KU LEUVEN

Generalized class group actions on oriented elliptic curves with level structure

S. Arpin, W. Castryck, J. Eriksen, G. Lorenzon, F. Vercauteren

The Isogeny Club S05E03

November 5, 2024

Orientations

- Commutative group actions
- Isogeny volcanoes

Level structures

- Rapid mixing graphs
- Security assumptions reductions

CSIDH with full level structure [GPV23]

...

Orientations

- Commutative group actions
- Isogeny volcanoes

Level structures

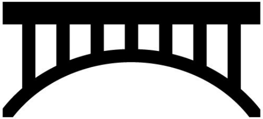
- Rapid mixing graphs
- Security assumptions reductions

CSIDH with full level structure [GPV23]

...

Orientations

- Commutative group actions
- Isogeny volcanoes



Level structures

- Rapid mixing graphs
- Security assumptions reductions

Overview

- Orientations, class group actions, level structures

  SCALLOP, CSIDH with full level structure
- A bigger story: generalized class group actions
- A family of generalized class groups
- Back to starting examples
- Security comments

Some notation:

- k field, char $k = p \geq 5$
- E/k elliptic curve defined over k
- K imaginary quadratic number field
- O, O' orders of K, namely subrings and free $\mathbb{Z}$-modules of rank 2
- f conductor of some $O' \subseteq O$, namely the index $[O : O']$

- I_O the group of invertible fractional ideals of O
- $P_O \leq I_O$ the subgroup of principal fractional ideals

The (ideal) class group of O is

$$\mathrm{cl}_O := \frac{I_O}{P_O}$$

- $\mathfrak{a} \subseteq O$ invertible ideal, $[\mathfrak{a}] \in \mathrm{cl}_O$
- $N(\mathfrak{a})$ the norm of $\mathfrak{a}$, namely $N(\mathfrak{a}) = [O : \mathfrak{a}]$

A (primitive) O-orientation on E is an embedding

$$\iota : O \hookrightarrow \mathrm{End}(E)$$

that cannot be extended to any $O' \supsetneq O$

- $\mathcal{E}\ell\ell_k(O)$ the set of E/k with a primitive O-orientation, up to oriented isomorphism
- $(E, \iota) \in \mathcal{E}\ell\ell_k(O)$

An isogeny ϕ from (E, ι) induces an orientation on the codomain

$$\iota_\phi(\alpha) := \frac{1}{\deg \phi} \phi \circ \iota(\alpha) \circ \hat{\phi} \quad \text{for all } \alpha \in O$$

(Up to some conditions) cl_O acts freely and (essentially) transitively on $\mathcal{E}\ell\ell_k(O)$

(Up to some conditions) cl_O acts freely and (essentially) transitively on $\mathcal{E}\ell\ell_k(O)$

$(E, \iota) \in \mathcal{E}\ell\ell_k(O)$, $\mathfrak{a} \subseteq O$,

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

$$\phi_{\mathfrak{a}} : (E, \iota) \to (E/E[\mathfrak{a}], \iota_{\phi_{\mathfrak{a}}})$$

(Up to some conditions) cl_O acts freely and (essentially) transitively on $\mathcal{E}\ell\ell_k(O)$

$(E, \iota) \in \mathcal{E}\ell\ell_k(O)$, $\mathfrak{a} \subseteq O$,

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

$$\phi_{\mathfrak{a}} : (E, \iota) \to (E/E[\mathfrak{a}], \iota_{\phi_{\mathfrak{a}}})$$

Then define action

$$* : \mathrm{cl}_O \times \mathcal{E}\ell\ell_k(O) \to \mathcal{E}\ell\ell_k(O)$$

$$[\mathfrak{a}] * (E, \iota) := (E/E[\mathfrak{a}], \iota_{\phi_{\mathfrak{a}}})$$

The action being free means that

$$[\mathfrak{a}] * (E, \iota) = (E, \iota) \text{ if and only if } [\mathfrak{a}] = [O] = 1_{\mathrm{cl}_O}$$

The action being transitive means that

$$\text{for any } (E_0, \iota_0), (E_1, \iota_1) \text{ there exists } \mathfrak{a} \text{ such that } (E_1, \iota_1) = [\mathfrak{a}] * (E_0, \iota_0)$$

For suitable parameters $* : \mathrm{cl}_O \times \mathcal{E}\ell\ell_k(O) \to \mathcal{E}\ell\ell_k(O)$ is cryptographic

Example (CSIDH (CLM+18))

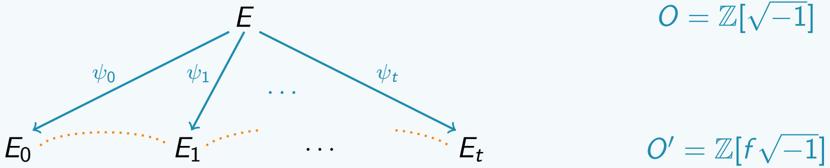
$k = \overline{\mathbb{F}}_p$, $K = \mathbb{Q}(\sqrt{-p})$, $O = \mathbb{Z}[\sqrt{-p}]$

$\mathcal{E}\ell\ell_k(O)$ is a set of supersingular $E/\mathbb{F}_p$ up to $\mathbb{F}_p$-isomorphism

cl_O acts freely and transitively on $\mathcal{E}\ell\ell_k(O)$

Example (SCALLOP, (FFK+23))

