# Post-Quantum Cryptography: Towards Commutative Supersingular Isogeny Key Exchange


Candidate
Giovanni Tognolini

Supervisor
Prof. Nadir Murru

University of Trento

19 March 2021

# Index

# Pre Quantum Diffie-Hellman

| Public parameters | A group $G = \langle P \rangle$ of order $N$. | |
|---|---|---|
| | **Alice** | **Bob** |
| Pick random secret | $a \in G$ | $b \in G$ |
| Compute public data | $A = [a]P$ | $B = [b]P$ |
| Exchange data | $A \longrightarrow$ | $\longleftarrow B$ |
| Compute shared secret | $S = [a]B$ | $S = [b]A$ |

Figure: Diffie-Hellman key-exchange protocol.

# The Quantum Threat

P. Shor $\xrightarrow{\text{Shor's algorithm}}$ Solves integer factorization problem and discrete logarithms in polynomial time.

# The Problem

Are we able to provide
a *drop-in* post-quantum replacement for DH?

# Section 2: Outline

# CRS: Theory

## Definition (Schreier graph)

Let $G$ be a group *acting freely* on a set $X$ through the map

$$G \times X \to X$$
$$(\sigma, x) \mapsto \sigma \cdot x$$

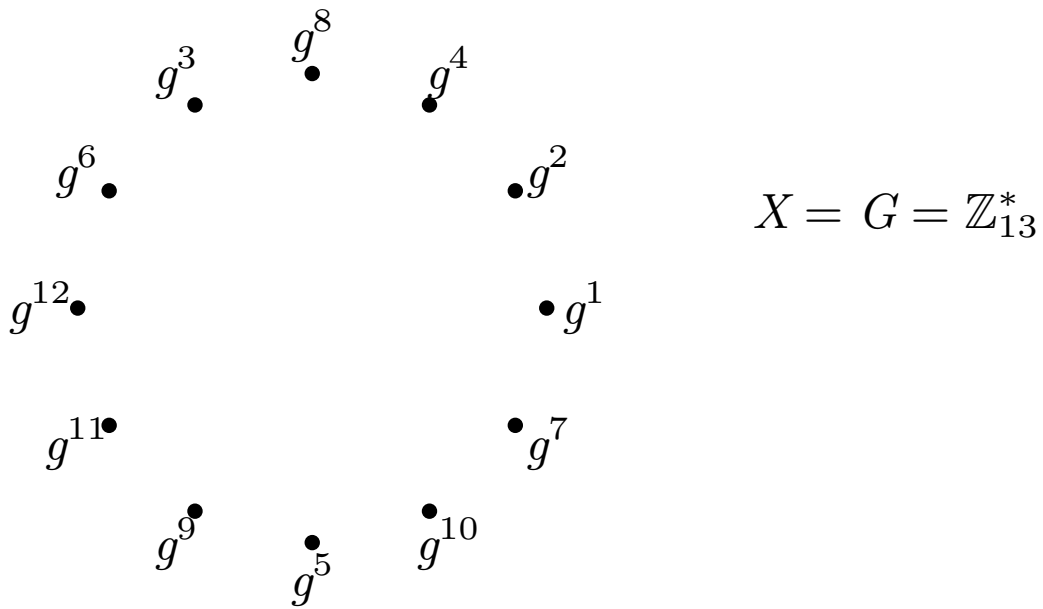
Let $S \subseteq G$ be a *symmetric* subset. The *Schreier graph* of $(S, X)$ is the graph whose vertices are the elements of $X$, and such that $x, x' \in X$ are connected by an edge if and only if $x' = \sigma \cdot x$ for some $\sigma \in S$.

## Definition (Schreier graph)

Let $G$ be a group *acting freely* on a set $X$ through the map

$$G \times X \to X$$
$$(\sigma, x) \mapsto \sigma \cdot x$$

Let $S \subseteq G$ be a *symmetric* subset. The *Schreier graph* of $(S, X)$ is the graph whose vertices are the elements of $X$, and such that $x, x' \in X$ are connected by an edge if and only if $x' = \sigma \cdot x$ for some $\sigma \in S$.



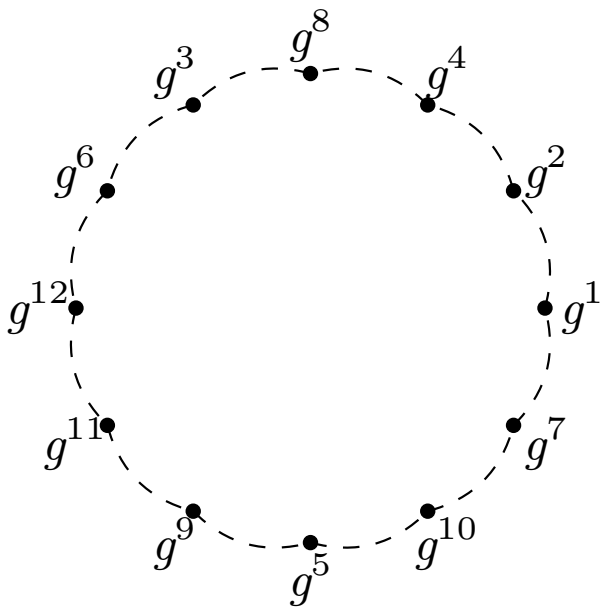

$$X = G = \mathbb{Z}_{13}^*$$

## Definition (Schreier graph)

Let $G$ be a group *acting freely* on a set $X$ through the map

$$G \times X \to X$$
$$(\sigma, x) \mapsto \sigma \cdot x$$

Let $S \subseteq G$ be a *symmetric* subset. The *Schreier graph* of $(S, X)$ is the graph whose vertices are the elements of $X$, and such that $x, x' \in X$ are connected by an edge if and only if $x' = \sigma \cdot x$ for some $\sigma \in S$.



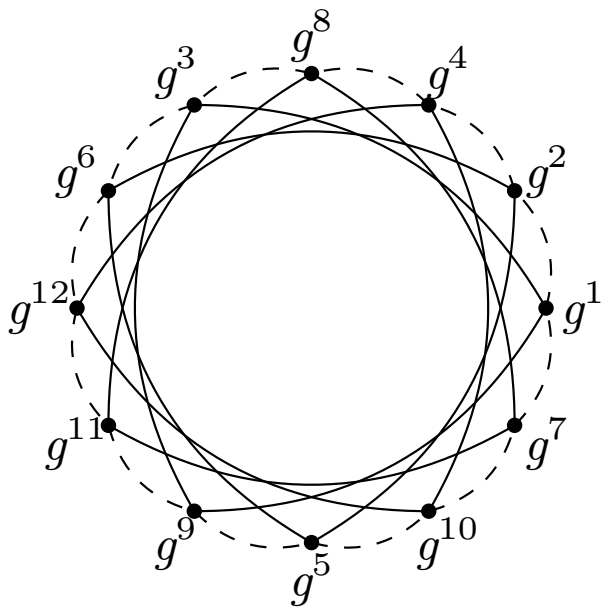

$$X = G = \mathbb{Z}_{13}^*$$
$$S = \{2, 2^{-1}\}$$

## Definition (Schreier graph)

Let $G$ be a group *acting freely* on a set $X$ through the map

$$G \times X \to X$$
$$(\sigma, x) \mapsto \sigma \cdot x$$

Let $S \subseteq G$ be a *symmetric* subset. The *Schreier graph* of $(S, X)$ is the graph whose vertices are the elements of $X$, and such that $x, x' \in X$ are connected by an edge if and only if $x' = \sigma \cdot x$ for some $\sigma \in S$.



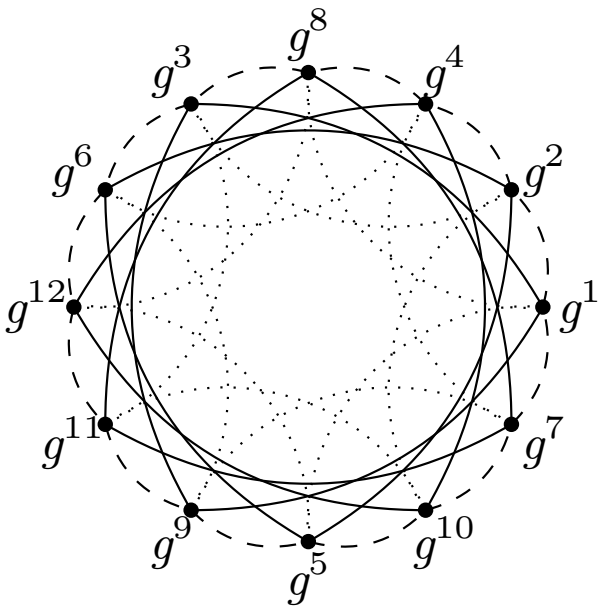

$$X = G = \mathbb{Z}_{13}^*$$
$$S = \{2, 2^{-1}\} \cup \{3, 3^{-1}\}$$

## Definition (Schreier graph)

Let $G$ be a group *acting freely* on a set $X$ through the map

$$G \times X \to X$$
$$(\sigma, x) \mapsto \sigma \cdot x$$

Let $S \subseteq G$ be a *symmetric* subset. The *Schreier graph* of $(S, X)$ is the graph whose vertices are the elements of $X$, and such that $x, x' \in X$ are connected by an edge if and only if $x' = \sigma \cdot x$ for some $\sigma \in S$.




$$X = G = \mathbb{Z}_{13}^*$$
$$S = \{2, 2^{-1}\} \cup \{3, 3^{-1}\} \cup \{5, 5^{-1}\}$$

## Where do we find a Schreier graph?

### Isogeny graph

**Definition (Isogeny)**

An *isogeny* is a morphism $\varphi : E \to E'$ such that $\varphi(O_E) = O_{E'}$

**Definition (Isogeny graph)**

Let $\mathbb{K}$ be a field. An *isogeny graph* is a directed graph such that:

- Its vertices are $\mathbb{K}$-isomorphism classes of elliptic curves over $\mathbb{K}$.
- Its edges are equivalence classes of isogenies defined over $\mathbb{K}$ between such curves

Where do we find a Schreier graph?

