# Generalized class group actions via class field theory

Eli Orvis

University of Colorado Boulder

April 30, 2025

# Introduction

Class group actions are useful tools in cryptography.

# Introduction

Class group actions are useful tools in cryptography.

1. CSIDH

# Introduction

Class group actions are useful tools in cryptography.

1. CSIDH
   1. $\mathrm{Cl}_{\mathcal{O}}$-action on supersingular curves over $\mathbb{F}_p$

# Introduction

Class group actions are useful tools in cryptography.

1. CSIDH
    1. $\mathrm{Cl}_{\mathcal{O}}$-action on supersingular curves over $\mathbb{F}_p$
2. SCALLOP

# Introduction

Class group actions are useful tools in cryptography.

1. CSIDH
   1. $\mathrm{Cl}_{\mathcal{O}}$-action on supersingular curves over $\mathbb{F}_p$
2. SCALLOP
   1. Class group actions by non-maximal orders

# Introduction

Class group actions are useful tools in cryptography.

1. CSIDH
   1. $\mathrm{Cl}_{\mathcal{O}}$-action on supersingular curves over $\mathbb{F}_p$
2. SCALLOP
   1. Class group actions by non-maximal orders

# Introduction

For isogenists, level structures are also useful.

# Introduction

For isogenists, level structures are also useful.

1. SIDH attacks

# Introduction

For isogenists, level structures are also useful.

1. SIDH attacks
2. Conceptualizing isogeny problems ...

| $\Gamma$ | Best attack | Schemes |
|---|---|---|
| $\left(\begin{smallmatrix}1 & \\ & 1\end{smallmatrix}\right)$ | poly | SIDH |
| $\left(\begin{smallmatrix}1 & * \\ & 1\end{smallmatrix}\right)$ | poly | [16,21] |
| $\left(\begin{smallmatrix}\lambda & \\ & \lambda\end{smallmatrix}\right)$ | exp | M-SIDH |
| $\left(\begin{smallmatrix}* & \\ & *\end{smallmatrix}\right)$ | exp | FESTA, binSIDH, CSIDH, SCALLOP |
| $\left(\begin{smallmatrix}* & * \\ & *\end{smallmatrix}\right)$ | exp | SIDH PoKs |
| $SL_2$ | exp | generic |

# Agenda

Recent work by various authors, combines these concepts, to look at *class group actions on elliptic curves with level structure*.

# Agenda

Recent work by various authors, combines these concepts, to look at *class group actions on elliptic curves with level structure*.
Our agenda:

# Agenda

Recent work by various authors, combines these concepts, to look at *class group actions on elliptic curves with level structure*.

Our agenda:

1. Review recent results,

# Agenda

Recent work by various authors, combines these concepts, to look at *class group actions on elliptic curves with level structure*.

Our agenda:

1. Review recent results,
2. Propose an alternative framework,

## Agenda

Recent work by various authors, combines these concepts, to look at *class group actions on elliptic curves with level structure*.

Our agenda:

1. Review recent results,
2. Propose an alternative framework,
3. Explore.

# Agenda

Recent work by various authors, combines these concepts, to look at *class group actions on elliptic curves with level structure*.

Our agenda:

1. Review recent results,
2. Propose an alternative framework,
3. Explore.

Joint work (in progress) with Sarah Arpin, Joseph Macula.

# Definitions

First, some definitions:

# Definitions

First, some definitions:

## Definition

An *orientation* is an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(E)$.

# Definitions

First, some definitions:

## Definition

An *orientation* is an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(E)$. An orientation is *primitive* if it cannot be extended.

# Definitions

First, some definitions:

## Definition

An *orientation* is an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(E)$. An orientation is *primitive* if it cannot be extended.

## Definition

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

$$\Phi : (\mathbb{Z}/N\mathbb{Z})^2 \to E[N],$$

up to pre-composition by an element of $\Gamma$.

# Galbraith, Perrin, Voloch

In 2023, GPS proposed a cryptosystem based on CSIDH with *full level* $N$ *structure*.

# Galbraith, Perrin, Voloch

In 2023, GPS proposed a cryptosystem based on CSIDH with *full level $N$ structure.*

Full level structure means that we take $\Gamma = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. In other words, we specify a basis of $E[N]$.