$k = \overline{\mathbb{F}}_p$, $K = \mathbb{Q}(\sqrt{-1})$
$O' = \mathbb{Z}[f\sqrt{-1}]$ suborder of conductor f of $O = \mathbb{Z}[\sqrt{-1}]$, $(f, p) = 1$.
$\mathrm{cl}_{O'}$ acts freely and (essentially) transitively on curves "downstairs" in f-isogeny volcano



E at the top has $j = 1728$, e.g. $y^2 = x^3 + x$ with O-orientation

$$\iota(\sqrt{-1})(x, y) := \mathbf{i}(x, y) = (-x, y\sqrt{-1})$$

.

$$\begin{tikzcd} & & E \arrow[dll, "\psi_0"'] \arrow[dl, "\psi_1"] \arrow[drr, "\psi_t"] & & \\ E_0 & E_1 & \cdots & & E_t \end{tikzcd}$$

$O = \mathbb{Z}[\sqrt{-1}]$

$O' = \mathbb{Z}[f\sqrt{-1}]$

Each curve "downstairs" is the codomain of an f-isogeny $\psi_j : E \to E_j$, $j = 0, 1, \ldots t$

$$E_j = E/C_j \quad \text{for some } f\text{-subgroup } C_j := \ker \psi_j \leq E$$

Think of C_j as *level structure* on E

Recall $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for any integer N, $(N, p) = 1$

$\Gamma \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, a Γ-level structure on E is a choice of isomorphism

$$\Phi : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \longrightarrow E[N]$$

up to precomposition with some $\gamma \in \Gamma$

In other words, fix basis P, Q of $E[N]$, up to base change by matrices $\gamma \in \Gamma$

Recall $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for any integer N, $(N, p) = 1$

$\Gamma \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, a Γ-level structure on E is a choice of isomorphism

$$\Phi : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \longrightarrow E[N]$$

up to precomposition with some $\gamma \in \Gamma$

In other words, fix basis P, Q of $E[N]$, up to base change by matrices $\gamma \in \Gamma$

Example

Fix $\Phi : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to E[N]$, let $P = \Phi(1, 0)$, $Q = \Phi(0, 1)$.

$$\Gamma = \Gamma_N^0 = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \quad \text{let } \gamma = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \Gamma_N^0,$$

$\Phi \circ \gamma(1, 0) = aP$, $\Phi \circ \gamma(0, 1) = bP + cQ$, then only fix cyclic N-subgroup $\langle P \rangle$

Example

- $\Gamma_N^0 = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$ -level structure fixes a cyclic N-subgroup
- $\Gamma_N^{0,0} = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}$ -level structure fixes two independent cyclic N-subgroups
- $\Gamma_N^1 = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\}$ -level structure fixes a point of order N
- $\Gamma_N = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ -level structure fixes a basis of of $E[N]$ (*full* level structure)

$$\begin{tikzcd}[column sep=small]
 & & & E \arrow[dlll, "\psi_0"'] \arrow[dll, "\psi_1"'] \arrow[dr, "\psi_t"] & \\
E_0 & E_1 & \cdots & \cdots & E_t
\end{tikzcd}$$

$$O = \mathbb{Z}[\sqrt{-1}]$$

$$O' = \mathbb{Z}[f\sqrt{-1}]$$

Each curve "downstairs" is the codomain of an f-isogeny $\psi_j : E \to E_j$, $j = 0, 1, \ldots t$

$$E_j = E/C_j \quad \text{for some } f\text{-subgroup } C_j := \ker \psi_j \leq E$$

Think of C_j as Γ_f^0-level structure on E

Can we somehow translate the action on E_j oriented by O' into an action on E oriented by O, but equipped with Γ_f^0-level structure?

Can we somehow translate the action on E_j oriented by O' into an action on E oriented by O, but equipped with Γ_f^0-level structure?

Can we somehow translate the action on E_j oriented by O' into an action on E oriented by O, but equipped with Γ_f^0-level structure?

For $(\alpha : \beta) \in \mathbb{P}^1(\mathbb{Z}/f\mathbb{Z})$, ideals

$$\mathfrak{a}_{\alpha,\beta} := (f^2, f(\alpha + \beta\sqrt{-1})) \subseteq O' = \mathbb{Z}[f\sqrt{-1}]$$

form all of $\mathrm{cl}_{O'}$

Letting $C_j = \langle P_j \rangle \leq E$,

$$[\mathfrak{a}_{\alpha,\beta}] * E/\langle P_j \rangle = E/\langle \alpha P_j - \beta\,\mathbf{i}(P_j) \rangle$$

Can we make this translation less mysterious?

Could it be part of a bigger story?

Can we make this translation less mysterious?

Could it be part of a bigger story?