Isogeny graph

**Definition (Isogeny)**

An *isogeny* is a morphism $\varphi : E \to E'$ such that $\varphi(O_E) = O_{E'}$

**Definition (Isogeny graph)**

Let $\mathbb{K}$ be a field. An *isogeny graph* is a directed graph such that:

- Its vertices are $\mathbb{K}$-isomorphism classes of elliptic curves over $\mathbb{K}$.
- Its edges are equivalence classes of isogenies defined over $\mathbb{K}$ between such curves

# CRS: Theory

## Observation

The structure of an isogeny graph strongly depends on the structure of $\mathrm{End}(E)$.

## Theorem (Deuring)

The ring $\mathrm{End}(E)$ is isomorphic to one of the following:

- The integer ring $\mathbb{Z}$.
- An order $\mathcal{O}$ in a quadratic imaginary field $(\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K \subseteq K := \mathbb{Q}(\sqrt{-d}))$.
- A maximal order in a quaternion algebra.

- We consider curves of type 2.
- We consider isogeny of degree a prime $l$.
- We would like $l$ such that $\left(\frac{\Delta_K}{l}\right) = 1$.

# CRS: Theory

## Observation

The structure of an isogeny graph strongly depends on the structure of $\mathrm{End}(E)$.

## Theorem (Deuring)

The ring $\mathrm{End}(E)$ is isomorphic to one of the following:

- The integer ring $\mathbb{Z}$.
- An order $\mathcal{O}$ in a quadratic imaginary field $(\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K \subseteq K := \mathbb{Q}(\sqrt{-d}))$.
- A maximal order in a quaternion algebra.

- We consider curves of type 2.
- We consider isogeny of degree a prime $l$.
- We would like $l$ such that $\left(\frac{\Delta_K}{l}\right) = 1$.

# CRS: Theory

## Observation

The structure of an isogeny graph strongly depends on the structure of $\mathrm{End}(E)$.

## Theorem (Deuring)

The ring $\mathrm{End}(E)$ is isomorphic to one of the following:

- The integer ring $\mathbb{Z}$.
- An order $\mathcal{O}$ in a quadratic imaginary field $(\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K \subseteq K := \mathbb{Q}(\sqrt{-d}))$.
- A maximal order in a quaternion algebra.

- We consider curves of type 2.
- We consider isogeny of degree a prime $l$.
- We would like $l$ such that $\left(\frac{\Delta_K}{l}\right) = 1$.

# CRS: Theory

## Observation

The structure of an isogeny graph strongly depends on the structure of $\mathrm{End}(E)$.

## Theorem (Deuring)

The ring $\mathrm{End}(E)$ is isomorphic to one of the following:

- The integer ring $\mathbb{Z}$.
- An order $\mathcal{O}$ in a quadratic imaginary field $(\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K \subseteq K := \mathbb{Q}(\sqrt{-d}))$.
- A maximal order in a quaternion algebra.

- We consider curves of type 2.
- We consider isogeny of degree a prime $l$.
- We would like $l$ such that $\left(\frac{\Delta_K}{l}\right) = 1$.

# CRS: Theory

## Observation

The structure of an isogeny graph strongly depends on the structure of $\mathrm{End}(E)$.

## Theorem (Deuring)

The ring $\mathrm{End}(E)$ is isomorphic to one of the following:

- The integer ring $\mathbb{Z}$.
- An order $\mathcal{O}$ in a quadratic imaginary field $(\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K \subseteq K := \mathbb{Q}(\sqrt{-d}))$.
- A maximal order in a quaternion algebra.

- We consider curves of type 2.
- We consider isogeny of degree a prime $l$.
- We would like $l$ such that $\left(\frac{\Delta_K}{l}\right) = 1$.

# CRS: Theory

## Observation

The structure of an isogeny graph strongly depends on the structure of $\mathrm{End}(E)$.

## Theorem (Deuring)

The ring $\mathrm{End}(E)$ is isomorphic to one of the following:

- The integer ring $\mathbb{Z}$.
- An order $\mathcal{O}$ in a quadratic imaginary field $(\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K \subseteq K := \mathbb{Q}(\sqrt{-d}))$.
- A maximal order in a quaternion algebra.

- We consider curves of type 2.
- We consider isogeny of degree a prime $l$.
- We would like $l$ such that $\left(\frac{\Delta_K}{l}\right) = 1$.

# CRS: Theory

## Observation

The structure of an isogeny graph strongly depends on the structure of $\mathrm{End}(E)$.

## Theorem (Deuring)

The ring $\mathrm{End}(E)$ is isomorphic to one of the following:

- The integer ring $\mathbb{Z}$.
- An order $\mathcal{O}$ in a quadratic imaginary field $(\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K \subseteq K := \mathbb{Q}(\sqrt{-d}))$.
- A maximal order in a quaternion algebra.

- We consider curves of type 2.
- We consider isogeny of degree a prime $l$.
- We would like $l$ such that $\left(\frac{\Delta_K}{l}\right) = 1$.

# CRS: Theory

## Observation

The structure of an isogeny graph strongly depends on the structure of $\mathrm{End}(E)$.

## Theorem (Deuring)

The ring $\mathrm{End}(E)$ is isomorphic to one of the following:

- The integer ring $\mathbb{Z}$.
- An order $\mathcal{O}$ in a quadratic imaginary field $(\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K \subseteq K := \mathbb{Q}(\sqrt{-d}))$.
- A maximal order in a quaternion algebra.

- We consider curves of type 2.
- We consider isogeny of degree a prime $l$.
- We would like $l$ such that $\left(\frac{\Delta_K}{l}\right) = 1$.

# CRS: Theory

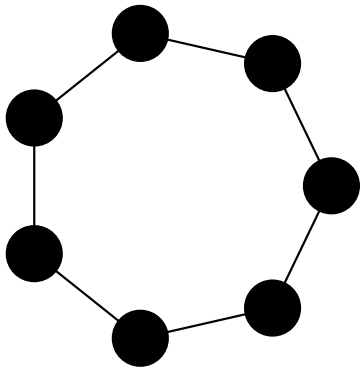
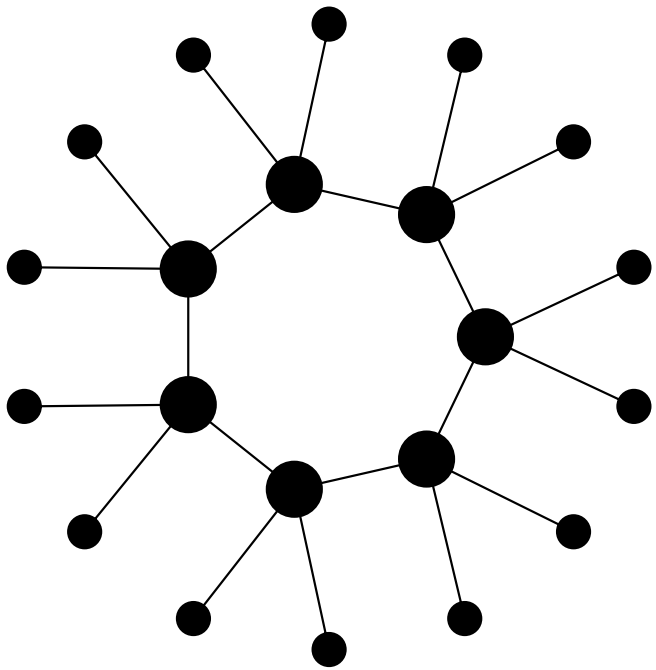



Figure: A volcano of 3-isogenies and the corresponding tower of orders.