# Galbraith, Perrin, Voloch

To find an appropriate class group they use:

$$\mathrm{Cl}_N(\mathcal{O}) = \frac{\{\text{frac. ideals coprime to } N\}}{\{\text{princ. frac. ideals } \alpha\mathcal{O},\ \alpha \equiv 1 \pmod{N}\}}$$

# Galbraith, Perrin, Voloch

To find an appropriate class group they use:

$$\mathrm{Cl}_N(\mathcal{O}) = \frac{\{\text{frac. ideals coprime to } N\}}{\{\text{princ. frac. ideals } \alpha\mathcal{O},\ \alpha \equiv 1 \pmod{N}\}}$$

Notes:

1. The class group action is still free, but not transitive.

# Galbraith, Perrin, Voloch

To find an appropriate class group they use:

$$\mathrm{Cl}_N(\mathcal{O}) = \frac{\{\text{frac. ideals coprime to } N\}}{\{\text{princ. frac. ideals } \alpha\mathcal{O},\ \alpha \equiv 1 \pmod{N}\}}$$

Notes:

1. The class group action is still free, but not transitive.
2. This does not improve security.

# Perrin, Voloch

PV studied ordinary elliptic curves with $\Gamma_0(N), \Gamma_1(N)$, and $\Gamma(N)$ level structures.

## Perrin, Voloch

PV studied ordinary elliptic curves with $\Gamma_0(N), \Gamma_1(N)$, and $\Gamma(N)$ level structures.

1. Count the size of craters in terms of $\ell \in \mathrm{Cl}(\mathcal{O})$,

# Perrin, Voloch

PV studied ordinary elliptic curves with $\Gamma_0(N), \Gamma_1(N)$, and $\Gamma(N)$ level structures.

1. Count the size of craters in terms of $\ell \in \mathrm{Cl}(\mathcal{O})$,
2. Obtain generalized class groups acting on each type of level structure.

## Perrin, Voloch

PV studied ordinary elliptic curves with $\Gamma_0(N), \Gamma_1(N)$, and $\Gamma(N)$ level structures.

1. Count the size of craters in terms of $\ell \in \mathrm{Cl}(\mathcal{O})$,
2. Obtain generalized class groups acting on each type of level structure. Use $\mathcal{I}_{\mathcal{O}}(N)$ modulo

## Perrin, Voloch

PV studied ordinary elliptic curves with $\Gamma_0(N), \Gamma_1(N)$, and $\Gamma(N)$ level structures.

1. Count the size of craters in terms of $\ell \in \mathrm{Cl}(\mathcal{O})$,
2. Obtain generalized class groups acting on each type of level structure. Use $\mathcal{I}_{\mathcal{O}}(N)$ modulo
    1. $\{$princ. ideals congruent to $\mathbb{Z}$ modulo $N\}$

## Perrin, Voloch

PV studied ordinary elliptic curves with $\Gamma_0(N), \Gamma_1(N)$, and $\Gamma(N)$ level structures.

1. Count the size of craters in terms of $\ell \in \mathrm{Cl}(\mathcal{O})$,
2. Obtain generalized class groups acting on each type of level structure. Use $\mathcal{I}_{\mathcal{O}}(N)$ modulo
    1. $\{$princ. ideals congruent to $\mathbb{Z}$ modulo $N\}$
    2. $\{$princ. ideals congruent to $\pm 1$ modulo $N\}$

# Arpin, Castryck, Eriksen, Lorenzon, Vercauteren

ACELV find sets of elliptic curves with level structure on which an arbitrary generalized class group acts freely and transitively.

## Arpin, Castryck, Eriksen, Lorenzon, Vercauteren

ACELV find sets of elliptic curves with level structure on which an arbitrary generalized class group acts freely and transitively.

### Definition

Let $H$ be a subgroup

$$\mathcal{P}_{\mathcal{O},1}(\mathfrak{m}) \leq H \leq \mathcal{I}_{\mathcal{O}}(\mathfrak{m}),$$

the *generalized class group associated to $H$* is

$$\mathrm{Cl}_{\mathcal{O}}(H) = \mathcal{I}_{\mathcal{O}}(\mathfrak{m})/H.$$

# Arpin, Castryck, Eriksen, Lorenzon, Vercauteren

ACELV find sets of elliptic curves with level structure on which an arbitrary generalized class group acts freely and transitively.

## Definition

Let $H$ be a subgroup

$$\mathcal{P}_{\mathcal{O},1}(\mathfrak{m}) \leq H \leq \mathcal{I}_{\mathcal{O}}(\mathfrak{m}),$$

the *generalized class group associated to $H$* is

$$\mathrm{Cl}_{\mathcal{O}}(H) = \mathcal{I}_{\mathcal{O}}(\mathfrak{m})/H.$$

Examples: Usual class group, ray class groups ...

