Adding Level Structure to Supersingular Elliptic Curve Isogeny Graphs

Sarah Arpin, University of Colorado Boulder

sarah.arpin@colorado.edu

UC Irvine Number Theory Seminar

October 14th, 2021

Table of Contents

Supersingular Elliptic Curves

Definition (Chapter V[Sil09])

Let E be an elliptic curve defined over a field K of characteristic $p \neq \infty$. E is **supersingular** iff one of the following equivalent conditions hold:

- the multiplication-by-p map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$,
- $\mathrm{End}(E)$ is a maximal order in a quaternion algebra.

For a given p, there are finitely many isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$.

Convention

p: a fixed **large** prime (cryptographic size)
$p \equiv 3 \pmod 4$ (minor adjustments for other p)

Frobenius Isogeny

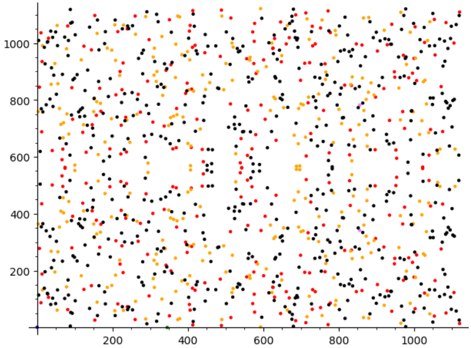
p-power Frobenius map $\pi_p : E \to E^{(p)}$
$\pi_p(x, y) = (x^p, y^p)$

- Induced by the field automorphism
- $a \in \mathbb{F}_p$, then $a^p = a$.
- If $E : y^2 = x^3 + ax + b$, then $E^{(p)} : y^2 = x^3 + a^p x + b^p$
- $j(E)^p = j(E^{(p)})$

Figure: https://commons.wikimedia.org/wiki/File:GeorgFrobenius_(cropped).jpg

Torsion Subgroups

The points of an elliptic curve form a group under addition [Sil09]. Below I have the same 'picture' of a supersingular elliptic curve over F_{1123}, this time the points are different colors according to their order in the group:



Blue = 1, green = 2, violet = 4, red = 281, orange = 562, black = 1124.

Isogenies

Definition

An **isogeny** $\phi : E_1 \to E_2$ is a morphism between elliptic curves such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. It has a dual $\widehat{\phi} : E_2 \to E_1$.

Theorem (Corollary III.4.9 and Proposition III.4.12 [Sil09])

The kernel of a nonzero isogeny is a finite group. A given finite subgroup of points uniquely determines a separable isogeny.

Theorem (Theorem III.4.10(c) [Sil09])

The degree of a separable isogeny is equal to the size of the kernel.

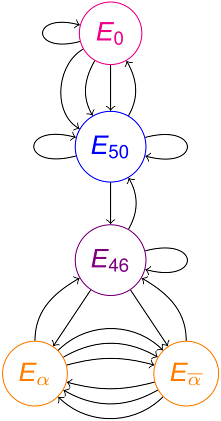
Convention

Isogenies will be degree ℓ or ℓ^r, with ℓ a small prime.

Supersingular elliptic curves over $\overline{\mathbb{F}}_p$ are all ℓ-power isogenous.

Supersingular ℓ-isogeny graph

$p = 53$, $\ell = 3$



- With the right conditions on p, can be taken to be *undirected* by identifying isogenies with their duals
- Connected
- Out-degree $\ell + 1$
- $\sim \lfloor \frac{p}{12} \rfloor$ nodes

Quaternion Algebras

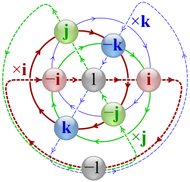


Figure: https://en.wikipedia.org/wiki/File:Cayley_Q8_quaternion_multiplication_graph.svg

Definition (Quaternion algebra ramified at p and ∞)

$B_{p,\,1}$: $\mathbb{Q}\langle i, j, ij\rangle$ such that $i^2 = -1$, $j^2 = -p$, and $ij = -ji$

If $E/\overline{\mathbb{F}}_p$ is supersingular, then $\mathrm{End}(E)$ is isomorphic to a maximal order in $B_{p,\,1}$.