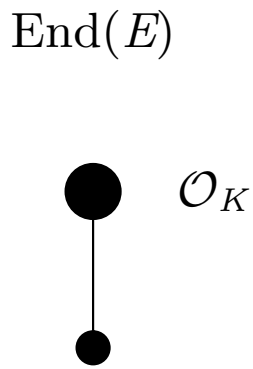
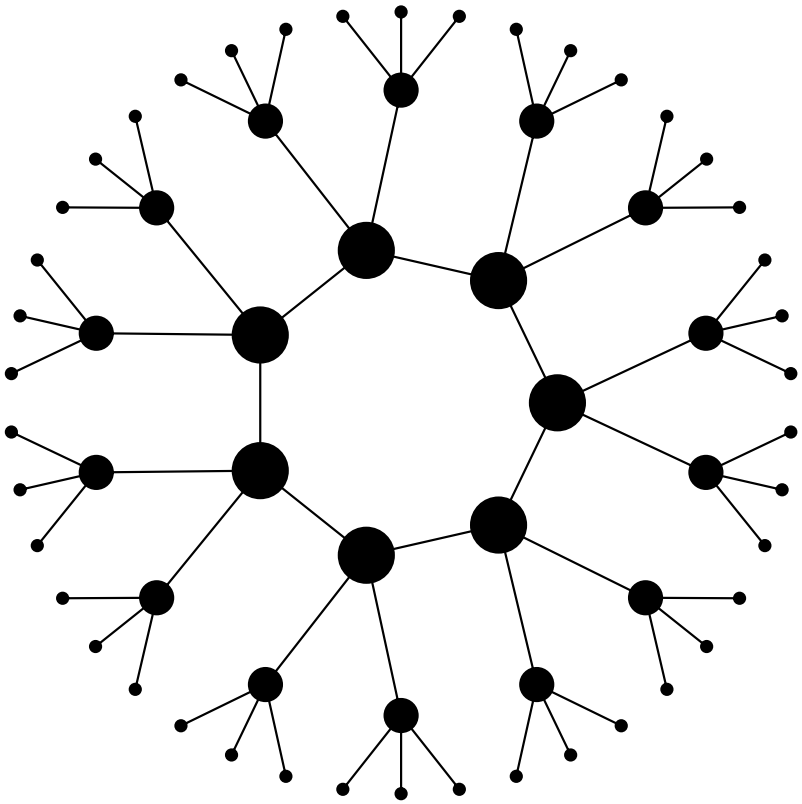



Figure: A volcano of 3-isogenies and the corresponding tower of orders.

# CRS: Theory



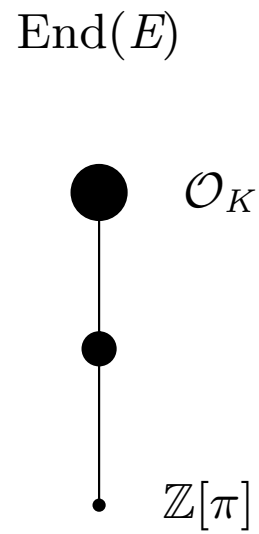
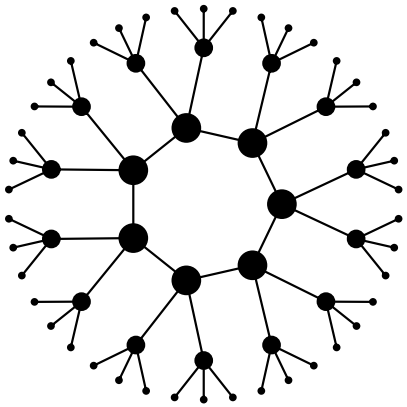
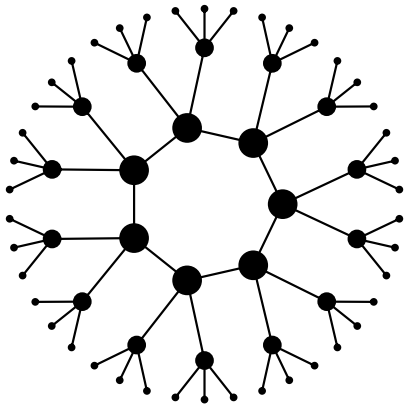
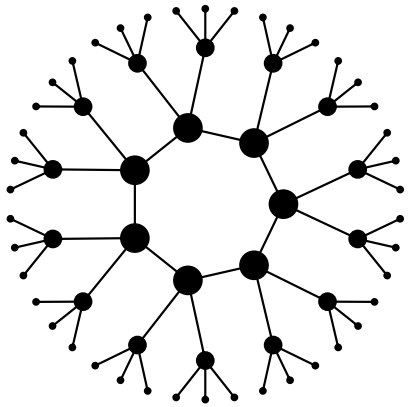



Figure: A volcano of 3-isogenies and the corresponding tower of orders.

**Definition (Ideal class group)**

Let $\mathcal{O}$ be an order in a number field $K$. The *ideal class group* of $\mathcal{O}$ is the quotient

$$\mathrm{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}).$$

**Definition ($\mathfrak{a}$-torsion)**

Let $\mathfrak{a} \subseteq \mathcal{O}$ be an integral invertible ideal of norm coprime to $q$. We define the *$\mathfrak{a}$-torsion subgroup* of $E$ as

$$E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\}.$$

The most unique property of (separable) isogenies is that they are entirely determined by their kernel.

$\downarrow$

Given an ideal $\mathfrak{a} \subseteq \mathcal{O}$ as above, it is natural to define the isogeny $\varphi_{\mathfrak{a}} : E \to E_{\mathfrak{a}}$, where $E_{\mathfrak{a}} = E/E[\mathfrak{a}]$

# CRS: Theory

**Theorem**

The class group $\mathrm{Cl}(\mathcal{O})$ acts *freely* and *transitively* on $\mathrm{Ell}_q(\mathcal{O})$ through the map

$$\begin{aligned} \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_q(\mathcal{O}) &\to \mathrm{Ell}_q(\mathcal{O}) \\ (\mathfrak{a}, E) &\mapsto \mathfrak{a} \cdot E := E/E[\mathfrak{a}] \end{aligned}$$

We have found a set $(\mathrm{Ell}_q(\mathcal{O}))$ and a group $(\mathrm{Cl}(\mathcal{O}))$ acting on it regularly

# CRS: Theory

**Where is our symmetric subset $S$?**

**Proposition**

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.

# CRS: Theory

Where is our symmetric subset $S$?

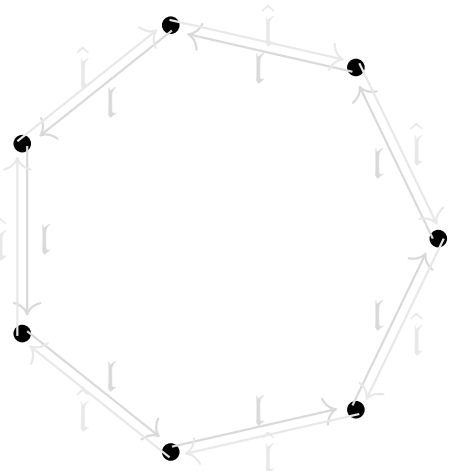
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

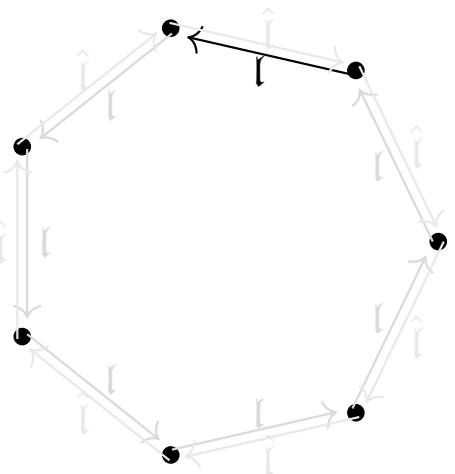
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

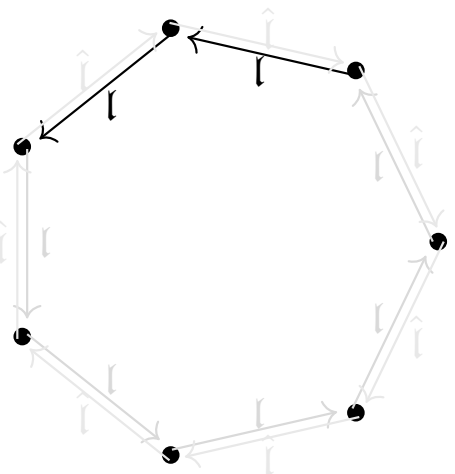
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