# Arpin, Castryck, Eriksen, Lorenzon, Vercauteren

## Definition

Let $\Gamma \leq \mathrm{Aut}(\mathcal{O}/\mathfrak{m})$. A $\Gamma$-level structure on an oriented supersingular curve $E$ is a choice of (group!) isomorphism $\Phi : \mathcal{O}/\mathfrak{m} \to E[\mathfrak{m}]$, up to pre-composition by $\Gamma$.

# Arpin, Castryck, Eriksen, Lorenzon, Vercauteren

## Definition

Let $\Gamma \leq \mathrm{Aut}(\mathcal{O}/\mathfrak{m})$. A $\Gamma$-level structure on an oriented supersingular curve $E$ is a choice of (group!) isomorphism $\Phi : \mathcal{O}/\mathfrak{m} \to E[\mathfrak{m}]$, up to pre-composition by $\Gamma$.

Question: What set of oriented curves with level structure does $\mathrm{Cl}_{\mathcal{O}}(H)$ act on?

# Arpin, Castryck, Eriksen, Lorenzon, Vercauteren

Consider subgroups $H$ of the form:

$$\mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\alpha\mathcal{O} | \alpha \in K^\times, \alpha \equiv \lambda \pmod{\mathfrak{m}},\ \text{for } \lambda \in \Lambda \perp N(\mathfrak{m})\}.$$

# Arpin, Castryck, Eriksen, Lorenzon, Vercauteren

Consider subgroups $H$ of the form:

$$\mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\alpha\mathcal{O} | \alpha \in K^\times, \alpha \equiv \lambda \pmod{\mathfrak{m}}, \text{ for } \lambda \in \Lambda \perp N(\mathfrak{m})\}.$$

From this, we construct the level structure

$$\Gamma_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\mu_\alpha | \alpha\mathcal{O} \in \mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m})\} \subset \mathrm{Aut}(\mathcal{O}/\mathfrak{m})$$

# Arpin, Castryck, Eriksen, Lorenzon, Vercauteren

Consider subgroups $H$ of the form:

$$\mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\alpha\mathcal{O} | \alpha \in K^\times, \alpha \equiv \lambda \pmod{\mathfrak{m}}, \text{ for } \lambda \in \Lambda \perp N(\mathfrak{m})\}.$$

From this, we construct the level structure

$$\Gamma_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\mu_\alpha | \alpha\mathcal{O} \in \mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m})\} \subset \mathrm{Aut}(\mathcal{O}/\mathfrak{m})$$

ACELV construct sets of elliptic curves on which $\mathrm{Cl}_{\mathcal{O}}(\mathfrak{m})$ acts freely, and freely and transitively:

# Arpin, Castryck, Eriksen, Lorenzon, Vercauteren

Consider subgroups $H$ of the form:

$\mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\alpha\mathcal{O} | \alpha \in K^\times, \alpha \equiv \lambda \pmod{\mathfrak{m}}, \text{ for } \lambda \in \Lambda \perp N(\mathfrak{m})\}.$

From this, we construct the level structure

$$\Gamma_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\mu_\alpha | \alpha\mathcal{O} \in \mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m})\} \subset \mathrm{Aut}(\mathcal{O}/\mathfrak{m})$$

ACELV construct sets of elliptic curves on which $\mathrm{Cl}_{\mathcal{O}}(\mathfrak{m})$ acts freely, and freely and transitively:

1. $Y_\Gamma := \{\text{prim. } \mathcal{O}\text{-oriented curves with } \Gamma \text{ structure}\}$

# Arpin, Castryck, Eriksen, Lorenzon, Vercauteren

Consider subgroups $H$ of the form:

$\mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\alpha\mathcal{O} | \alpha \in K^\times, \alpha \equiv \lambda \pmod{\mathfrak{m}}, \text{ for } \lambda \in \Lambda \perp N(\mathfrak{m})\}$.

From this, we construct the level structure

$$\Gamma_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\mu_\alpha | \alpha\mathcal{O} \in \mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m})\} \subset \mathrm{Aut}(\mathcal{O}/\mathfrak{m})$$

ACELV construct sets of elliptic curves on which $\mathrm{Cl}_{\mathcal{O}}(\mathfrak{m})$ acts freely, and freely and transitively:

1. $Y_\Gamma := \{\text{prim. } \mathcal{O}\text{-oriented curves with } \Gamma \text{ structure}\}$
2. $Z_\Gamma := \{\mathcal{O}\text{-module isomorphism level structures} \subset Y_\Gamma\}$