Quaternion Algebras: A Comparison to Number Fields

Quaternion Algebra	Number Field
Noncommutative	Commutative
$B_{p,\,\infty}/\mathbb{Q}$	$K/\mathbb{Q}$
Maximal orders (finitely many)	$\mathcal{O}_K$
Eichler orders of level N	Orders of conductor N: $\mathbb{Z} + N\mathcal{O}_K$
Class set of left or right ideals Class group of two-sided ideals	Class group of ideals

Deuring Correspondence

A categorical equivalence:

Theorem (Deuring Correspondence, [Deu41])

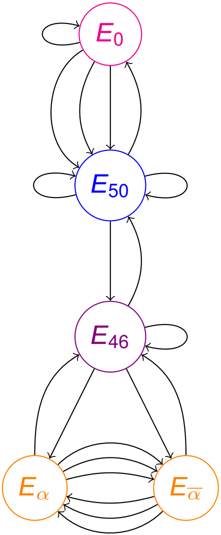
There is a bijection between isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and left ideal classes of a fixed maximal order $\mathcal{O}$ of $B_{p,\infty}$.

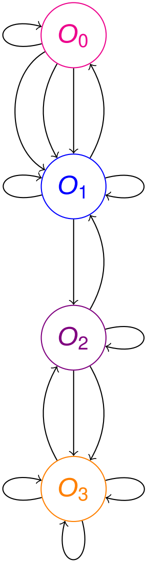
Theorem (Deuring Correspondence II)

If $E/\overline{\mathbb{F}}_p$ is supersingular, then there is a maximal order $\mathcal{O}$ of $B_{p,\infty}$ such that $\mathrm{End}(E) \cong \mathcal{O}$. This association is either 2-1 or 1-1, depending on the size of the two-sided ideal class group of $\mathcal{O}$.

The Deuring correspondence is **not** computationally feasible, in terms of runtime.

Quaternion $\mathcal{G}_{p,\ell}$, $p = 53$, $\ell = 3$





Cryptographic Motivation

Post-Quantum Cryptography

- NIST: 2015 call for proposals of post-quantum safe cryptography protocols. Now in Round 3.
- Supersingular Isogeny Graph Cryptography: $\sim$ 15 years old: original hash function by Charles-Goren-Lauter [**CGL06**]; SIKE key exchange [**SIKE**]

Hard Problems

- Path-finding in supersingular ℓ-isogeny graph
- Path-finding with additional torsion point information

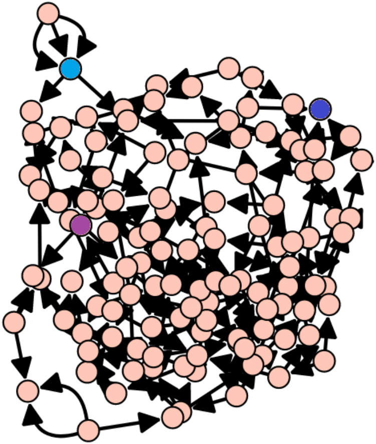
Supersingular Isogeny Diffie-Hellman (SIKE)

Alice	Public	*Babette*
	E	
$\xleftarrow{\varphi_A}$		$\xrightarrow{\varphi_B}$
E_A		E_B
E_B + $\varphi_B(P_A), \varphi_B(Q_A)$		E_A + $\varphi_A(P_B), \varphi_A(Q_B)$
$\downarrow$ "φ_A"		$\downarrow$ "φ_B"
"φ_A"$(E_B) \cong E_2$		"φ_B"$(E_A) \cong E_2$

φ_A is degree $\ell_A^{e_A}$ and φ_B is degree $\ell_B^{e_B}$
$E[\ell_A^{e_A}] = \langle P_A, Q_A \rangle$ and $E[\ell_B^{e_B}] = \langle P_B, Q_B \rangle$

Hard Problems

1. Given E_1, E_2, find an ℓ^n-isogeny between them.
2. Given E, $\varphi_A(E)$, and $\varphi_B(E)$, $\varphi_A(P_B)$, $\varphi_A(Q_B)$, $\varphi_B(P_A)$, and $\varphi_B(Q_A)$, find $\varphi_A(\varphi_B(E)) \cong \varphi_B(\varphi_A(E))$.