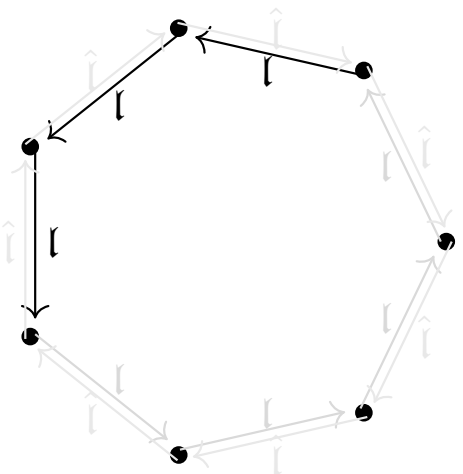
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

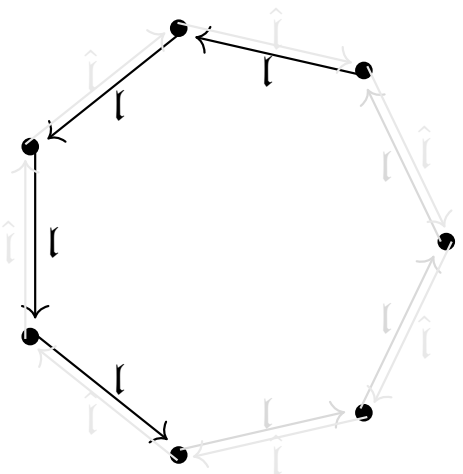
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

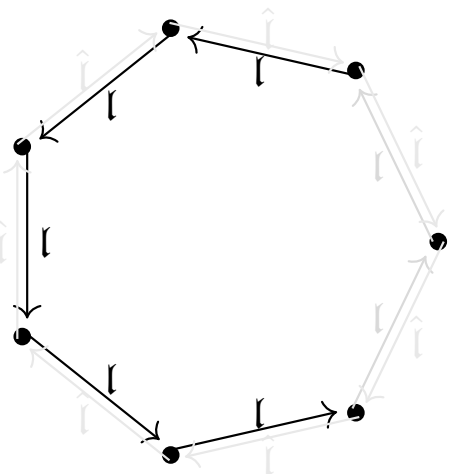
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

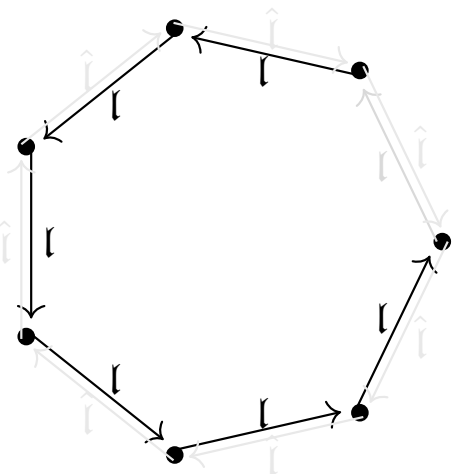
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

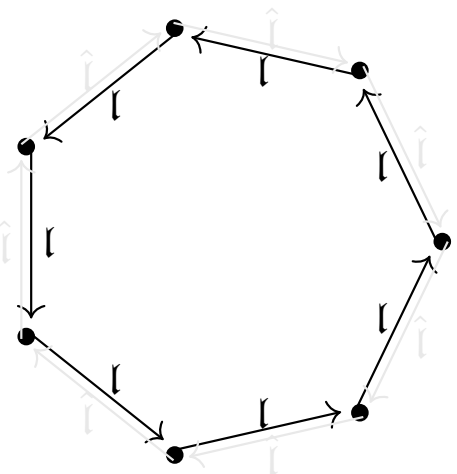
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

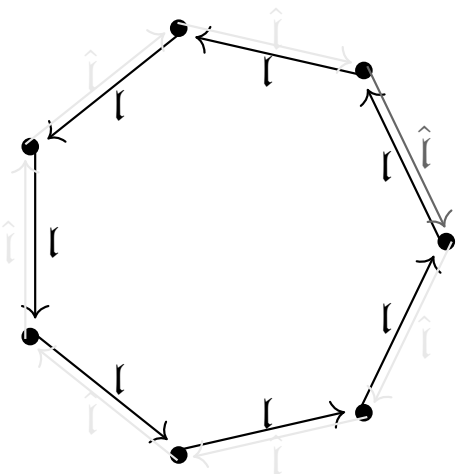
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

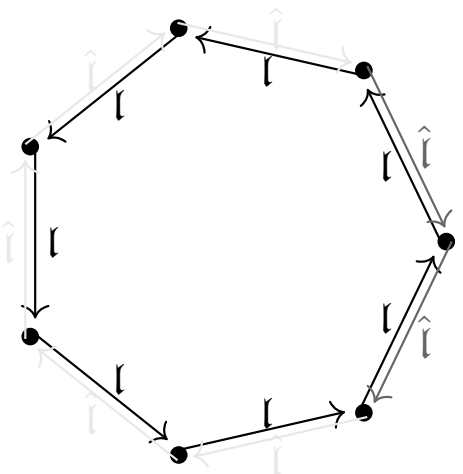
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

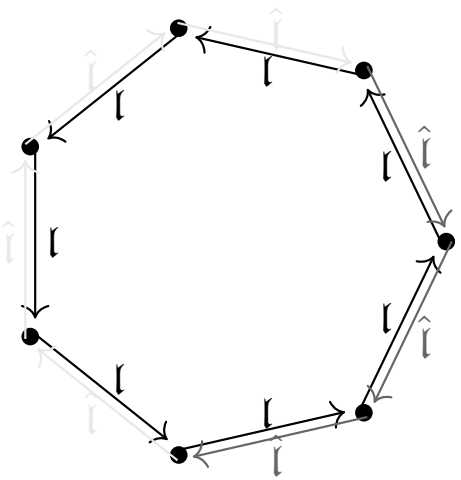
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

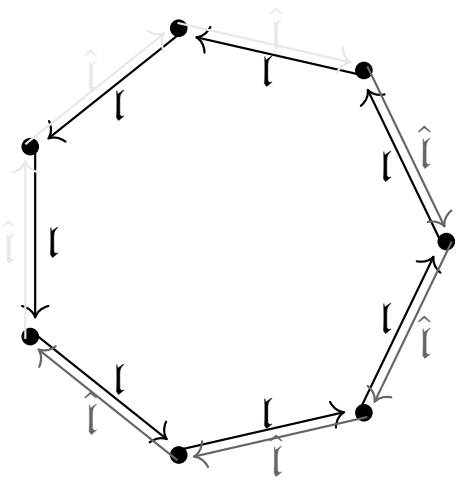
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

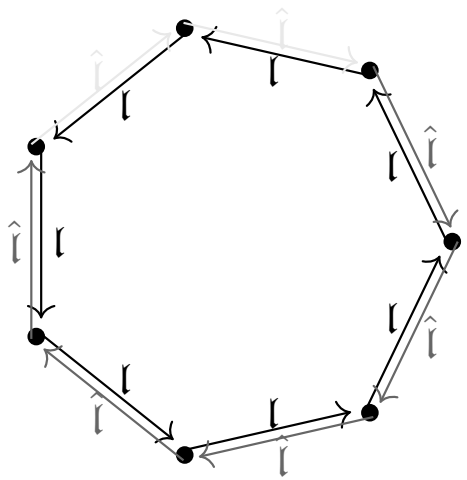
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

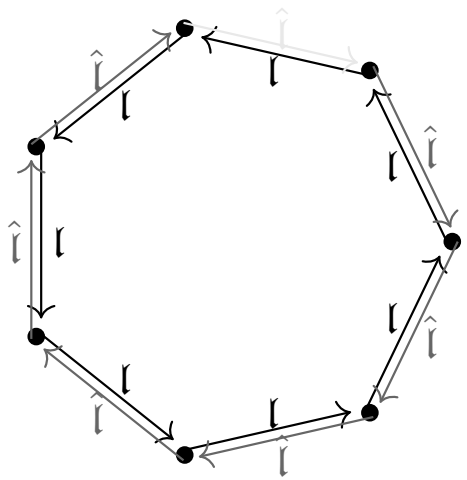
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



# CRS: Theory

Where is our symmetric subset $S$?

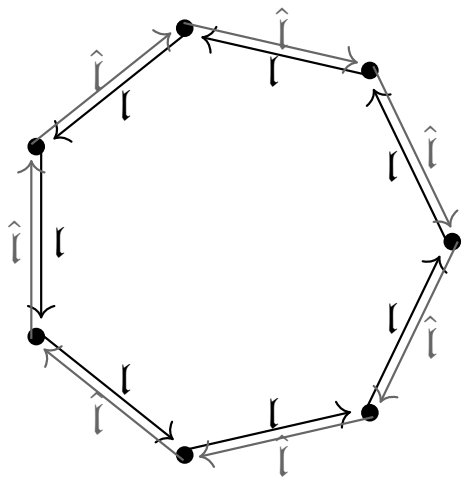
## Proposition

The following are equivalent:

- $l$ Elkies prime.
- $(l) = \mathfrak{l} \cdot \hat{\mathfrak{l}}$, where $\mathfrak{l} = (\pi - \lambda, l)$ and $\hat{\mathfrak{l}} = (\pi - \mu, l)$ where

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod l$$

.