# Arpin, Castryck, Eriksen, Lorenzon, Vercauteren

**Theorem**

*Let* $\mathfrak{m} \subset \mathcal{O}$ *be a proper ideal, and let* $H = \mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m})$*. Then*

$$[\mathfrak{a}] \star (E, \Phi) = (\varphi_{\mathfrak{a}}(E), \varphi_{\mathfrak{a}} \circ \Phi)$$

*is a well-defined free action of* $\mathrm{Cl}_H$ *on* $Z_{\Gamma_{\mathcal{O},\Lambda}(\mathfrak{m})}$*. If* $\Lambda \subset \mathcal{O}^\times\mathbb{Z}$ *then this extends to a free action of* $\mathrm{Cl}_H$ *on* $Y_{\Gamma_{\mathcal{O},\Lambda}(\mathfrak{m}}$*.*

# Class Field Theory

Class field theory provides a correspondence

$$\text{generalized class groups} \leftrightarrow \text{abelian extensions of } K$$

# Class Field Theory

Class field theory provides a correspondence

$$\text{generalized class groups} \leftrightarrow \text{abelian extensions of } K$$

In particular, the generalized class group is isomorphic to the corresponding Galois group.

# Class Field Theory

For imaginary quadratic fields, we have

# Class Field Theory

For imaginary quadratic fields, we have

1. $\mathcal{I}_{\mathcal{O}}(\mathfrak{m})/\mathcal{P}_{\mathcal{O}}(\mathfrak{m}) \leftrightarrow \mathrm{Gal}(K(j(E_0), \ldots, j(E_n))/K)$

# Class Field Theory

For imaginary quadratic fields, we have

1. $\mathcal{I}_{\mathcal{O}}(\mathfrak{m})/\mathcal{P}_{\mathcal{O}}(\mathfrak{m}) \leftrightarrow \mathrm{Gal}(K(j(E_0), \ldots, j(E_n))/K)$
2. $\mathcal{I}_{\mathcal{O}}(\mathfrak{m})/\mathcal{P}_{\mathcal{O},1}(\mathfrak{m}) \leftrightarrow \mathrm{Gal}(K(j(E), h(E[\mathfrak{m}])/K)$,

where $h$ is the Weber function.

# Class Field Theory

For imaginary quadratic fields, we have

1. $\mathcal{I}_{\mathcal{O}}(\mathfrak{m})/\mathcal{P}_{\mathcal{O}}(\mathfrak{m}) \leftrightarrow \mathrm{Gal}(K(j(E_0), \ldots, j(E_n))/K)$
2. $\mathcal{I}_{\mathcal{O}}(\mathfrak{m})/\mathcal{P}_{\mathcal{O},1}(\mathfrak{m}) \leftrightarrow \mathrm{Gal}(K(j(E), h(E[\mathfrak{m}])/K)$,

where $h$ is the Weber function.

Item one conceptually explains the regular class group action.

# Class Field Theory

For imaginary quadratic fields, we have

1. $\mathcal{I}_{\mathcal{O}}(\mathfrak{m})/\mathcal{P}_{\mathcal{O}}(\mathfrak{m}) \leftrightarrow \mathrm{Gal}(K(j(E_0), \ldots, j(E_n))/K)$
2. $\mathcal{I}_{\mathcal{O}}(\mathfrak{m})/\mathcal{P}_{\mathcal{O},1}(\mathfrak{m}) \leftrightarrow \mathrm{Gal}(K(j(E), h(E[\mathfrak{m}])/K)$,

where $h$ is the Weber function.

Item one conceptually explains the regular class group action.

Question: Can we gain insight into generalized class group actions from item two?

# Counting level structures

## Proposition

*Let $\Lambda$ be a multiplicatively closed subset of $\mathcal{O}$ containing $1$. Then there exists a unique subgroup $\mathcal{O}^\times/\mathfrak{m} \leq \tilde{\Lambda} \leq (\mathcal{O}/\mathfrak{m})^\times$ such that*

$$\mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\alpha\mathcal{O} | \alpha \in K^\times, \alpha \pmod{\mathfrak{m}} \in \tilde{\Lambda}\}.$$

# Counting level structures

## Proposition

*Let $\Lambda$ be a multiplicatively closed subset of $\mathcal{O}$ containing $1$. Then there exists a unique subgroup $\mathcal{O}^\times/\mathfrak{m} \leq \tilde{\Lambda} \leq (\mathcal{O}/\mathfrak{m})^\times$ such that*

$$\mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\alpha\mathcal{O} | \alpha \in K^\times, \alpha \pmod{\mathfrak{m}} \in \tilde{\Lambda}\}.$$

Notice:

