Neighborhoods of vertices in the graph of principally polarized superspecial abelian surfaces

Zijian Zhou

Joint work with Zheng Xu, Yi Ouyang

zhouzijian.edu@gmail.com

5th Pythagorean Conference, Kalamata, Greece, June 1-6, 2025

Elliptic Curves

Elliptic Curves

Elliptic curve is a smooth, projective, algebraic curve of genus one, on which there is a specified point O.
When elliptic curve E defined over field K, $\mathrm{char}(K) \neq 2, 3$, the curve can be written as Weierstrass form

$$y^2 = x^3 + ax + b.$$

According to endomorphism ring, elliptic curves over finite fields can be divided into two types:

Ordinary & Supersingular

If endomorphism ring $\mathrm{End}(E)$ is an order of a quadratic imaginary field, then we say that E is ordinary.
If endomorphism ring $\mathrm{End}(E)$ is an order in a quaternion algebra, then we say that E is supersingular.

Examples of supersingular curves with $j = 0, 1728$

The elliptic curve $E : y^2 = x^3 + x$ of j-invariant 1728 is supersingular if and only if $p \equiv 3 \bmod 4$.
The elliptic curve $E : y^2 = x^3 + 1$ of j-invariant 0 is supersingular if and only if $p \equiv 2 \bmod 3$.

Isogenies

Isogeny

An isogeny is a surjective group homomorphism between two algebraic groups with finite kernel.
In particular, an isogeny $\phi : E_1 \to E_2$ between elliptic curves are a surjective morphism with $\phi(O) = O$.
Any subgroup K of $E_1[\ell]$ can define an isogeny $\phi : E_1 \to E_1/K$, which can be computed by Vélu's formula.

Vélu's formula

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over k and let G be a finite subgroup of $E(\bar{k})$ of odd order. For each nonzero $Q = (x_Q, y_Q)$ in G define

$$t_Q := 3x_Q^2 + A, \quad u_Q := 2y_Q^2, \quad w_Q := u_Q + t_Q x_Q,$$

$$t := \sum_{\substack{Q \in G \\ Q \neq 0}} t_Q, \quad w := \sum_{\substack{Q \in G \\ Q \neq 0}} w_Q, \quad r(x) := x + \sum_{\substack{Q \in G \\ Q \neq 0}} \left(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right).$$

The rational map

$$\alpha(x, y) := (r(x), r'(x)y)$$

is a separable isogeny from E to $E' : y^2 = x^3 + A'x + B'$, where $A' := A - 5t$ and $B' := B - 7w$, with $\ker \alpha = G$. If G is defined over k then so are α and E'.

The Isogeny Path Problem in isogeny-based Crypto

The Mother of All Problems

Given (supersingular) elliptic curves E and E' over a (large) finite field, find a (chain of low-degree) isogenies

$$\phi_n \circ \cdots \circ \phi_1 \ : \ E \to E'.$$

CSIDH/CSI-FiSh

- E and E' are supersingular curves defined over $\mathbb{F}_p$.

SIDH/SIKE

- E and E' are supersingular curves defined over $\mathbb{F}_{p^2}$.
- Additional information given on a secret short chain $E \to E'$;
- In instantiations, E is fixed and special (in a cryptanalytic sense).

SQISign[1]

- Based on the correspondence between ideals/orders quaternion algebra and isogenies/endomorphism rings of supersingular elliptic curves.
- $+$ Random Oracle Model (rewinding).
- Variants: SQISignHD, SQISign2D-West, SQISign2D-East...

[1]NIST PQC signature candidate

The Isogeny Path Problem in isogeny-based Crypto

The Mother of All Problems

Given (supersingular) elliptic curves $\underline{E}$ and $\underline{E'}$ over a (large) finite field, find a (chain of low-degree) isogenies

$$\phi_n \circ \cdots \circ \phi_1 \ : \ E \to E'.$$

Eisenträger et al., 2018:
Computing Isogenies ⇔ Studying Ideals in Maximal Orders ⇔ Finding Paths in Isogeny Graphs

Isogeny graph

The supersingular ℓ-isogeny graphy is the graph whose vertices set V is the supersingular j invariant and an edge between two vertices is associated to ℓ-isogeny between the corresponding curves.

SQISign

- Variants: SQISignHD, SQISign2D-West, SQISign2D-East...