We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

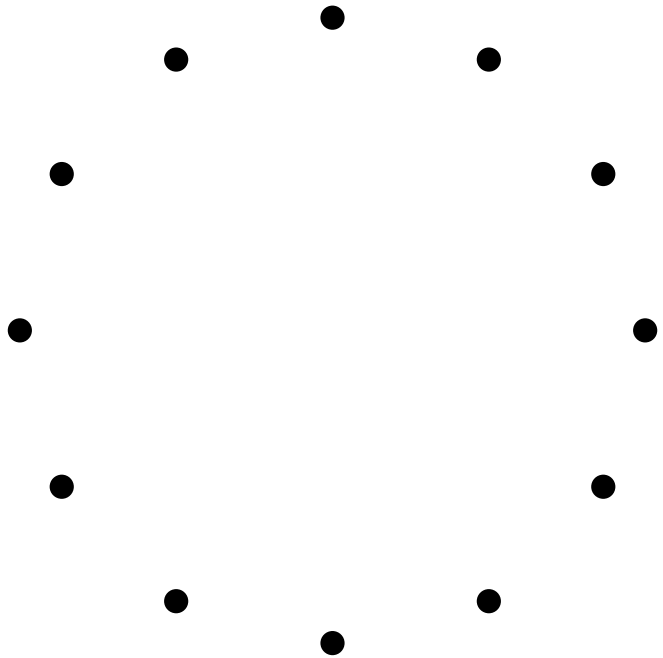


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

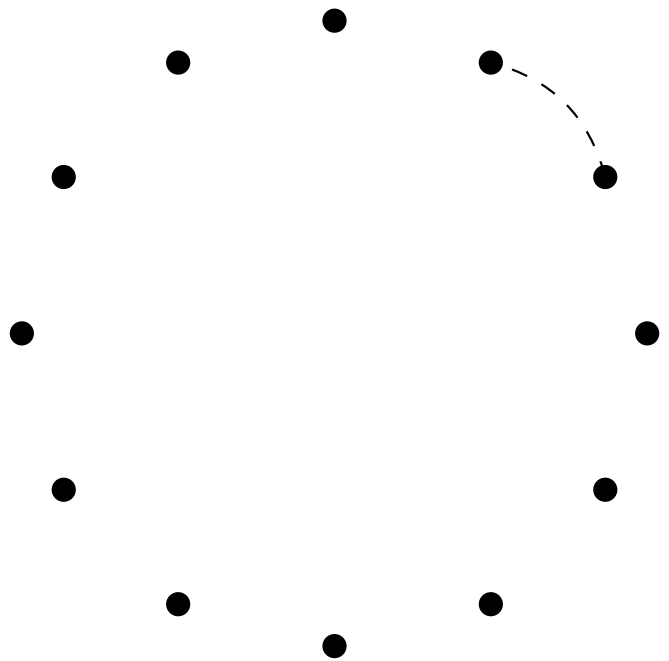


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

# CRS: Theory

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

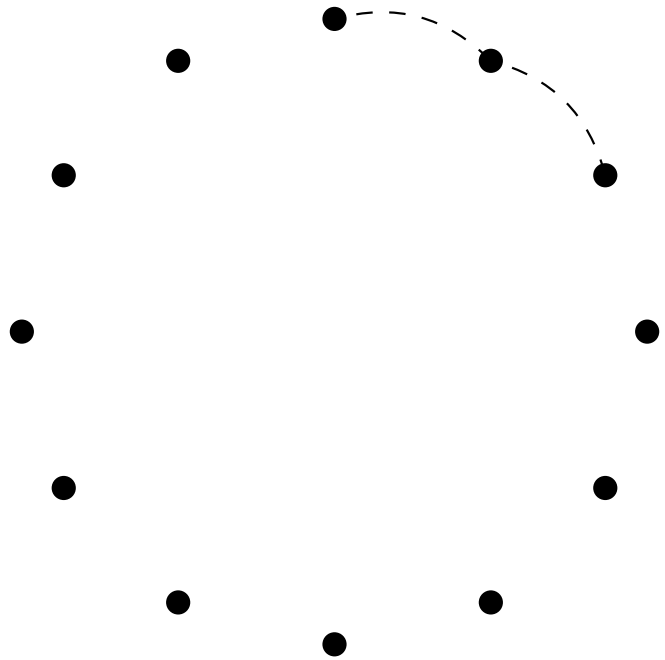


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

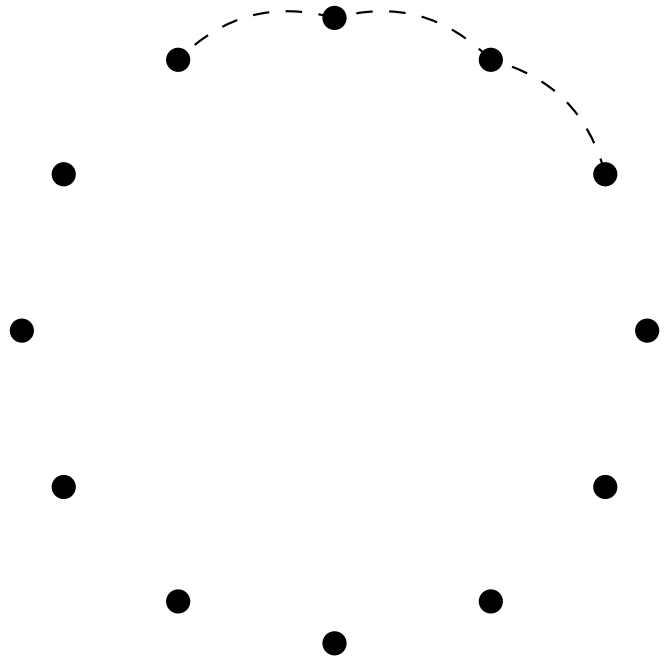


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

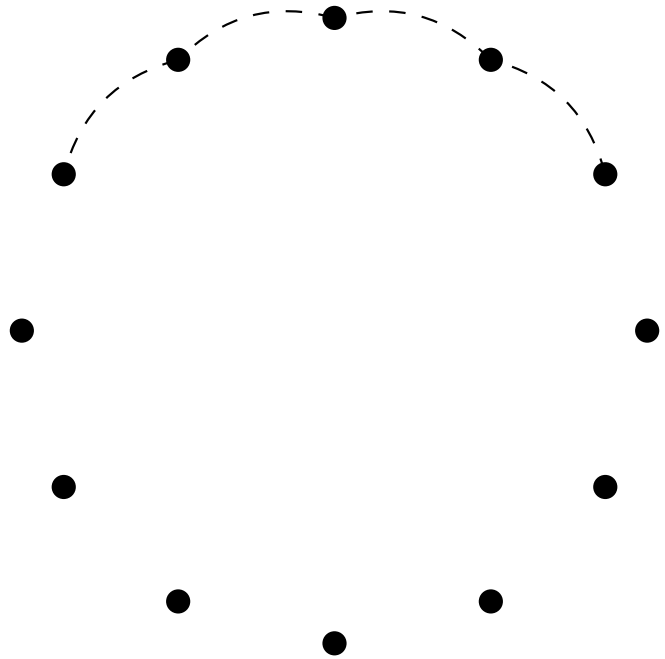


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

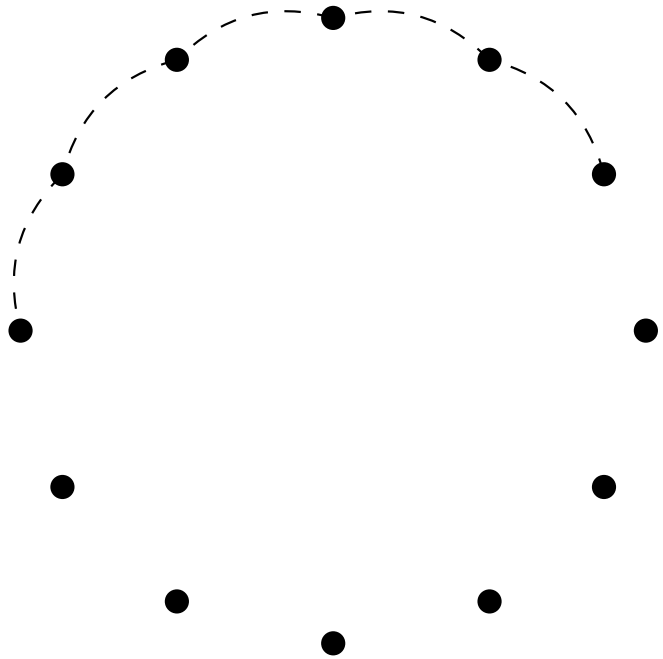


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

# CRS: Theory

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