How to study security?

Deuring Correspondence

- Relationships between underlying hard problems [Eis+18]. The path-finding problem is equivalent to computing the Deuring correspondence.
- The path-finding problem for quaternion algebras has been solved [Koh+14].

Graph Structure

- It is easier to path-find between $\mathbb{F}_p$ points of $\mathcal{G}_{p,\ell}$ [DG16]
- The structure of the subgraph of $\mathbb{F}_p$-points of $\mathcal{G}_{p,\ell}$ is known [Arp+19]
- Public torsion point information could be a weakness [Pet17] [Que+21]. More investigation is needed.

Isogeny Graph $\mathcal{E}_{p,\ell}^{N}$ With Level Structure

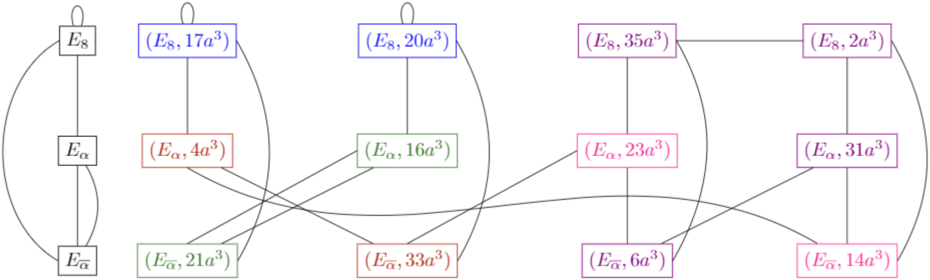
Idea: Keep track of $\varphi_A(P_B), \varphi_A(Q_B)$ in the supersingular ℓ-isogeny graph

- Nodes: (E, G)
  - E: supersingular elliptic curve
  - $G \quad E(\overline{\mathbb{F}}_p)$ of (small) prime order N
- Edges: $(E, G) - (E', G')$ corresponding to an ℓ-isogeny φ:
  - $\varphi(E) = E'$
  - $\varphi(G) = G'$

Graph Properties

- $(N + 1)$ nodes for every node of $\mathcal{G}_{p,\ell}$.
- $(\ell + 1)$-regular, just like $\mathcal{G}_{p,\ell}$
- $\mathcal{E}_{p,\ell}^{N}$ is connected, just like $\mathcal{G}_{p,\ell}$

$p = 37$, $\ell = 2$, $N = 3$



- Black graph on the left: $\mathcal{G}_{p,\ell}$ Supersingular 2-isogeny graph for $p = 37$
- Colorful graph on the right: $\mathcal{E}^3_{37,2}$ Supersingular 2-isogeny graph for $p = 37$ with added level structure for $N = 3$.
- We can see how 2-isogenies act (differently) on 3-torsion points

The Quaternion Picture

What is the endomorphism ring of a node of $\mathcal{E}_{p,\ell}^N$?

$\mathrm{End}(E, G) := \{\alpha \in \mathrm{End}(E) : \alpha(G) \subseteq G\}$

Theorem (Arpin)

$\mathrm{End}(E, G)$ is isomorphic to an Eichler order of level $|G|$ of $B_{p,\,1}$.

Equivalence of Categories

- $\mathcal{S}_N$
  - Objects: Pairs (E, G) with E a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and an order N subgroup $G \subseteq E[N]$
  - Morphisms: $(E, G) \to (E', G')$ a nonzero isogeny $\psi : E \to E'$ such that $\psi(G) \subseteq G'$.
- $\mathcal{LM}$
  - Objects: invertible left $\mathrm{End}(E, G)$-modules
  - Morphisms: nonzero left $\mathrm{End}(E, G)$-module homomorphisms.

Theorem (Arpin)

Fix $(E, G) \in \mathcal{S}_N$. $Hom(-, (E, G)) : \mathcal{S}_N^{op} \to \mathcal{LM}$ is a contravariant equivalence of categories.