Some evidence:

There is a free and transitive action on curves in $\mathcal{E}\ell\ell_{\overline{\mathbb{F}}_p}(\mathbb{Z}[\sqrt{-p}])$ with Γ_N-level structure by a *ray class group* [GPV23], [CK23]

- $\mathfrak{m}$ modulus of $\mathcal{O}$, namely a non-zero ideal $\mathfrak{m} \subseteq \mathcal{O}$

For any $\mathfrak{m}$, each class in $\mathrm{cl}_{\mathcal{O}}$ contains an $\mathfrak{a} \subseteq \mathcal{O}$ coprime with $\mathfrak{m}$, namely

$$\mathfrak{a} + \mathfrak{m} = \mathcal{O}$$

- $\mathfrak{m}$ modulus of O, namely a non-zero ideal $\mathfrak{m} \subseteq O$

For any $\mathfrak{m}$, each class in cl_O contains an $\mathfrak{a} \subseteq O$ coprime with $\mathfrak{m}$, namely

$$\mathfrak{a} + \mathfrak{m} = O$$

- $I_O(\mathfrak{m}) \leq I_O$ the subgroup generated by all invertible ideals in O coprime with $\mathfrak{m}$
- $P_O(\mathfrak{m}) := I_O(\mathfrak{m}) \cap P_O \leq P_O$ the subgroup generated by all invertible principal ideals in O coprime with $\mathfrak{m}$

There is a natural isomorphism

$$\frac{I_O(\mathfrak{m})}{P_O(\mathfrak{m})} \cong \mathrm{cl}_O$$

A ray for modulus $\mathfrak{m}$ is a principal fractional ideal

$$\alpha O, \alpha \in K^*, \text{ such that } \alpha \equiv 1 \bmod \mathfrak{m}$$

$\alpha \equiv \beta \bmod \mathfrak{m}$ means if $\alpha = \alpha_1/\alpha_2, \beta = \beta_1/\beta_2$, $\alpha_i, \beta_i \in O$, then $\alpha_1\beta_2 - \alpha_2\beta_1 \in \mathfrak{m}$

The ray group $P_{O,\{1\}}(\mathfrak{m}) \leq P_O(\mathfrak{m})$ is the group of rays for modulus $\mathfrak{m}$

- $\mathrm{I}_O(\mathfrak{m}) \leq I_O$ the subgroup generated by all invertible ideals in O coprime to $\mathfrak{m}$
- $P_O(\mathfrak{m}) \leq P_O$ the subgroup generated by all invertible principal ideals in O coprime to $\mathfrak{m}$
- $P_{O,\{1\}}(\mathfrak{m}) \leq P_O(\mathfrak{m})$ is the group of rays for modulus $\mathfrak{m}$

- $I_O(\mathfrak{m}) \le I_O$ the subgroup generated by all invertible ideals in O coprime to $\mathfrak{m}$
- $P_O(\mathfrak{m}) \le P_O$ the subgroup generated by all invertible principal ideals in O coprime to $\mathfrak{m}$
- $P_{O,\{1\}}(\mathfrak{m}) \le P_O(\mathfrak{m})$ is the group of rays for modulus $\mathfrak{m}$

The ray class group for modulus $\mathfrak{m}$ is

$$\mathrm{cl}_{P_{O,\{1\}}(\mathfrak{m})} := \frac{I_O(\mathfrak{m})}{P_{O,\{1\}}(\mathfrak{m})}$$

- $\mathrm{I}_O(\mathfrak{m}) \le I_O$ the subgroup generated by all invertible ideals in O coprime to $\mathfrak{m}$
- $P_O(\mathfrak{m}) \le P_O$ the subgroup generated by all invertible principal ideals in O coprime to $\mathfrak{m}$
- $P_{O,\{1\}}(\mathfrak{m}) \le P_O(\mathfrak{m})$ is the group of rays for modulus $\mathfrak{m}$

The ray class group for modulus $\mathfrak{m}$ is

$$\mathrm{cl}_{P_{O,\{1\}}(\mathfrak{m})} := \frac{I_O(\mathfrak{m})}{P_{O,\{1\}}(\mathfrak{m})}$$

A congruence subgroup for modulus $\mathfrak{m}$ is a subgroup

$$P_{O,\{1\}}(\mathfrak{m}) \le H \le P_O(\mathfrak{m})$$

- $\mathrm{I}_O(\mathfrak{m}) \leq I_O$ the subgroup generated by all invertible ideals in O coprime to $\mathfrak{m}$
- $P_O(\mathfrak{m}) \leq P_O$ the subgroup generated by all invertible principal ideals in O coprime to $\mathfrak{m}$
- $P_{O,\{1\}}(\mathfrak{m}) \leq P_O(\mathfrak{m})$ is the group of rays for modulus $\mathfrak{m}$

The ray class group for modulus $\mathfrak{m}$ is

$$\mathrm{cl}_{P_{O,\{1\}}(\mathfrak{m})} := \frac{I_O(\mathfrak{m})}{P_{O,\{1\}}(\mathfrak{m})}$$

A congruence subgroup for modulus $\mathfrak{m}$ is a subgroup

$$P_{O,\{1\}}(\mathfrak{m}) \leq H \leq P_O(\mathfrak{m})$$

A generalized class group is

$$\mathrm{cl}_H := \frac{I_O(\mathfrak{m})}{H}$$

- H congruence subgroup, namely $P_{O,\{1\}}(\mathfrak{m}) \leq H \leq P_O(\mathfrak{m})$
- cl_H generalized class group relative to H

Example (The extremal cases)

If $H = P_O(\mathfrak{m})$, $\mathrm{cl}_H = \frac{I_O(\mathfrak{m})}{P_O(\mathfrak{m})} \cong \mathrm{cl}_O$ is the class group of O

- H congruence subgroup, namely $P_{\mathcal{O},\{1\}}(\mathfrak{m}) \leq H \leq P_{\mathcal{O}}(\mathfrak{m})$
- cl_H generalized class group relative to H

Example (The extremal cases)

