Arpin - Martindale - Lecture IV

Class Group Actions in HD isogeny-based cryptography

CSIDH - Castryck - Lange - Martindale - Panny - Renes

Isogeny - Based Protocol

Features $\mathbb{F}_p$ - isogeny graph

- Vertices / $\mathbb{F}_p$
- Isogenies come from imaginary quadratic order's class group

Want a "Kani" rep./eval. of such isogenies

Orientations on Elliptic Curves

E : elliptic curve / $\mathbb{F}_q$

K : imaginary quadratic field st

$$\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$$

$\mathcal{O}$: order in K such that

$$\iota(\mathcal{O}) = \iota(K) \cap \mathrm{End}(E)$$

<u>Def</u>: (E, ι) "K-oriented elliptic curve"

E is primitively $\mathcal{O}$-oriented

An isogeny $\varphi : E \to E'$ induces an orientation on E':

$$\iota'(-) = \frac{1}{\deg \varphi} \varphi \circ \iota(-) \circ \hat{\varphi}$$

$$SS_{\mathcal{O}}^{pr} = \left\{ (E, \iota) : \begin{array}{l} E \text{ supersing.} \\ \iota : \text{prim. } \mathcal{O}\text{-orien.} \end{array} \right\} / \cong$$

Three flavors of isog.: $\deg \varphi = \ell$

Let $\mathcal{O}'$ denote the order ι' is primitive wrt.

1) $\mathcal{O}' = \mathcal{O}$ $\quad \varphi$ is horizontal

2) $[\mathcal{O}' : \mathcal{O}] = \ell$ $\quad \varphi$ is ascending

3) $[\mathcal{O} : \mathcal{O}'] = \ell$ $\quad \varphi$ is descending

Types 1) and 2) come from ideals

$$\mathfrak{a} \subseteq \mathcal{O}, \quad N(\mathfrak{a}) = \ell.$$

$\varphi_{\mathfrak{a}}$ has kernel: $E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha))$

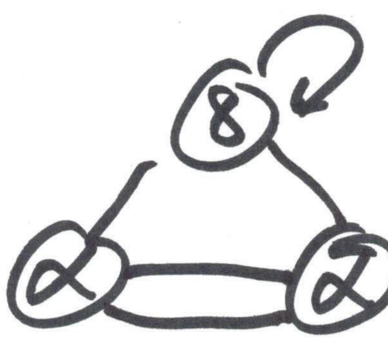
<u>horizontal</u> when $N(\mathfrak{a})$ is coprime to the conductor $f(\mathcal{O})$ of $\mathcal{O}$

$\underline{Cl(\mathcal{O})}$ $\circlearrowright$ $SS_{\mathcal{O}}^{pr}$ free and

$\begin{cases} \text{transitive if } p \text{ is ramified in } K \\ 2 \text{ orbits if } p \text{ is inert} \end{cases}$