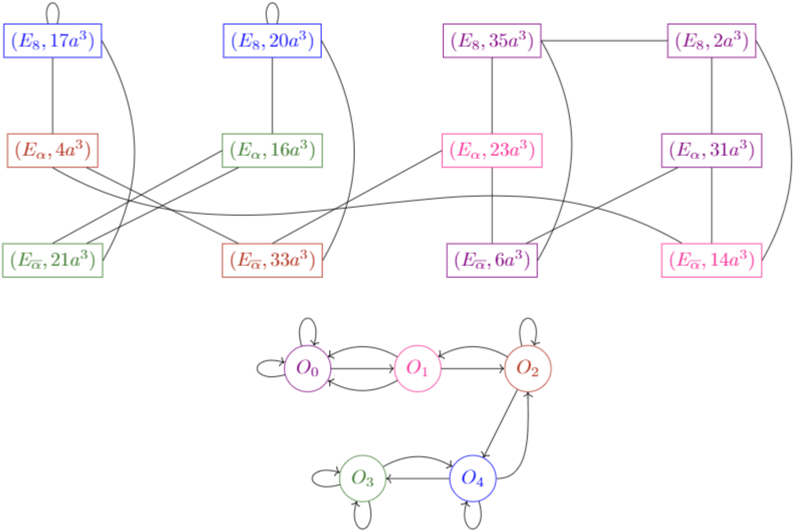
Correspondence to Eichler Orders

Theorem (Arpin)

Given a pair $(E, G) \in \mathcal{E}_{p,\ell}^{N}$, there is an Eichler order $\mathcal{O}$ of level N in $B_{p,\infty}$ such that End$(E, G) \cong \mathcal{O}$. This association is either 4-1, 2-1, or 1-1, depending on the size of the two-sided ideal class group of $\mathcal{O}$.*

*Curves with extra automorphisms ($j = 0, 1728$) may not conform.

$p = 37$, $N = 3$, $\ell = 2$


$(E_8, 17a^3)$
$(E_8, 20a^3)$
$(E_8, 35a^3)$
$(E_8, 2a^3)$
$(E_\alpha, 4a^3)$
$(E_\alpha, 16a^3)$
$(E_\alpha, 23a^3)$
$(E_\alpha, 31a^3)$
$(E_{\overline{\alpha}}, 21a^3)$
$(E_{\overline{\alpha}}, 33a^3)$
$(E_{\overline{\alpha}}, 6a^3)$
$(E_{\overline{\alpha}}, 14a^3)$
O_0
O_1
O_2
O_3
O_4

Coincidence of End(E, G)

What are the reasons for 4-1, 2-1, or 1-1 maps from endomorphism rings of pairs (E, G) to Eichler orders? (Arpin)

Four nodes of $\mathcal{E}^N_{p,\ell}$ with isomorphic endomorphism rings: $\mathcal{O}$:

1. (E, G), where G is the kernel of an isogeny $\varphi_G : E \to E'$,
2. $(E^{(p)}, G^{(p)})$, where $G^{(p)}$ is the image of G under π_p,
3. (E', G'), where E' is the codomain of φ_G and $G' = \ker(\widehat{\varphi})$,
4. $((E')^{(p)}, (G')^{(p)})$, where $(G')^{(p)}$ is the image of G' under π_p

The possibilities for coincidence of the above nodes are:

1. All four distinct.
2. $(E, G) = (E^{(p)}, G^{(p)})$ and $(E', G') = ((E')^{(p)}, (G')^{(p)})$.
3. $(E, G) = (E', G')$ and $(E^{(p)}, G^{(p)}) = ((E')^{(p)}, (G')^{(p)})$.
4. $(E, G) = ((E')^{(p)}, (G')^{(p)})$ and $(E', G') = (E^{(p)}, G^{(p)})$.
5. $(E, G) = ((E')^{(p)}, (G')^{(p)}) = (E', G') = (E^{(p)}, G^{(p)})$.

Case 4: N-isogenous conjugate pair.
Case 5: For suitable p, not going to happen.