If $H = P_{\mathcal{O}}(\mathfrak{m})$, $\mathrm{cl}_H = \frac{I_{\mathcal{O}}(\mathfrak{m})}{P_{\mathcal{O}}(\mathfrak{m})} \cong \mathrm{cl}_{\mathcal{O}}$ is the class group of $\mathcal{O}$

If $H = P_{\mathcal{O},\{1\}}(\mathfrak{m})$, $\mathrm{cl}_H = \frac{I_{\mathcal{O}}(\mathfrak{m})}{P_{\mathcal{O},\{1\}}(\mathfrak{m})}$ is the ray class group for modulus $\mathfrak{m}$

Example (Suborder class group)

If $\mathfrak{m} = f\mathcal{O}$ and

$$H = \{\alpha\mathcal{O} \mid \alpha \in K^* \text{ and } \alpha \equiv g \bmod f\mathcal{O} \text{ for some } g \in \mathbb{Z}, (g, f) = 1\} =: P_{\mathcal{O},\mathbb{Z}}(f\mathcal{O})$$

then

$$\mathrm{cl}_H \cong \mathrm{cl}_{\mathcal{O}'}$$

where $\mathcal{O}' \subseteq \mathcal{O}$ suborder of conductor f

Recall SCALLOP: $\mathcal{O} = \mathbb{Z}[\sqrt{-1}]$, $\mathcal{O}' = \mathbb{Z}[f\sqrt{-1}]$, $\mathrm{cl}_{\mathcal{O}'}$ acts freely and transitively on $\mathcal{E}\ell\ell_k(\mathcal{O}')$

$H \leq P_O(\mathfrak{m})$ implies $\mathrm{cl}_H \geq \mathrm{cl}_O$

Then there is a well-defined action

$$\mathrm{cl}_H \times \mathcal{E}\ell\ell_k(O) \to \mathcal{E}\ell\ell_k(O)$$

$$([\mathfrak{a}], (E, \iota)) \mapsto (E/E[\mathfrak{a}], \iota_{\phi_\mathfrak{a}})$$

$H \leq P_O(\mathfrak{m})$ implies $\mathrm{cl}_H \geq \mathrm{cl}_O$

Then there is a well-defined action

$$\mathrm{cl}_H \times \mathcal{E}\ell\ell_k(O) \to \mathcal{E}\ell\ell_k(O)$$

$$([\mathfrak{a}], (E, \iota)) \mapsto (E/E[\mathfrak{a}], \iota_{\phi_\mathfrak{a}})$$

No longer free if $H \lneq P_O(\mathfrak{m})$, $\mathrm{cl}_H \gneq \mathrm{cl}_O$

$H \leq P_O(\mathfrak{m})$ implies $\mathrm{cl}_H \geq \mathrm{cl}_O$

Then there is a well-defined action

$$\mathrm{cl}_H \times \mathcal{E}\ell\ell_k(O) \to \mathcal{E}\ell\ell_k(O)$$

$$([\mathfrak{a}], (E, \iota)) \mapsto (E/E[\mathfrak{a}], \iota_{\phi_\mathfrak{a}})$$

No longer free if $H \lneq P_O(\mathfrak{m})$, $\mathrm{cl}_H \gneq \mathrm{cl}_O$

Free on bigger set than $\mathcal{E}\ell\ell_k(O)$ $\to$ add extra information: $\mathfrak{m}$-*level structure*

Lemma

Let $\mathfrak{m} \subseteq \mathcal{O}$ be an invertible ideal of norm coprime to p. There is an isomorphism of $\mathcal{O}$-modules

$$E[\mathfrak{m}] \cong \mathcal{O}/\mathfrak{m}$$

It is in particular an isomorphism of groups

Lemma

Let $\mathfrak{m} \subseteq O$ be an invertible ideal of norm coprime to p. There is an isomorphism of O-modules

$$E[\mathfrak{m}] \cong O/\mathfrak{m}$$

It is in particular an isomorphism of groups

When $\mathfrak{m} = NO$, $(N, p) = 1$, $E[NO] = E[N]$ and

$$E[NO] \cong O/NO \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$$

In general,

$$E[\mathfrak{m}] \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \text{ for some } b \mid a$$

Definition

Let $\mathfrak{m}$ be an invertible ideal in O of norm coprime to p. Let $\Gamma \leq \mathrm{GL}(O/\mathfrak{m})$. Let E be primitively O-oriented. A Γ-level structure on E is a choice of a *group* isomorphism

$$\Phi : O/\mathfrak{m} \to E[\mathfrak{m}]$$

up to pre-composition with some $\gamma \in \Gamma$ and post-composition with oriented automorphisms

In other words, fix basis P, Q of $E[\mathfrak{m}]$, up to base changes by $\gamma \in \Gamma$

- Y_Γ the set of primitively O-oriented curves with with Γ-level structure, up to oriented isomorphism

- Y_Γ the set of primitively O-oriented curves with with Γ-level structure, up to oriented isomorphism

Recap

→ cl_H acts on $\mathcal{E}\ell\ell_k(O)$, not freely

→ enlarge $\mathcal{E}\ell\ell_k(O)$ to Y_Γ with Γ-level structure

Recap

$\rightarrow$ cl_H acts on $\mathcal{E}\ell\ell_k(\mathcal{O})$, not freely

$\rightarrow$ enlarge $\mathcal{E}\ell\ell_k(\mathcal{O})$ to Y_Γ with Γ-level structure