Table: Number of edges from single vertexes in isogeny graph

supersingular elliptic curve	SSPPAS
ℓ-isogeny (kernel $\cong \mathbb{Z}/\ell\mathbb{Z}$)	(ℓ,ℓ)-isogeny (kernel $\cong (\mathbb{Z}/\ell\mathbb{Z})^2$)
$\ell+1$ edges starting from one vertex in graph	$(\ell^2+1)(\ell+1)$ edges in graph

Quaternion Algebra

Quaternion algebra

- Choose a prime q such that $q \equiv 3 \pmod 8$, $\left(\frac{p}{q}\right) = -1$. Then the unique quaternion algebra $B_{p,\infty}$ ramified exactly at p and ∞ can be written as

$$B_{p.\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k,$$

  where $j^2 = -p$, $i^2 = -q$ and $k = ij = -ji$.
- The endomorphism ring of supersingular elliptic curve is a maximal order of quanternion algebra $B_{p,\infty}$.

Example 1

Let E_{1728} denote a supersingular elliptic curves over $\mathbb{F}_{p^2}$ with j-invariant 1728. Then

$$\mathrm{End}(E_{1728}) = \mathbb{Z} + \mathbb{Z}\,i + \mathbb{Z}\,\frac{1+j}{2} + \mathbb{Z}\,\frac{i+k}{2},$$

where $i^2 = -1$, $j^2 = -p$ and $p \equiv 3 \pmod 4$.

Correspondence between elliptic curves and quaternion algebra

Ibukiyama 1982: There is 1-1 correspondence between supersingular j-invariants $j \in \mathbb{F}_p$ and the maximal orders of certain forms in $B_{p,\infty}$.

Deuring 1941, Waterhouse 1969, Kohel 1996: **Deuring Correspondence**

Supersingular curves E over $\mathbb{F}_{p^2}$ *(up to isomorphism)*	Maximal orders in $B_{p,\infty}$ $\mathcal{O} \simeq \mathbf{End}(E)$ *(up to equivalence)*
Isogenies $\varphi : E \longrightarrow F$	Left $\mathcal{O}$-ideals I_φ
Degree $\mathbf{deg}(\varphi)$	Norm $\mathbf{n}(I_\varphi)$

Correspondence between elliptic curves and quaternion algebra

Ibukiyama 1982:There is 1-1 correspondence between supersingular j-invariants $j \in \mathbb{F}_p$ and the maximal orders of certain forms in $B_{p,\infty}$.
Deuring 1941, Waterhouse 1969, Kohel 1996: **Deuring Correspondence**

Deuring Correspondence

Suppose E is a supersingular elliptic curve over $\mathbb{F}_{p^2}$, $\mathrm{End}(E) = \mathcal{O}$ is a maximal order of $B_{p,\infty}$.

For I a left integral ideal of $\mathcal{O}$, let $E[I]$=$\{P \in E \mid \alpha(P) = O$ for every $\alpha \in I\}$, then the isogeny

$$\phi_I : E \to E_I = E/E[I]$$

has $\ker \phi_I = E[I]$ and $\deg(\phi_I) = \mathrm{Nrd}(I)$ the reduced norm of I.

On the other hand, if $\phi : E \to E'$ is an isogeny of degree n, then $\ker \phi$ is of order n and $I_\phi = \{\alpha \in \mathcal{O} \mid \alpha(P) = O$ for all $P \in \ker \phi\}$ is a left $\mathcal{O}$-ideal of reduced norm n.

Correspondence between elliptic curves and quaternion algebra

Ibukiyama 1982:There is 1-1 correspondence between supersingular j-invariants $j \in \mathbb{F}_p$ and the maximal orders of certain forms in $B_{p,\infty}$.
Deuring 1941, Waterhouse 1969, Kohel 1996: **Deuring Correspondence**
Kohel, Lauter, Petit, Tignol 2014, Luca De Feo et al. 2020:

KLPT algorithm: Geometric view of ideal I

For isogeny $\phi : E \to E'$ corresponds to ideal I, we have ideal $I \longleftrightarrow \mathrm{Hom}(E', E) \circ \phi$, i.e. I is the subset of $\mathrm{End}(E)$ encoding the set of all isogenies $E' \to E_0$ with ϕ. The norm of every element of I is divisible by $\deg \phi$ (equal to $\deg \phi$).