Mirror Paths

Frobenius acts on the $\mathcal{G}_{p,\ell}$: if $\varphi : E_1 \to E_2$ is an ℓ-isogeny, then there exists an ℓ-isogeny $E_1^{(p)} \to E_2^{(p)}$.
How do can these paths connect?

- α_i: j-invariants in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$
- a: j-invariant in $\mathbb{F}_p$

Option 1: Through an $\mathbb{F}_p$ vertex

$$\alpha_0 \;—\; \alpha_1 \;—\; a \;—\; \overline{\alpha}_1 \;—\; \overline{\alpha}_0$$

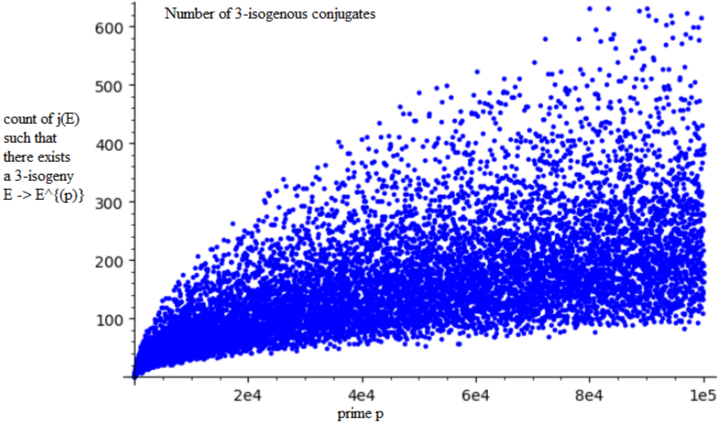
Option 2: Through an ℓ-isogenous pair of conjugate vertices

$$\alpha_0 \;—\; \alpha_1 \;—\; \alpha_2 \;—\; \overline{\alpha}_2 \;—\; \overline{\alpha}_1 \;—\; \overline{\alpha}_0$$

How often are paths of the second type?

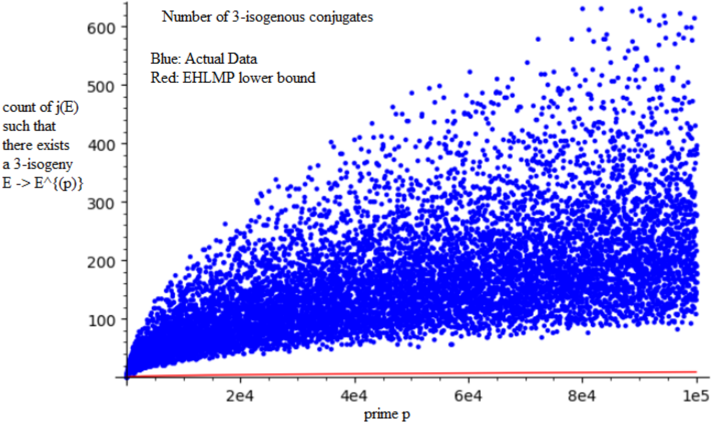
How often are conjugate j-invariants 3-isogenous?

Data: [Arp+19].



How often are conjugate j-invariants 3-isogenous?

Data: [Arp+19]. Lower bound: [Eis+20] Eisentraeger, Hallgren, Leonardi, Morrison, Park



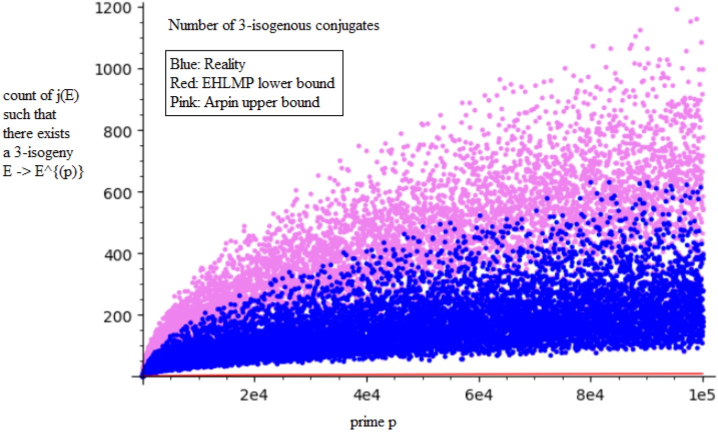
A Bound From Quaternion Algebras

Using the fact that some of the 2-1 associations to Eichler orders are due to N-isogenous conjugate pairs, I obtain an upper bound:

$$4T - (N+1)(\#\mathcal{S}_p)$$

How often are conjugate j-invariants 3-isogenous?