Now

$\rightarrow$ define a family of congruence subgroups H

$\rightarrow$ find corresponding level structure

$\rightarrow$ find $Z_\Gamma \subseteq Y_\Gamma$ where cl_H acts transitively

Recall ray class group

$$\mathrm{cl}_{O,\{1\}}(\mathfrak{m}) = \frac{I_O(\mathfrak{m})}{P_{O,\{1\}}(\mathfrak{m})}$$

where

$$P_{O,\{1\}}(\mathfrak{m}) = \{\alpha O \mid \alpha \in K^* \text{ and } \alpha \equiv 1 \bmod \mathfrak{m}\}$$

Recall a ray class group is

$$\mathrm{cl}_{O,\{1\}}(\mathfrak{m}) = \frac{I_O(\mathfrak{m})}{P_{O,\{1\}}(\mathfrak{m})}$$

where

$$P_{O,\{1\}}(\mathfrak{m}) = \{\alpha O \mid \alpha \in K^* \text{ and } \alpha \equiv 1 \bmod \mathfrak{m}\}$$

$\Lambda \subseteq O$ multiplicatively closed subset, define

$$P_{O,\Lambda}(\mathfrak{m}) = \{\alpha O \mid \alpha \in K^* \text{ and } \alpha \equiv \lambda \bmod \mathfrak{m} \text{ for some } \lambda \in \Lambda \text{ coprime to } N(\mathfrak{m})\}$$

- $\Lambda \subseteq O$ multiplicatively closed
- $P_{O,\Lambda}(\mathfrak{m}) := \{\alpha O \mid \alpha \in K^* \text{ and } \alpha \equiv \lambda \bmod \mathfrak{m} \text{ for some } \lambda \in \Lambda \text{ coprime to } N(\mathfrak{m})\}$

Example (The extremal cases)

If $\Lambda = \{1\}$, $P_{O,\{1\}}(\mathfrak{m})$ is the group of rays for modulus $\mathfrak{m}$, defining the ray class group $\mathrm{cl}_{P_{O,\{1\}}(\mathfrak{m})}$

- $\Lambda \subseteq O$ multiplicatively closed
- $P_{O,\Lambda}(\mathfrak{m}) := \{\alpha O \mid \alpha \in K^* \text{ and } \alpha \equiv \lambda \bmod \mathfrak{m} \text{ for some } \lambda \in \Lambda \text{ coprime to } N(\mathfrak{m})\}$

Example (The extremal cases)

If $\Lambda = \{1\}$, $P_{O,\{1\}}(\mathfrak{m})$ is the group of rays for modulus $\mathfrak{m}$, defining the ray class group $\mathrm{cl}_{P_{O,\{1\}}(\mathfrak{m})}$

If $\Lambda = O$, $P_{O,O}(\mathfrak{m}) = P_O(\mathfrak{m})$ is the group of invertible principal ideals coprime to $\mathfrak{m}$, defining the class group cl_O

- $\Lambda \subseteq O$ multiplicatively closed
- $P_{O,\Lambda}(\mathfrak{m}) := \{\alpha O \mid \alpha \in K^* \text{ and } \alpha \equiv \lambda \bmod \mathfrak{m} \text{ for some } \lambda \in \Lambda \text{ coprime to } N(\mathfrak{m})\}$

Example (The extremal cases)

If $\Lambda = \{1\}$, $P_{O,\{1\}}(\mathfrak{m})$ is the group of rays for modulus $\mathfrak{m}$, defining the ray class group $\mathrm{cl}_{P_{O,\{1\}}(\mathfrak{m})}$

If $\Lambda = O$, $P_{O,O}(\mathfrak{m}) = P_O(\mathfrak{m})$ is the group of invertible principal ideals coprime to $\mathfrak{m}$, defining the class group cl_O

Example (Suborder class group)

If $\Lambda = \mathbb{Z}$, $\mathfrak{m} = fO$, $P_{O,\mathbb{Z}}(fO)$ is the congruence subgroup defining the class group $\mathrm{cl}_{O'}$ of a suborder $O' \subseteq O$ of conductor f

Congruence subgroups $P_{O,\{1\}}(\mathfrak{m}) \leq H = P_{O,\Lambda}(\mathfrak{m}) \leq P_O(\mathfrak{m})$ define generalized class groups $\mathrm{cl}_{P_{O,\Lambda}(\mathfrak{m})}$

Want to act on primitively O-oriented elliptic curves with Γ-level structure, *which Γ?*

Congruence subgroups $P_{\mathcal{O},\{1\}}(\mathfrak{m}) \leq H = P_{\mathcal{O},\Lambda}(\mathfrak{m}) \leq P_{\mathcal{O}}(\mathfrak{m})$ define generalized class groups $\mathrm{cl}_{P_{\mathcal{O},\Lambda}(\mathfrak{m})}$

Want to act on primitively $\mathcal{O}$-oriented elliptic curves with Γ-level structure, *which Γ?*

$$\Gamma_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\mu_\alpha \mid \alpha\mathcal{O} \in P_{\mathcal{O},\Lambda}(\mathfrak{m})\} \qquad \leq \mathrm{GL}(\mathcal{O}/\mathfrak{m})$$

where μ_α multiplication by α on $\mathcal{O}/\mathfrak{m}$

Congruence subgroups $P_{O,\{1\}}(\mathfrak{m}) \leq H = P_{O,\Lambda}(\mathfrak{m}) \leq P_O(\mathfrak{m})$ define generalized class groups $\mathrm{cl}_{P_{O,\Lambda}(\mathfrak{m})}$