Isogeny graphs of oriented scc's

"Usual" 2-isog. graph over $\overline{\mathbb{F}}_{37}$



$\iota_8 : \mathbb{Z}[\sqrt{-2}] \hookrightarrow \mathrm{End}(E_8)$

$Cl(\mathbb{Z}[\sqrt{-2}]) = \{[1]\}$

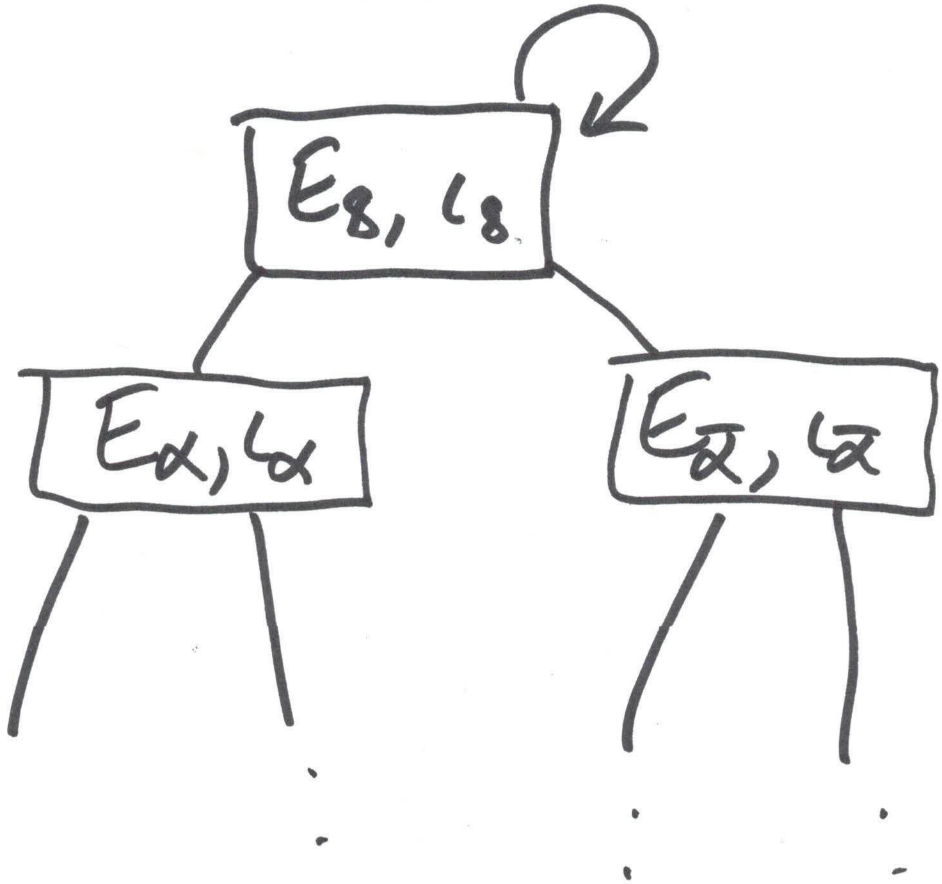
(37) inert $\to$ 2 orbits related by Frob.