Recall,
Computing Isogenies ⇔ Studying Ideals in Maximal Orders ⇔ Finding Paths in Isogeny Graphs

The *isogeny graphs* are essential for harnessing their cryptographic potential in isogeny-based systems.
Do analogous results occur in the context of abelian varieties?

Abelian Varieties

Definition

- *An abelian variety A is a complete connected group variety.*
- *A polarized divisor is an ample divisor D on A, which corresponds to an isogeny (polarization) $\lambda_D : A \to \hat{A}$ from A to its dual.*
- *A principal polarization is a polarization that is an isomorphism. A principally polarized abelian variety (PPAV) is an abelian variety equipped with a principal polarization.*

Remark

An elliptic curve is a principally polarized abelian variety of dimension one.

Counterpart of supersingular elliptic curves

Definition (Supersingular abelian varieties)

A abelian varietyis called supersingular if all slopes of the Newton polygon are $1/2$.

Definition (Sueprspecial abelian varieties)

A abelian variety is called superspecial if Frobenius acts as 0 on $H^1(A, \mathcal{O}_A)$

Remark

Any supersingular abelian variety is **isogenous** to a product of supersingular elliptic curves.
Any superspecial abelian variety is **isomorphic** to a product of supersingular elliptic curves.
Then superspecial $\implies$ supersingular. Hence superspecial (principally polarized) abelian varieties are the right counterpart of the supersingular elliptic curves!

Maximal m-Isotropic Subgroup

A (polarized) isogeny φ between two principally polarized abelian varieties $(A, \lambda_A), (B, \lambda_B)$:

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle [N]\lambda_A}\downarrow & & \downarrow{\scriptstyle \lambda_B} \\ \hat{A} & \xleftarrow[\hat{\varphi}]{} & \hat{B} \end{array}$$

what do the *kernels* of isogenies look like?

Maximal m-Isotropic Subgroup

A (polarized) isogeny φ between two principally polarized abelian varieties $(A, \lambda_A), (B, \lambda_B)$:

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle [N]\lambda_A}\downarrow & & \downarrow{\scriptstyle \lambda_B} \\ \hat{A} & \xleftarrow[\hat{\varphi}]{} & \hat{B} \end{array}$$

what do the *kernels* of isogenies look like?

Mumford 08: the subgroup of abelian variety is the kernel of some isogeny between principally polarized abelian varieties iff it is maximal isotropic.

Definition (m-isotropic subgroup)

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.

Isogenies and Superspecial principally polarized abelian surface (SSPPAS)

A (polarized) isogeny φ between two principally polarized abelian varieties $(A, \lambda_A), (B, \lambda_B)$:

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle [N]\lambda_A}\downarrow & & \downarrow{\scriptstyle \lambda_B} \\ \hat{A} & \xleftarrow[\hat{\varphi}]{} & \hat{B} \end{array}$$

Deligne, Ogus, Shioda, Oort 1979: Any superspecial abelian variety of dimension $g > 1$ defined over $\bar{\mathbb{F}}_p$ is isomorphic to E^g with E a supersingular elliptic curve over $\bar{\mathbb{F}}_p$.

Remark

For superspecial abelian varieties A, B, we have $A \cong B$. Then

$$\{\text{isogenies between SSPPAVs}\} \iff \{\text{endomorphisms} + \text{principally polarizations}\}$$

Moreover, for isogeny between products of ellipti curves $\varphi : E_1 \times E_2 \to E_3 \times E_4$

$$\varphi : \begin{pmatrix} P \\ Q \end{pmatrix} \mapsto \begin{pmatrix} \alpha_{13} & \alpha_{23} \\ \alpha_{14} & \alpha_{24} \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix}$$

with $\alpha_{ij} : E_i \to E_j$ an isogeny or zero map of elliptic curves. A matrix with entries in quanternion algebra!

Isogeny Graph of SSPPAS

Definition

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

1. Isogeny graphs of principally polarized superspecial abelian varieties are connected.
2. The (ℓ,ℓ)-isogeny graph of SSPPAS are assume to be Ramanujan.
3. Finding paths in the isogeny graph leads to constructing isogenies between two SSPPAS.

Isogeny Graph of SSPPAS

Well know results: There are two types of PPSSAS, i.e. the Jacobian and products of supersingular elliptic curves, the numbers of each type increase dramatically as p grows.