Want to act on primitively O-oriented elliptic curves with Γ-level structure, *which Γ?*

$$\Gamma_{O,\Lambda}(\mathfrak{m}) = \{\mu_\alpha \mid \alpha O \in P_{O,\Lambda}(\mathfrak{m})\} = \{\mu_\lambda \mid \lambda \in O^*\Lambda \text{ coprime to } N(\mathfrak{m})\} \leq \mathrm{GL}(O/\,\mathfrak{m})$$

where μ_α, μ_λ multiplication by α, λ on $O/\,\mathfrak{m}$

- Y_Γ the set of primitively O-oriented curves with with Γ-level structure, up to oriented isomorphism

If Γ consists of O-module automorphisms of $O/\mathfrak{m}$,

- $Z_\Gamma \subseteq Y_\Gamma$ the subset in which the level structure is an O-*module* isomorphism

Theorem

Let $\mathfrak{m} \subseteq O$ be an invertible ideal, let $H = P_{O,\Lambda}(\mathfrak{m})$. Then

$$[\mathfrak{a}] * (E, \iota, \Phi) = (E/E[\mathfrak{a}], \iota_{\phi_\mathfrak{a}}, \phi_\mathfrak{a} \circ \Phi)$$

is a well-defined free and transitive action of cl_H on $Z_{\Gamma_{O,\Lambda}(\mathfrak{m})}$
If $\Lambda \subseteq O^* \mathbb{Z}$, it extends to a free action on $Y_{\Gamma_{O,\Lambda}(\mathfrak{m})}$

Example *Back to SCALLOP!*

$O = \mathbb{Z}[\sqrt{-1}]$, $\mathfrak{m} = fO$, then $E[\mathfrak{m}] = E[f] \cong \mathbb{Z}/f\mathbb{Z} \times \mathbb{Z}/f\mathbb{Z}$

Take $\Lambda = \mathbb{Z} \subseteq O$, $H = P_{O,\mathbb{Z}}(fO)$, then $\mathrm{cl}_H \cong \mathrm{cl}_{O'}$, $O' \subseteq O$ suborder of conductor f

Example *Back to SCALLOP!*

$O = \mathbb{Z}[\sqrt{-1}]$, $\mathfrak{m} = fO$, then $E[\mathfrak{m}] = E[f] \cong \mathbb{Z}/f\mathbb{Z} \times \mathbb{Z}/f\mathbb{Z}$

Take $\Lambda = \mathbb{Z} \subseteq O$, $H = P_{O,\mathbb{Z}}(fO)$, then $\mathrm{cl}_H \cong \mathrm{cl}_{O'}$, $O' \subseteq O$ suborder of conductor f

$\Gamma = \Gamma_{O,\mathbb{Z}}(fO) = \{\mu_\lambda \mid \lambda \in \mathbb{Z}, (\lambda, f) = 1\} = \Gamma_f^0 \leq \mathrm{GL}_2(\mathbb{Z}/f\mathbb{Z})$

Example *Back to SCALLOP!*

$O = \mathbb{Z}[\sqrt{-1}]$, $\mathfrak{m} = fO$, then $E[\mathfrak{m}] = E[f] \cong \mathbb{Z}/f\,\mathbb{Z} \times \mathbb{Z}/f\,\mathbb{Z}$

Take $\Lambda = \mathbb{Z} \subseteq O$, $H = P_{O,\mathbb{Z}}(fO)$, then $\mathrm{cl}_H \cong \mathrm{cl}_{O'}$, $O' \subseteq O$ suborder of conductor f

$\Gamma = \Gamma_{O,\mathbb{Z}}(fO) = \{\mu_\lambda \mid \lambda \in \mathbb{Z}, (\lambda, f) = 1\} = \Gamma_f^0 \leq \mathrm{GL}_2(\mathbb{Z}/f\,\mathbb{Z})$

The set of primitively O-oriented curves with Γ-level structure is

$$Y_{\Gamma_f^0} = \{(E, P, Q) \mid E \in \mathcal{E}\ell\ell_k(O), P, Q \text{ a basis of } E[f]\}/\sim$$

$$(E, P, Q) \sim (E, \lambda P, \lambda Q) \text{ for any } \lambda \in (\mathbb{Z}/f\,\mathbb{Z})^*$$

By our Theorem, $\mathrm{cl}_H \cong \mathrm{cl}_{O'}$ acts freely and transitively on $Z_{\Gamma_f^0} \subseteq Y_{\Gamma_f^0}$

In $Z_{\Gamma_f^0}$, level structure is isomorphism

$$\begin{aligned} \Phi : O/fO &\to E[f] \quad \text{of } O\text{-modules} \\ 1 &\mapsto P \end{aligned}$$

such that $P, \iota(\sqrt{-1})(P) = \mathbf{i}(P)$ basis of $E[f]$, up to Γ_f^0

By our Theorem, $\mathrm{cl}_H \cong \mathrm{cl}_{O'}$ acts freely and transitively on $Z_{\Gamma_f^0} \subseteq Y_{\Gamma_f^0}$