$(2) = (\sqrt{-2})^2$ ramified

$\mathbb{Z}[\sqrt{-2}]$

$\mathbb{Z}[2\sqrt{-2}]$
class # 2

$\mathbb{Z}[4\sqrt{-2}]$
class # 4



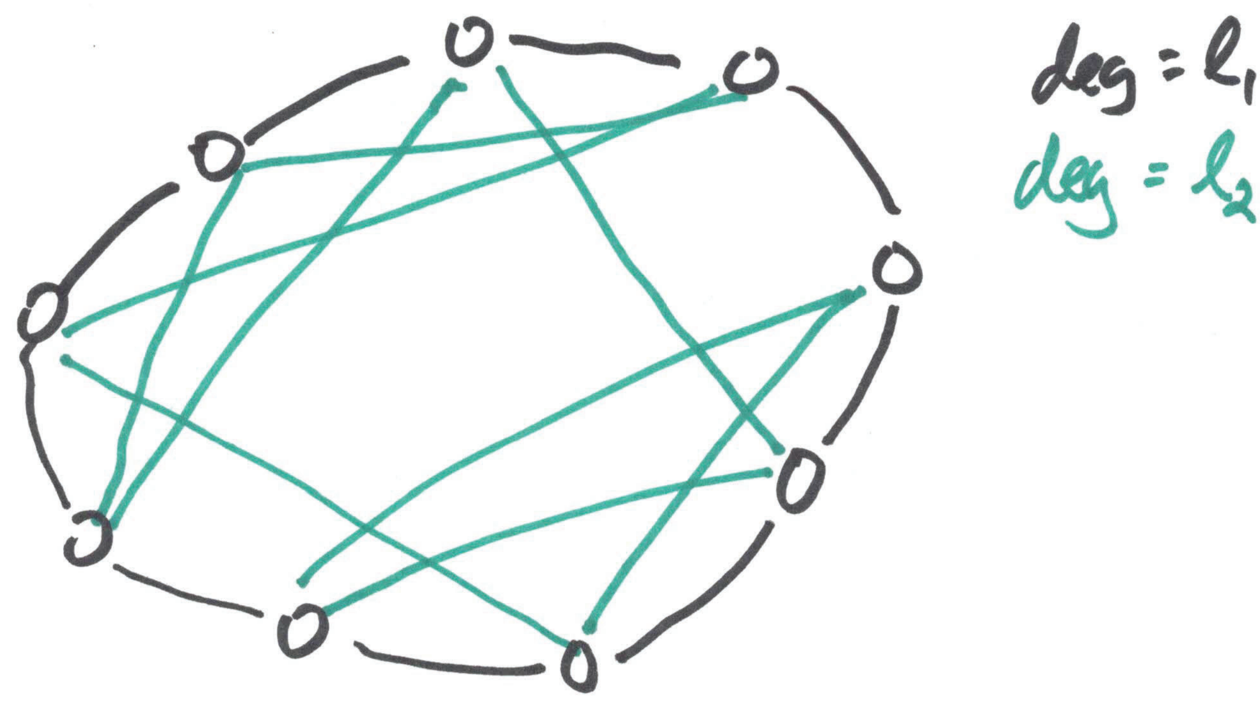
CSIDH-Style Isogeny Graph

$p = 4 \cdot \ell_1 \cdot \ell_2 \cdots \ell_r - 1$

Consider $\mathbb{Z}[\sqrt{-p}] \hookrightarrow \mathrm{End}(E)$

happens for every supersingular e.c. $/ \mathbb{F}_p$

$\rightsquigarrow SS^{pr}_{\mathbb{Z}[\sqrt{-p}]}$



$Cl(\mathbb{Z}[\sqrt{-p}]) \circlearrowright SS^{pr}_{\mathbb{Z}[\sqrt{-p}]}$

Clapoti (Page - Robert)

$E \in SS_{\mathcal{O}}^{pr}$ and $[\mathfrak{a}] \in Cl(\mathcal{O})$

$\varphi_{\mathfrak{a}} : E \to E_{\mathfrak{a}}$ ← want to get $E_{\mathfrak{a}}$

Proposition: Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be integral $\mathcal{O}$-ideals coprime to $f(\mathcal{O})$ suppose $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}] \in Cl(\mathcal{O})$, $N(\mathfrak{b})$ and $N(\mathfrak{c})$ coprime, $\exists$ $(N = (N(\mathfrak{b}) + N(\mathfrak{c})))$-isogeny

$\Phi : E \times E \to E_{\bar{\mathfrak{a}}} \times E_{\mathfrak{a}}$ w/

$\ker \Phi = \{([N(\mathfrak{b})]P, (\varphi_{\mathfrak{b}} \circ \varphi_{\bar{\mathfrak{c}}})P : P \in E[N]\}$

$$\begin{tikzcd} E \arrow[r, "\varphi_{\mathfrak{a}}"] \arrow[d, "\varphi_{\bar{\mathfrak{c}}}"] & E_{\mathfrak{a}} \arrow[d, "\varphi_{\bar{\mathfrak{c}}}"] \\ E_{\bar{\mathfrak{c}}} \arrow[r, "\varphi_{\mathfrak{b}}"] & E \end{tikzcd}$$

$$\overset{2^r}{\cancel{N}} = N(\mathfrak{b}) + N(\mathfrak{c})$$

Let $p = c \cdot 2^e - 1$

so $E/\mathbb{F}_p$ has

$$\# E(\mathbb{F}_p) = p+1 = c \cdot 2^e$$

Goal: Find $\mathfrak{b}, \mathfrak{c}$ equiv. to $\mathfrak{a}$

satisfying: $\boxed{N(\mathfrak{b}) + N(\mathfrak{c}) = 2^r}$

<u>Lemma 2.5 (Page-Robert)</u> Given invertible $\mathfrak{a} \subseteq \mathcal{O}$ there is a randomized poly. time alg. to find $\mathfrak{b}, \mathfrak{c}$ in the same class as $\mathfrak{a}$ w/ norm poly. in $\Delta_{\mathcal{O}}$ <u>and coprime</u>.

Next: Need to ensure $N(\mathfrak{b}) + N(\mathfrak{c})$ is 2^r (or "nice")

Remarks:

1) $\boxed{uN(b) + vN(c) = 2^r}$ where

u and v can be written

$$u = u_1^2 + u_2^2 \qquad v = v_1^2 + v_2^2$$

~~2)~~ PEGASIS, qt-PEGASIS

2) Translate quaternion ideals in this framework: Qlapoti

3) KLaPoTi: use KLPT to solve this equation

qt - PEGASIS

Input: $E/\mathbb{F}_p$, $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\omega]$

$\mathfrak{a} = (N, \alpha)$ is an ideal of

Output: $\varphi_{\mathfrak{a}}(E) = E_{\mathfrak{a}}$

Via Nested Kani diagrams.