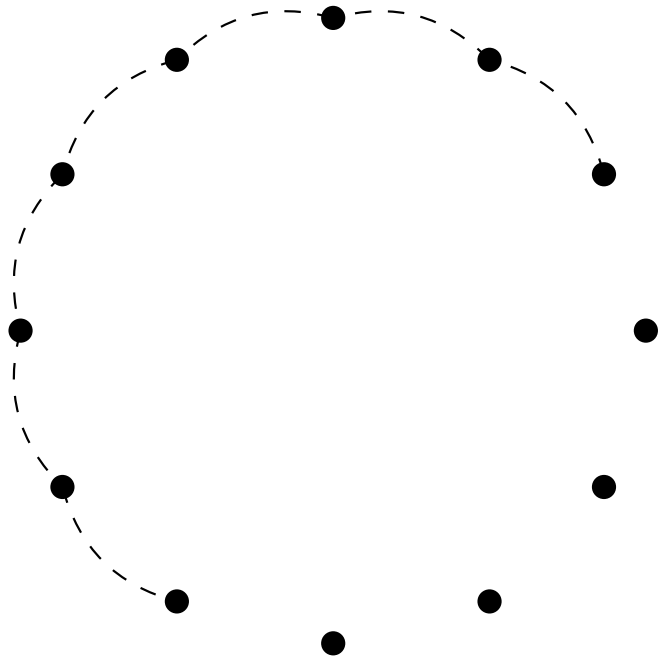


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

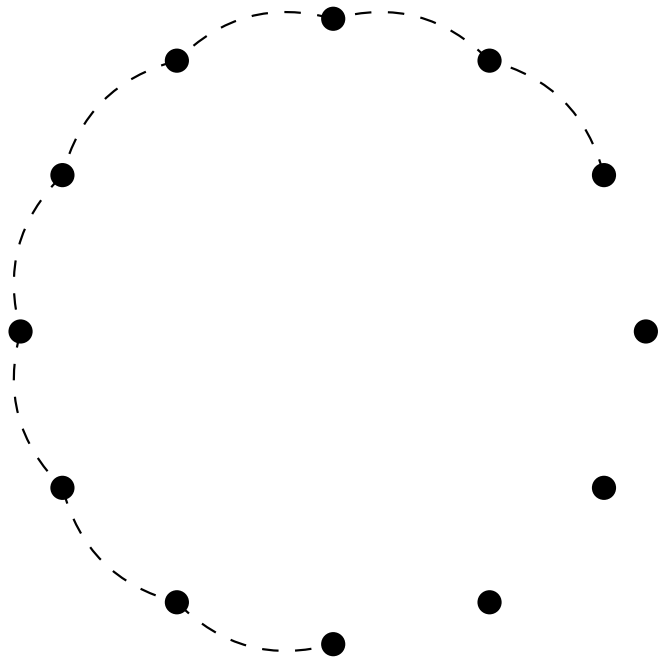


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

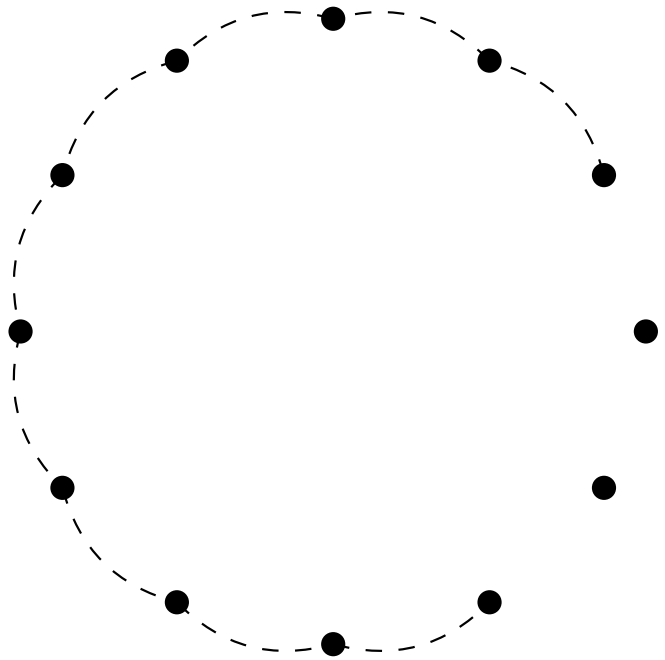


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

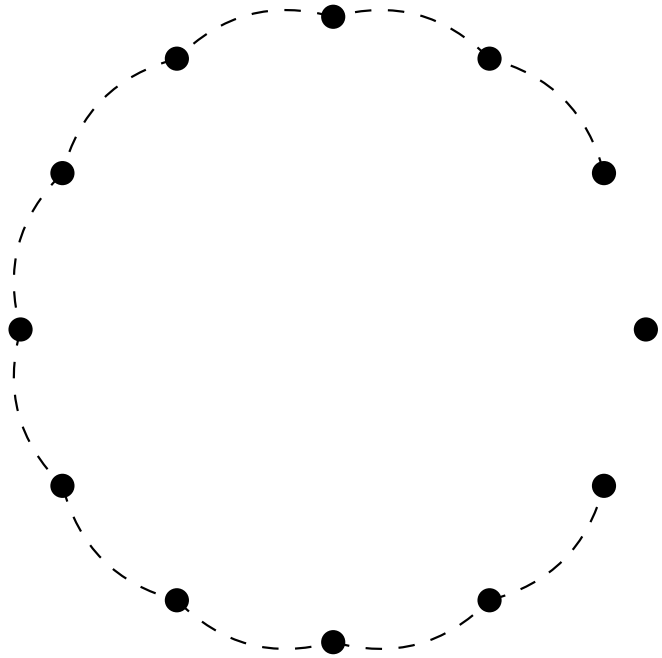


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

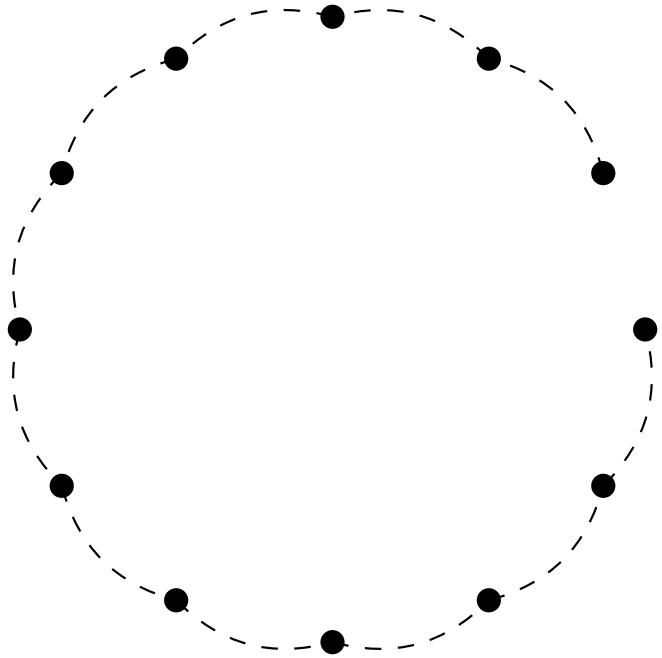


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

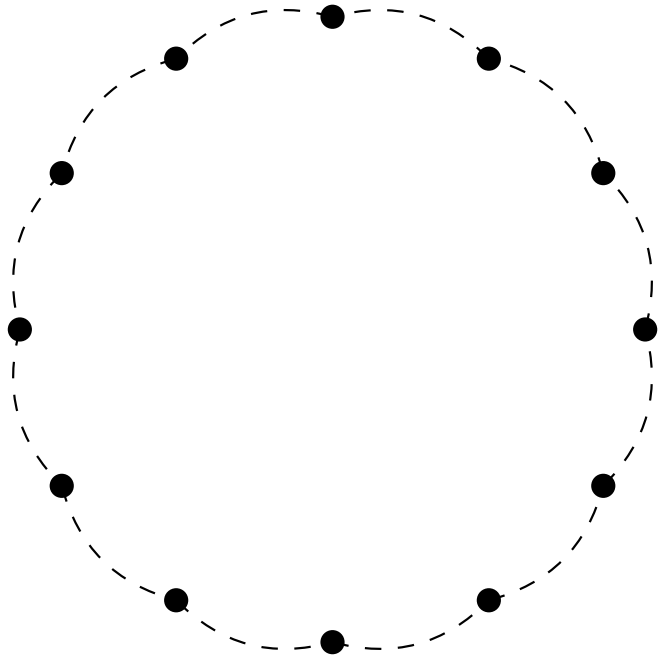


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

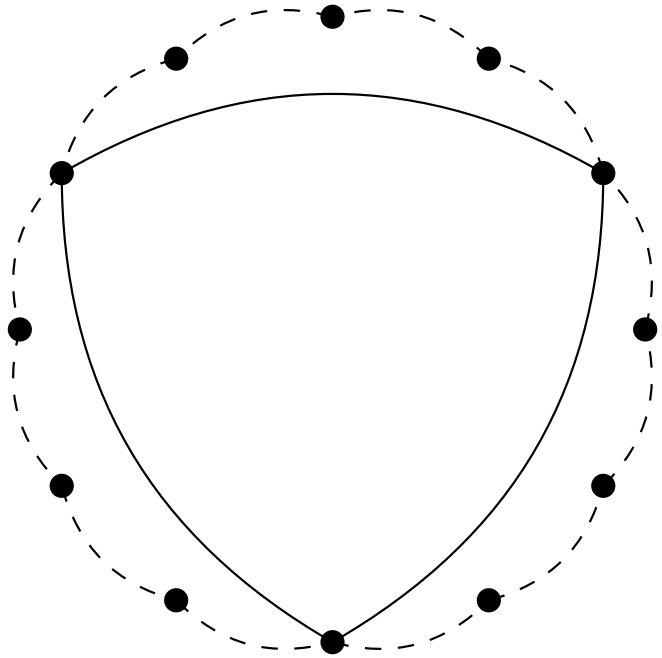


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

# CRS: Theory

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