In $Z_{\Gamma_f^0}$, level structure is isomorphism

$$\begin{aligned} \Phi : O/fO &\to E[f] \quad \text{of } O\text{-modules} \\ 1 &\mapsto P \end{aligned}$$

such that $P, \iota(\sqrt{-1})(P) = \mathbf{i}(P)$ basis of $E[f]$, up to Γ_f^0

$$Z_{\Gamma_f^0} = \{(E, P) \mid E \in \mathcal{E}\ell\ell_k(O), P, \mathbf{i}(P) \text{ a basis of } E[f]\}/\sim$$

$$(E, P) \sim (E, \lambda P) \text{ for any } \lambda \in (\mathbb{Z}/f\,\mathbb{Z})^*$$

By our Theorem, $\mathrm{cl}_H \cong \mathrm{cl}_{O'}$ acts freely and transitively on $Z_{\Gamma_f^0} \subseteq Y_{\Gamma_f^0}$

In $Z_{\Gamma_f^0}$, level structure is isomorphism

$$\begin{aligned} \Phi : O/fO &\to E[f] \quad \text{of } O\text{-modules} \\ 1 &\mapsto P \end{aligned}$$

such that $P, \iota(\sqrt{-1})(P) = \mathbf{i}(P)$ basis of $E[f]$, up to Γ_f^0

$$Z_{\Gamma_f^0} = \{(E,P) \mid E \in \mathcal{E}\ell\ell_k(O), P, \mathbf{i}(P) \text{ a basis of } E[f]\}/\sim$$
$$(E,P) \sim (E, \lambda P) \text{ for any } \lambda \in (\mathbb{Z}/f\,\mathbb{Z})^*$$

In $Z_{\Gamma_f^0}$, level structure is given by f-subgroups $C = \langle P \rangle \leq E$!

If f prime inert in $\mathbb{Q}(\sqrt{-1})$,

$$Z_{\Gamma_{O,\mathbb{Z}}(fO)} = Z_{\Gamma_f^0} = \{(E, C_j) \mid E \in \mathcal{E}\ell\ell_k(O), C_j = \ker \psi_j \leq E\}, \quad j = 0, \dots t$$

$$\begin{tikzcd}
 & & & E \arrow[dlll, "\psi_0"'] \arrow[dll, "\psi_1"] \arrow[drr, "\psi_t"] & \cdots & \\
E_0 & E_1 & & \cdots & & E_t
\end{tikzcd}$$

$O = \mathbb{Z}[\sqrt{-1}]$

$O' = \mathbb{Z}[f\sqrt{-1}]$

If f prime inert in $\mathbb{Q}(\sqrt{-1})$,

$$Z_{\Gamma_{O,\mathbb{Z}}(fO)} = Z_{\Gamma_f^0} = \{(E, C_j) \mid E \in \mathcal{E}\ell\ell_k(O), C_j = \ker \psi_j \leq E\}, \quad j = 0, \dots t$$

$$\begin{tikzcd}
 & & E \arrow[dll, "\psi_0"'] \arrow[dl, "\psi_1"] \arrow[drr, "\psi_t"] & & \\
E_0 & E_1 & \cdots & & E_t
\end{tikzcd}$$

$O = \mathbb{Z}[\sqrt{-1}]$

$O' = \mathbb{Z}[f\sqrt{-1}]$

$\Lambda = \mathbb{Z} \not\subseteq O^* \mathbb{Z}$ but $\Gamma_{O,\mathbb{Z}}(fO)$ and $\Gamma_{O,O^* \mathbb{Z}}(fO)$ define same level structure

Replacing with $\Lambda = O^* \mathbb{Z}$ action extends freely to $Y_{\Gamma_{O,O^* \mathbb{Z}}(fO)}$

Example *Back to CSIDH with full level structure!*

$O = \mathbb{Z}[\sqrt{-p}]$, $\mathfrak{m} = NO$, then $E[\mathfrak{m}] = E[N]$

$\Lambda = \{1\}$, $H = P_{O,\{1\}}(NO)$, then $\mathrm{cl}_H = \mathrm{cl}_{P_{O,\{1\}}(NO)}$ the ray class group

Example *Back to CSIDH with full level structure!*

$O = \mathbb{Z}[\sqrt{-p}]$, $\mathfrak{m} = NO$, then $E[\mathfrak{m}] = E[N]$

$\Lambda = \{1\}$, $H = P_{O,\{1\}}(NO)$, then $\mathrm{cl}_H = \mathrm{cl}_{P_{O,\{1\}}(NO)}$ the ray class group

$\Gamma = \Gamma_{O,\{1\}}(NO) = \{\mu_\lambda \mid \lambda = 1\} = \Gamma_N$ full level structure

$$Y_{\Gamma_N} = \{(E, P, Q) \mid E \in \mathcal{E}\ell\ell_k(O), P, Q \text{ a basis of } E[N]\}/\sim$$

$$(E, P, Q) \sim (E, -P, -Q) \text{ since } [-1] \text{ oriented automorphism}$$

$\mathrm{cl}_{P_{O,\{1\}}(NO)}$ acts freely and transitively on Z_{Γ_N}

A $\mathbb{Z}[\sigma]$-module morphism is $1 \mapsto P$, such that $P, \iota(\sigma)(P)$ basis of $E[N]$

$$Z_{\Gamma_N} = \{(E,P) \mid E \in \mathcal{E}\ell\ell_k(O), P, \iota(\sqrt{-p})(P) \text{ a basis of } E[N]\}/\sim$$
$$(E,P) \sim (E,-P) \text{ since } [-1] \text{ oriented automorphism}$$