Proposition

1. *Jacobian type $\mathcal{J}_p$, consisting of Jacobians of superspecial hyperelliptic curve of genus 2 with the canonical principal polarization $(\mathrm{Jac}(C), C)$, 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 $(E_1 \times E_2, \{0\} \times E_2 + E_1 \times \{0\})$, 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 $\bar{\mathbb{F}}_p$.

Isogeny Graph of SSPPAS

Well know results: There are two types of PPSSAS, i.e. the Jacobian and products of supersingular elliptic curves, the numbers of each type increase dramatically as p grows. Flynn and Ti 2019: the number of edges are "big" enough.

Table: Cryptosystems on supersingular elliptic curve vs on SSPPAS

supersingular elliptic curve	SSPPAS
ℓ-isogeny (kernel $\cong \mathbb{Z}/\ell\mathbb{Z}$)	(ℓ,ℓ)-isogeny (kernel $\cong (\mathbb{Z}/\ell\mathbb{Z})^2$)
$\ell+1$ edges starting from one vertex in graph	$(\ell^2+1)(\ell+1)$ edges in graph

Deuring correspondence in higher dimensions?

In case of dimension one, we have the Deuring Correspondence. Could we have similar results for higher dimensions?

Deuring correspondence in higher dimensions?

In case of dimension one, we have the Deuring Correspondence. Could we have similar results for higher dimensions?

Yes! But we need the matrices with entries in $\mathcal{O} := \mathrm{End}(E)$:

1. $\mathrm{End}(E^g) \cong M_g(\mathcal{O})$, principle polarization $\{0\} \times E^{g-1} + \cdots + E^{g-1} \times \{0\}$
2. $\mathrm{Aut}(E^g) \cong \mathrm{GL}_g(\mathcal{O}) = \{M \in M_g(\mathcal{O}) \mid M \text{ is invertible}\}$.
3. The reduced norm $\mathrm{Nrd} : \mathcal{O} \to \mathbb{Z}$ generalizes to the reduced norm $\mathrm{Nrd} : M_g(\mathcal{O}) \to \mathbb{Z}$. We also have
$$\mathrm{GL}_g(\mathcal{O}) \cong \{M \in M_g(\mathcal{O}) \mid \mathrm{Nrd}(M) = 1\}.$$
4. $\mathrm{End}(A) \cong M_g(\mathcal{O})$ for any SSAV of dimension g, this is induced by the isomorpism $\iota_A : A \to E^g$.

Polarization and Positive Definite Matrices

Put $\mathcal{H} \subseteq M_n(\mathcal{O})$ the subset of positive-definite Hermitian matrices of reduced norm 1 . Consider group action:

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

Jordan and Zaytman 2020: there is a one-to-one correspondence between $\mathcal{H} / \mathrm{GL}_g(\mathcal{O})$ and the set of isomorphism classes of PPSSAV of dimension g.

Particularly:

Ibukuyama, Katsura and Oort 1986: For $g = 2$ and $d \in \mathbb{Z}_+$, there is a one-to-one correspondence

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

NS(A): $\mathrm{NS}(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$ the Néron-Severi group

We can compute!

1. Compute the number of matrices $M \in M_2(\mathcal{O})$ such that $M^+ M = \ell I$,
2. Then the number of loops at $E_{1728} \times E_{1728}$ = number of equivalent classes of M after acting automorphism groups.

For instances, since $p > 4\ell$, the number of $M \in M_2(\mathcal{O})$ such that $M^+ M = \ell I$ is equal to the number of integer solutions of $x^2 + y^2 + z^2 + w^2 = \ell$.

Loops at $E_{1728} \times E_{1728}$ in $\mathcal{G}_{p,\ell}$

Recall that the out-degree of every vertex in $\mathcal{G}_p$ is $(\ell+1)(\ell^2+1)$.
The number of loops at $E_{1728} \times E_{1728}$ in the (ℓ,ℓ)-isogeny graph is given by

Theorem 1

Let $p \equiv 3 \pmod 4$ be a prime and E_{1728} be the supersingular elliptic curve over $\mathbb{F}_p$ with j-invariant 1728. Suppose $p > 4\ell$.