# Counting level structures

## Proposition

*Let $\Lambda$ be a multiplicatively closed subset of $\mathcal{O}$ containing 1. Then there exists a unique subgroup $\mathcal{O}^\times/\mathfrak{m} \leq \tilde{\Lambda} \leq (\mathcal{O}/\mathfrak{m})^\times$ such that*

$$\mathcal{P}_{\mathcal{O},\Lambda}(\mathfrak{m}) = \{\alpha\mathcal{O} | \alpha \in K^\times, \alpha \pmod{\mathfrak{m}} \in \tilde{\Lambda}\}.$$

Notice:

$$\begin{aligned}(\mathcal{O}/\mathfrak{m})^\times/(\mathcal{O}^\times/\mathfrak{m}) &\cong \mathcal{P}_{\mathcal{O}}(\mathfrak{m})/\mathcal{P}_{\mathcal{O},1}(\mathfrak{m}) \\ &\cong \text{Gal(Ray class field/Hilbert class field)}\end{aligned}$$

# Counting level structures

## Proposition

*We have natural bijections between*

$$\begin{tikzcd}
\text{Level structures } \Gamma_{\mathcal{O},\Lambda} \arrow[rr, leftrightarrow] \arrow[dr, leftrightarrow] & & \text{Intermediate fields } H \leq L \leq R \arrow[dl, leftrightarrow] \\
& \text{Subgroups } G \leq (\mathcal{O}/\mathfrak{m})^\times/(\mathcal{O}^\times/\mathfrak{m}) &
\end{tikzcd}$$

# Counting level structures

## Proposition

*We have natural bijections between*

$$\begin{tikzcd}[column sep=small] \text{Level structures } \Gamma_{\mathcal{O},\Lambda} \arrow[rr, leftrightarrow] \arrow[dr, leftrightarrow] & & \text{Intermediate fields } H \leq L \leq R \arrow[dl, leftrightarrow] \\ & \text{Subgroups } G \leq (\mathcal{O}/\mathfrak{m})^\times/(\mathcal{O}^\times/\mathfrak{m}) & \end{tikzcd}$$

## Corollary

*If $[R : H] = q$ is prime, then the construction in AECLV gives only two level structures: full and trivial.*

# The $Z_\Gamma$ action from the field perspective

Question: What is special about $Z_\Gamma$ from the class-field perspective?

Introduction
Agenda
Recent work
Field Theory Perspective
Future Directions

# The $Z_\Gamma$ action from the field perspective

Question: What is special about $Z_\Gamma$ from the class-field perspective?

Recall: $Z_\Gamma = \{(E, \Phi) : \Phi \text{is an } \mathcal{O}\text{-module isomorphism}\}/\sim$.

# The $Z_\Gamma$ action from the field perspective

Question: What is special about $Z_\Gamma$ from the class-field perspective?

Recall: $Z_\Gamma = \{(E, \Phi) : \Phi \text{is an } \mathcal{O}\text{-module isomorphism}\}/\sim$.

Writing $\mathcal{O} = \mathbb{Z}[\sigma]$, this is equivalently the level structures $(E, P, \sigma(P))$, where $P$ is an $\mathcal{O}$-module generator for $E[\mathfrak{m}]$.

# The $Z_\Gamma$ action from the field perspective

Restrict to the case of full level structure. Then the corresponding field is the Ray class field

$$K(j(E), h(E[\mathfrak{m}]) = H(h(E[\mathfrak{m}]).$$

# The $Z_\Gamma$ action from the field perspective

Restrict to the case of full level structure. Then the corresponding field is the Ray class field

$$K(j(E), h(E[\mathfrak{m}]) = H(h(E[\mathfrak{m}])).$$

## Proposition

*Let $P$ be an element of $E[\mathfrak{m}]$ that generates $E[\mathfrak{m}]$ as an $\mathcal{O}$-module. Then $h(P)$ is a primitive element for $R = H(h(E[\mathfrak{m}]))/H$.*

Some future directions to explore:

1. In what cases can we describe the level structure explicitly from properties of the corresponding field?
2. Does this perspective help clarify what happens when we take $\mathcal{P}_{\mathcal{O}}(\mathfrak{m}) \subsetneq H$?
3. Can we use these class group actions to answer computational questions about abelian extensions of $K$?

Some future directions to explore:

1. In what cases can we describe the level structure explicitly from properties of the corresponding field?
2. Does this perspective help clarify what happens when we take $\mathcal{P}_{\mathcal{O}}(\mathfrak{m}) \subsetneq H$?
3. Can we use these class group actions to answer computational questions about abelian extensions of $K$?

Thanks!