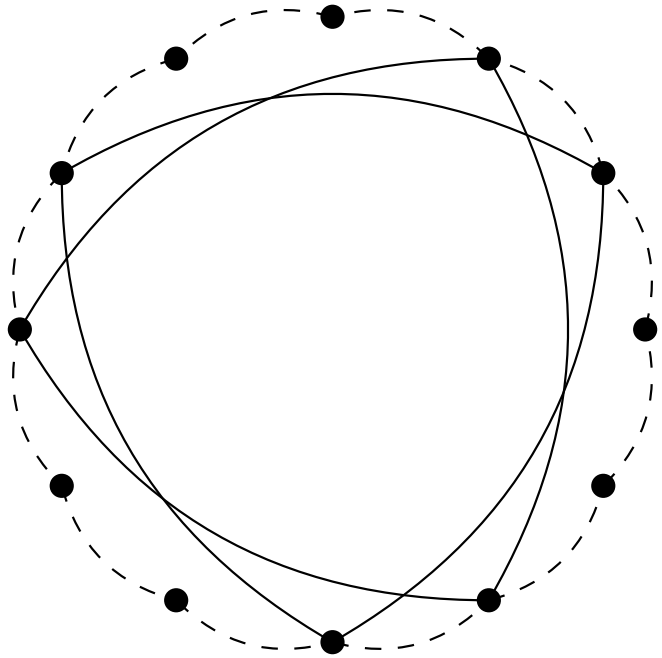


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

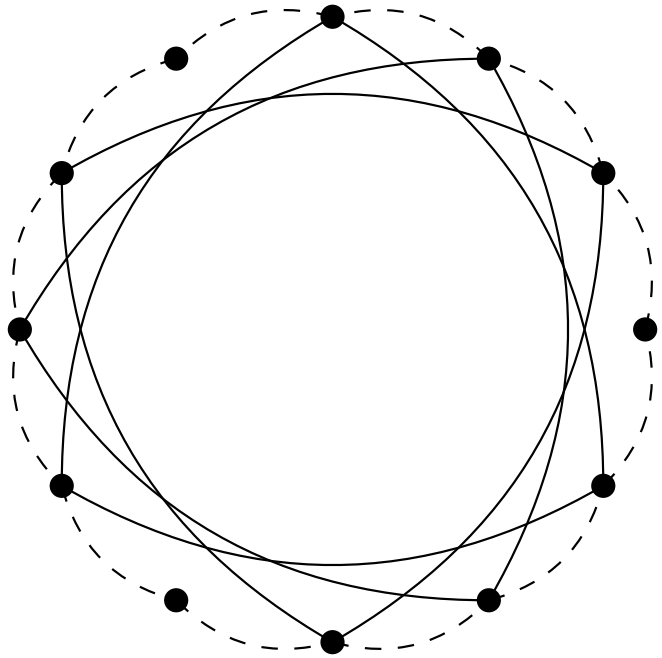


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

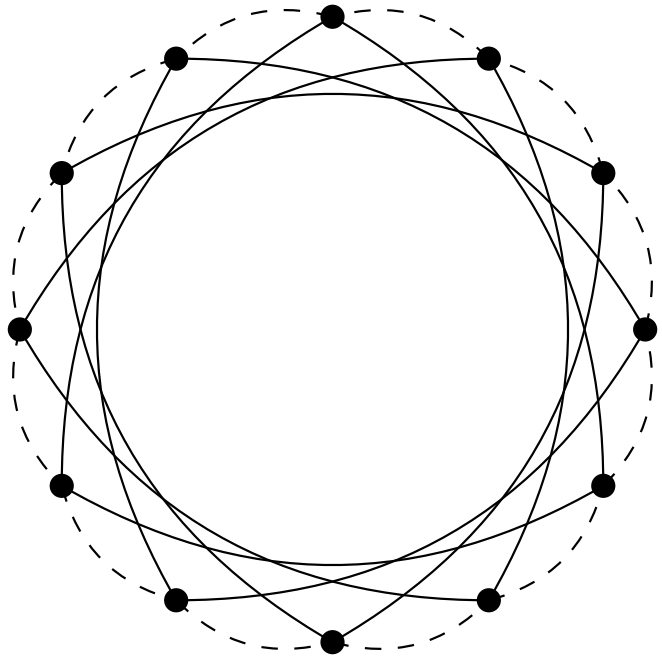


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

# CRS: Theory

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

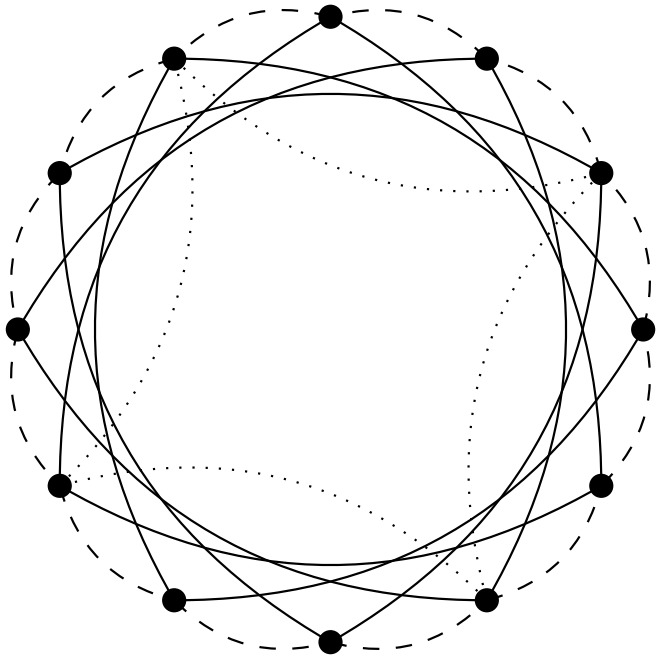


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

# CRS: Theory

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

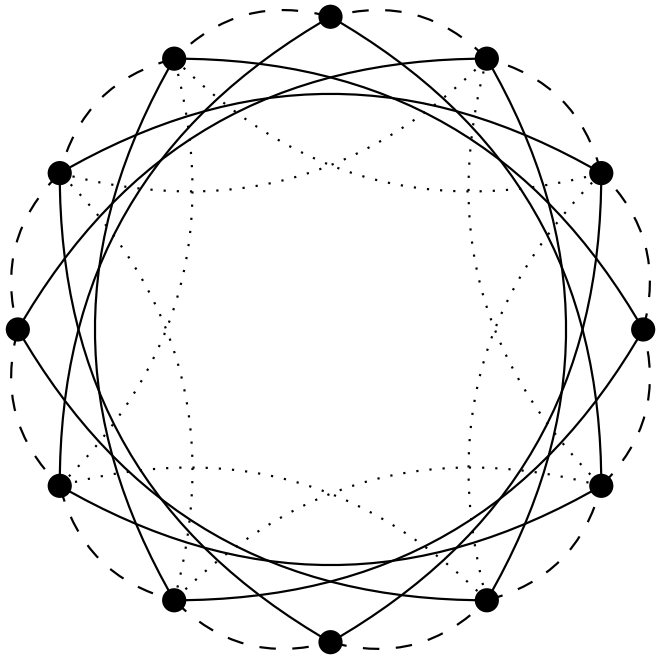


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

# CRS: Theory

We could collect more pairs $(\mathfrak{l}, \hat{\mathfrak{l}})$ together to build a symmetric subset of $\mathrm{Cl}(\mathcal{O})$.