Data: [Arp+19]. Lower bound: [Eis+20] Eisentraeger, Hallgren, Leonardi, Morrison, Park Upper bound: Arpin



An Exact Count

Theorem (Arpin, Chenu-Smith [CS21])

$\alpha(1)$: *number of pairs (E, ψ), where E is a supersingular elliptic curve and ψ is a degree-N isogeny E to $E^{(p)}$.*
$2\alpha(1)$ *equals the number of pairs of a supersingular elliptic curve E and an embedding $\mathbb{Z}[\sqrt{-pN}]$ into $End(E)$.*

$$2\alpha(1) = \begin{cases} |\,\mathcal{C}l(\mathbb{Z}[\frac{1+\sqrt{\ \ pN}}{2}])\,| + |\,\mathcal{C}l(\mathbb{Z}[\sqrt{-pN}])\,| & , -pN \equiv 3 \pmod 4 \\ |\,\mathcal{C}l(\mathbb{Z}[\sqrt{-pN}])\,| & , -pN \equiv 1 \pmod 4 \end{cases}$$

(The factor of two appears because two embeddings which differ by a factor of 1 on the generator $\sqrt{\ \ pN}$ are counted as distinct, whereas the two isogenies ψ, ψ are not considered distinct.)

Summary

- The structure of $\mathcal{G}_{p,\ell}$ can be analyzed through properties of $\mathcal{E}^{N}_{p,\ell}$.
- Supersingular isogeny graph cryptographic protocol seems very safe so far, but more research is always needed.
- Counting isogenous conjugate pairs relates to answering questions about the two-sided ideal class group of an Eichler order.

Thank You !

Reference I

Sarah Arpin et al. **Adventures in Supersingularland**. 2019. arXiv: 1909.07779 [math.NT].

Mathilde Chenu and Benjamin Smith. **Higher-degree supersingular group actions**. 2021. arXiv: 2107.08832 [cs.CR].

Max Deuring. "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.". In: **Abh. Math. Sem. Hansischen Univ.** 14 (1941), pp. 197–272.

Christina Delfs and Steven D. Galbraith. "Computing isogenies between supersingular elliptic curves over F_p". In: **Des. Codes Cryptogr.** 78.2 (2016), pp. 425–440. ISSN: 0925-1022. DOI: 10.1007/s10623-014-0010-1.

Reference II

Kirsten Eisenträger et al. "Supersingular isogeny graphs and endomorphism rings: reductions and solutions". In: **Advances in cryptology—EUROCRYPT 2018. Part III**. Vol. 10822. Lecture Notes in Comput. Sci. Springer, Cham, 2018, pp. 329–368.

Kirsten Eisentraeger et al. **Computing endomorphism rings of supersingular elliptic curves and connections to pathfinding in isogeny graphs**. 2020. arXiv: 2004.11495 [math.NT].

David Kohel et al. "On the quaternion ℓ-isogeny path problem". In: **LMS J. Comput. Math.** 17.suppl. A (2014), pp. 418–432. DOI: 10.1112/S1461157014000151.

Reference III

- Christophe Petit. "Faster algorithms for isogeny problems using torsion point images". In: **Advances in cryptology—ASIACRYPT 2017. Part II**. Vol. 10625. Lecture Notes in Comput. Sci. Springer, Cham, 2017, pp. 330–353. DOI: 10.1007/978-3-319-70697-9_12.
- Victoria de Quehen et al. **Improved torsion point attacks on SIDH variants**. 2021. arXiv: 2005.14681 [math.NT].
- Joseph H. Silverman. **The arithmetic of elliptic curves**. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6.