenies Between Superspecial Abelian Surfaces, Open Book Series, vol. 4(1), 2020, pp. 283–300.
[25] T. Katsura, K. Takashima, Decomposed Richelot isogenies of Jacobian varieties of hyperelliptic curves and generalized Howe curves, arXiv preprint, arXiv:2108.06936, 2021.
[26] S. Li, Y. Ouyang, Z. Xu, Neighborhood of the supersingular elliptic curve isogeny graph at $j = 0$ and 1728, Finite Fields Appl. 61 (2020) 101600.
[27] S. Li, Y. Ouyang, Z. Xu, Endomorphism rings of supersingular elliptic curves over $\mathbb{F}_p$, Finite Fields Appl. 62 (2020) 101619.
[28] K. McMurdy, Explicit representation of the endomorphism rings of supersingular elliptic curves, Preprint, August, 2014, 20.
[29] L. Maino, C. Martindale, L. Panny, G. Pope, B. Wesolowski, A direct key recovery attack on SIDH, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer Nature Switzerland, Cham, 2023, pp. 448–471.
[30] J.S. Milne, Abelian Varieties, Springer, 1986.
[31] D. Mumford, Abelian Varieties, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Tata Institute of Fundamental Research, Bombay, 2008.
[32] A. Ogus, Supersingular K3 crystals, in: Journées de Géométrie Algébrique de Rennes (Rennes, 1978), vol. II, in: Astérisque, vol. 64, Soc. Math. France, Paris, 1979, pp. 3–86.
[33] Y. Ouyang, Z. Xu, Loops of isogeny graphs of supersingular elliptic curves at $j = 0$, Finite Fields Appl. 58 (2019) 174–176.
[34] D. Robert, Breaking SIDH in polynomial time, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer Nature Switzerland, Cham, 2023, pp. 472–503.
[35] T. Shioda, Supersingular K3 surfaces, in: Algebraic Geometry, Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978, in: Lecture Notes in Math., vol. 732, Springer, Berlin, 1979, pp. 564–591.
[36] J.H. Silverman, The Arithmetic of Elliptic Curves, Springer, New York, 2009.
[37] K. Takashima, Counting superspecial Richelot isogenies by reduced automorphism groups, in: Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties, 2022.