1. *if $\ell \equiv 1 \bmod 4$, then $E_{1728} \times E_{1728}$ has $\ell + 3$ loops;*
2. *if $\ell \equiv 3 \bmod 4$, then $E_{1728} \times E_{1728}$ has $\ell + 1$ loops;*
3. *if $\ell = 2$, then $E_{1728} \times E_{1728}$ has 3 loops.*

Neighborhood of $E_{1728} \times E_{1728}$ in $\mathcal{G}_{p,\ell}$

Theorem 2

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.*

Loops at $E_0 \times E_0$ in $\mathcal{G}_{p,\ell}$

The number of loops at $E_0 \times E_0$ in the (ℓ, ℓ)-isogeny graph is given by

Theorem 3

Let $p \equiv 2 \pmod 3$ *be a prime and* E_0 *be the supersingular elliptic curve over* $\mathbb{F}_p$ *with* j*-invariant* 0. *Suppose* $p > 3\ell$.

1. *if* $\ell \equiv 1 \bmod 3$, *then* $E_0 \times E_0$ *has* $\ell + 3$ *loops;*
2. *if* $\ell \equiv 2 \bmod 3$, *then* $E_0 \times E_0$ *has* $\ell + 1$ *loops;*
3. *if* $\ell = 3$, *then* $E_0 \times E_0$ *has* 1 *loops.*

Neighborhood of $E_0 \times E_0$ in $\mathcal{G}_{p,\ell}$

Theorem 4

Suppose $p > 3\ell^2$. Consider the neighborhood of $[E_0 \times E_0]$.
(1) *If $\ell \equiv 1 \mod 3$, 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 $\ell \equiv 2 \mod 3$, 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,*

Loops of $E \times E'$

Theorem 5

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* $E \times E'$.

Neighborhood of $E \times E'$

Theorem 6

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**

Loops of $E \times E$

Theorem 7

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* $(\mathbf{N}1)$.
2. *If* $\ell \equiv 3 \pmod 4$, *then there is no loop of* $E \times E$.

Neighborhood of $E \times E$

Theorem 8

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	$\mathbf{D}1$	$\frac{\ell^2+\ell}{2}$	2	$\mathbf{N}2$
$\frac{(\ell+1)\ell}{2}$	2	$\mathbf{D}2$	$\frac{\ell^3-\ell^2-2\ell-2}{4}$	4	$\mathbf{N}3$

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	$\mathbf{D}1$	$\frac{\ell^2+\ell}{2}$	2	$\mathbf{N}2$
$\frac{(\ell+1)\ell}{2}$	2	$\mathbf{D}2$	$\frac{\ell^3-\ell^2-2\ell}{4}$	4	$\mathbf{N}3$

Thanks for listening!

- G. Adj, O. Ahmadi, A. Menezes, On isogeny graphs of supersingular elliptic curves over finite fields, Finite Fields Appl. **55** (2019), 268-283.
- E. Florit, B. Smith, Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph. Arithmetic, Geometry, Cryptography, and Coding Theory 2021. American Mathematical Society, 2021, 779.
- B. W. Jordan, Y. Zaytman, Isogeny graphs of superspecial abelian varieties and Brandt matrices. arXiv preprint arXiv:2005.09031, 2020.
- B. W. Jordan, Y. Zaytman, Isogeny complexes of superspecial abelian varieties. arXiv preprint arXiv:2205.07383, 2022.
- S. Li, Y. Ouyang, Z. Xu, Endomorphism rings of supersingular elliptic curves over $\mathbb{F}_p$, Finite Fields Appl. **62** (2020), 101619.
- D. Mumford, Abelian Varieties. Tata Institute of Fundamental Research Studies in Mathematics, vol. 5. Tata Institute of Fundamental Research, Bombay (2008).
- A. Ogus, Supersingular K3 crystals. Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. II, pp. 3–86, Astérisque, 64, Soc. Math. France, Paris, 1979.
- Y. Ouyang, Z. Xu, Loops of isogeny graphs of supersingular elliptic curves at $j = 0$, Finite Fields Appl. **58** (2019), 174-176.
- T. Shioda, Supersingular K3 surfaces. Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978), pp. 564–591, Lecture Notes in Math., 732, Springer, Berlin, 1979.
- Z. Xu, Y. Ouyang, Z. Zhou, Neighborhood of vertices in the isogeny graph of principally polarized superspecial abelian surfaces. Finite Fields and Their Applications, **103** (2025), 102579.