$\mathrm{cl}_{P_{O,\{1\}}(NO)}$ acts freely and transitively on Z_{Γ_N}

A $\mathbb{Z}[\sigma]$-module morphism is $1 \mapsto P$, such that $P, \iota(\sigma)(P)$ basis of $E[N]$

$$Z_{\Gamma_N} = \{(E,P) \mid E \in \mathcal{E}\ell\ell_k(O), P, \iota(\sqrt{-p})(P) \text{ a basis of } E[N]\}/\sim$$

$$(E,P) \sim (E,-P) \text{ since } [-1] \text{ oriented automorphism}$$

$\Lambda = \{1\} \subseteq O^* \mathbb{Z}$ so action extends freely to Y_{Γ_N}

Example *Back to the class group action!*

$O = \mathbb{Z}[\sigma]$ for some $\sigma \in K$, $\mathfrak{m} = NO$, then $E[\mathfrak{m}] = E[N]$

$\Lambda = O$, $H = P_{O,O}(\mathfrak{m}) = P_O(\mathfrak{m})$, then $\mathrm{cl}_H \cong \mathrm{cl}_O$ the class group of O

$\Gamma = \Gamma_{O,O}(NO) = \{\mu_\lambda \mid \lambda \in O \text{ coprime to } N\}$

$$Y_\Gamma = \{(E, P, Q) \mid E \in \mathcal{E}\ell\ell_k(O), P, Q \text{ a basis of } E[N]\}/\sim$$
$$(E, P, Q) \sim (E, \iota(\lambda)(P), \iota(\lambda)(Q)) \text{ for any } \lambda \in O \text{ coprime to } N$$

cl_O acts freely and transitively on Z_Γ

A $\mathbb{Z}[\sigma]$-module morphism is $1 \mapsto P$, such that $P, \iota(\sigma)(P)$ basis of $E[N]$

$$Z_\Gamma = \{(E, P) \mid E \in \mathcal{E}\ell\ell_k(O), P, \iota(\sigma)(P) \text{ a basis of } E[N]\}/\sim$$

$$(E, P) \sim (E, \iota(\lambda)(P)) \text{ for any } \lambda \in O \text{ coprime to } N$$

cl_O acts freely and transitively on Z_Γ

A $\mathbb{Z}[\sigma]$-module morphism is $1 \mapsto P$, such that $P, \iota(\sigma)(P)$ basis of $E[N]$

$$Z_\Gamma = \{(E, P) \mid E \in \mathcal{E}\ell\ell_k(O), P, \iota(\sigma)(P) \text{ a basis of } E[N]\} / \sim$$

$$(E, P) \sim (E, \iota(\lambda)(P)) \text{ for any } \lambda \in O \text{ coprime to } N$$

$$Z_\Gamma = \mathcal{E}\ell\ell_k(O)$$

cl_O acts freely and transitively on Z_Γ

A $\mathbb{Z}[\sigma]$-module morphism is $1 \mapsto P$, such that $P, \iota(\sigma)(P)$ basis of $E[N]$

$$Z_\Gamma = \{(E, P) \mid E \in \mathcal{E}\ell\ell_k(O), P, \iota(\sigma)(P) \text{ a basis of } E[N]\}/\sim$$

$$(E, P) \sim (E, \iota(\lambda)(P)) \text{ for any } \lambda \in O \text{ coprime to } N$$

$$Z_\Gamma = \mathcal{E}\ell\ell_k(O)$$

$\Lambda = O \not\subseteq O^* \mathbb{Z}$ so action does not extend to Y_Γ

$\mathrm{cl}_H \geq \mathrm{cl}_O$ acts on larger sets than $\mathcal{E}\ell\ell_k(O)$

Is the vectorization problem harder for the action of cl_H*?*

$\mathrm{cl}_H \geq \mathrm{cl}_O$ acts on larger sets than $\mathcal{E}\ell\ell_k(O)$

Is the vectorization problem harder for the action of cl_H?

CSIDH with full level structure reduces to standard CSIDH [GPV23]

In general, vectorisation problem for cl_H reduces to that of cl_O

$\mathrm{cl}_H \geq \mathrm{cl}_O$ acts on larger sets than $\mathcal{E}\ell\ell_k(O)$

Is the vectorization problem harder for the action of cl_H*?*

CSIDH with full level structure reduces to standard CSIDH [GPV23]

In general, vectorisation problem for cl_H reduces to that of cl_O

For SCALLOP: reduction through large prime degree isogenies!

References

[GPV23] S. Galbraith, D. Perrin, and J. Voloch. CSIDH with level structure. *IACR Cryptol. ePrint Arch.*, page 1726, 2023.

[FFK+23] L. De Feo, T. Fouotsa, P. Kutas, A. Leroux, S. Merz, L. Panny, and B. Wesolowski. SCALLOP: scaling the CSI-FiSh. In *Public-Key Cryptography - PKC 2023 Part I, volume 13940 of Lecture Notes in Computer Science*, pages 345–375. Springer, 2023.

[CLM+18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. CSIDH: an efficient post-quantum commutative group action. In *Advances in cryptology—ASIACRYPT 2018. Part III, volume 11274 of Lecture Notes in Comput. Sci.*, pages 395–427. Springer, Cham, 2018.

[CK23] L. Colò and D. Kohel. *On the modular OSIDH protocol*, 2023. Preprint

https://www.leonardocolo.com/documents/articles/mosidh.pdf.

Thank you!