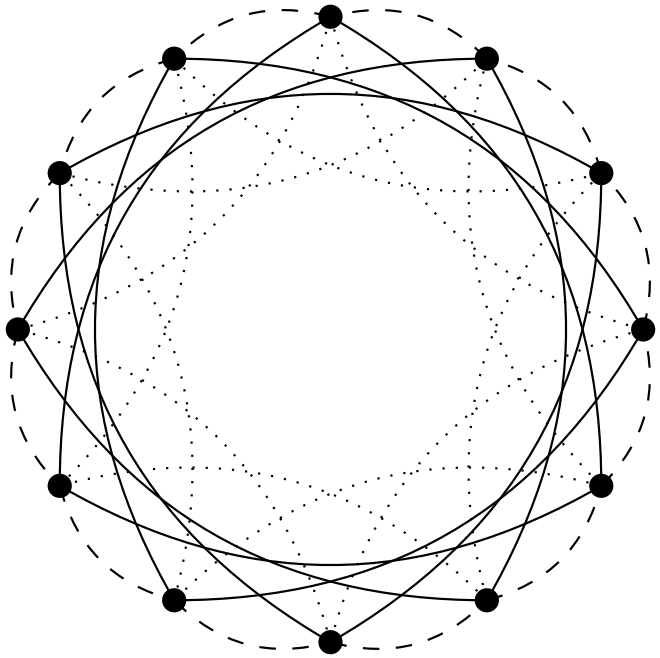


Figure: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees

# CRS: The Protocol

| Public parameters | An elliptic curve $E$ over a finite field $\mathbb{F}_q$<br>A set of Elkies primes $L = \{l_1, \ldots, l_m\}$<br>A Frobenius eigenvalue $\lambda_i$ for each $l_i$ | |
|---|---|---|
| | **Alice** | **Bob** |
| Pick random secret | $\rho_A \in L^*$ | $\rho_B \in L^*$ |
| Compute public data | $E_A = \rho_A(E)$ | $E_B = \rho_B(E)$ |
| Exchange data | $E_A \longrightarrow$ | $\longleftarrow E_B$ |
| Compute shared secret | $E_{AB} = \rho_A(E_B)$ | $E_{AB} = \rho_B(E_A)$ |

Table: Couveignes-Rostovtsev-Stolbunov key exchange protocol.

# CRS: Security

**Definition (Key recovery problem)**

Given two elliptic curves $E_0, E$ defined over $\mathbb{F}_p$ with the same rational endomorphism ring $\mathcal{O}$, find an ideal $\mathfrak{a}$ of $\mathcal{O}$ such that $[\mathfrak{a}]E_0 = E$.

# CRS: Problems

## Observation

- Breaking the CRS scheme amounts to solve an instance of the abelian hidden-shift problem, for which quantum algorithms with subexponential time complexity are known to exist.
- The protocol is unacceptably slow.

# CRS: Problems

## Observation

- Breaking the CRS scheme amounts to solve an instance of the abelian hidden-shift problem, for which quantum algorithms with subexponential time complexity are known to exist.
- The protocol is unacceptably slow.

# Index

# CSIDH: Main Idea

Try to use supersingular curves and supersingular isogeny graphs.

For these curves the *full* endomorphism ring is isomorphic to and order in a quaternion algebra.

However, if we consider:

- Curves over $\mathbb{F}_p$.
- Isogenies over $\mathbb{F}_p$.

$\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathcal{O} \subseteq \mathbb{Q}(\sqrt{-d})$

We can adapt the previous theory!

# CSIDH: Benefits

## Supersingular curves' benefits

- Structure of $\mathrm{Cl}(\mathcal{O})$.
- Elkies primes.
- Efficient evaluation of the class group action.
- Public key & PKV.

# CSIDH: Class group structure

$$\#\operatorname{Cl}(\mathcal{O}) \approx \sqrt{|D_\pi|} = \sqrt{|t_\pi^2 - 4p|}$$

- The size of $\operatorname{Cl}(\mathcal{O})$ is as big as possible.
- For a fixed security level we can do an almost minimal choice for $p$.

# CSIDH: Elkies primes

## Previous problem

Inefficiency in the search for Elkies primes.

And now?

$E$ supersingular elliptic curve over $\mathbb{F}_p$, $p = 4 \cdot l_1 \cdots l_n - 1$

$$\begin{aligned} \#E(\mathbb{F}_p) &\equiv p + 1 \pmod{l_i} \\ &\equiv 4 \cdot l_1 \cdots l_n - 1 + 1 \pmod{l_i} \\ &\equiv 0 \pmod{l_i} \end{aligned}$$

$$\begin{aligned} \pi^2 - t\pi + p &\equiv 0 \pmod{l_i} \\ \pi^2 + p &\equiv 0 \pmod{l_i} \\ \pi^2 - 1 &\equiv 0 \pmod{l_i} \\ (\pi + 1)(\pi - 1) &\equiv 0 \pmod{l_i} \end{aligned}$$

Every $l_i$ is an Elkies prime and $\mathfrak{l}_i = (\pi - 1, l), \hat{\mathfrak{l}}_i = (\pi + 1, l)$

# CSIDH: Class group action

**How to compute $[\mathfrak{l}]E$ for $\mathfrak{l} = (l, \pi - \lambda)$**

- Find a basis of the $l$-torsion.
- Compute the eigenspaces of the Frobenius.
- Apply Vélu type formulas to a basis point $P$ of the correct eigenspace.

**Observation ($\lambda = 1$)**

In this case $P$ (has order $l$ and) lies in $\ker(\pi - 1)$, i.e. is defined over $\mathbb{F}_p$.

**Observation ($\lambda = -1$)**

In this case $P$ (has order $l$ and) lies in $\ker(\pi + 1)$, i.e. is defined over $\mathbb{F}_{p^2}$.

# CSIDH: Public key & PKV

Before we encoded an elliptic curve with its j-invariant.

And now?

## Proposition

Suppose

- $p \geq 5$, $p \equiv 3 \pmod 8$.
- $E/\mathbb{F}_p$ supersingular elliptic curve.

Then

$$\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\pi] \iff E \cong_{\mathbb{F}_p} E_A : y^2 = x^3 + Ax^2 + x$$

for some $A \in \mathbb{F}_p$. Moreover, if such an $A$ exists then it is unique.

# CSIDH: Public key & PKV

## Observation (Public key)

We can use the coefficient $A$ as public key.

## Observation (Public key validation)

When we receive $A$ all we have to do is to check that $y^2 = x^3 + Ax^2 + x$ is supersingular.

# CSIDH: The Protocol

| Public parameters | A prime $p$ of the form $4 \cdot l_1 \cdots l_n - 1$<br>$E := y^2 = x^3 + x$ over $\mathbb{F}_p$ | |
|---|---|---|
| | **Alice** | **Bob** |
| Pick random secret | $(e_1, ..., e_n) \in \{-m, ..., m\}^*$ | $(e'_1, ..., e'_n) \in \{-m, ..., m\}^*$ |
| Compute public data | $E_A = [\mathfrak{a}]E = [\mathfrak{l}_1^{e_1} ... \mathfrak{l}_n^{e_n}]E$ | $E_B = [\mathfrak{b}]E = [\mathfrak{l}_1^{e'_1} ... \mathfrak{l}_n^{e'_n}]E$ |
| Exchange data | $E_A \longrightarrow$ | $\longleftarrow E_B$ |
| Compute shared secret | $E_{AB} = [\mathfrak{a}]E_B$ | $E_{AB} = [\mathfrak{b}]E_A$ |

Table: CSIDH key exchange protocol.

# Conclusions

- Does not avoid subexponential attack (HSP).
- Drop-in post quantum replacement for Diffie Hellman.
- Speed is practical (80 ms for a single key-exchange).
- Smallest public key size in the portfolio of PQ-crypto.

*Thanks*

Extra

# Keys' dimension

## Public key

$A \in \mathbb{F}_p$ can be represented with $\log p$ bits.

## Private Key

We need to find how big is the quantity $n \cdot \log m$.

$$
\begin{aligned}
(2m+1)^n &\approx \#\,\mathrm{Cl}(\mathcal{O}) \\
\log(2m+1)^n &\approx \log \#\,\mathrm{Cl}(\mathcal{O}) \\
n \cdot \log(2m+1) &\approx \log \sqrt{p} \\
n \cdot \log m &\approx \log p/2
\end{aligned}
$$

# CRS: Volcanology

Couveignes focuses on regular curves $E/\mathbb{F}_q$, with $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathbb{Q}(\sqrt{-d})$.

Given $E/\mathbb{F}_q$, how many isogenies defined over $\mathbb{F}_q$ do have $E$ as domain?

## Proposition

Let $E/\mathbb{F}_q$ an elliptic curve and $l \neq p$ be a prime.

1. There are $l+1$ distinct isogenies of degree  with domain $E$ defined over the algebraic closure $\overline{\mathbb{F}}_q$.
2. There are $0, 1, 2$ or $l+1$ isogenies of degree $l$ with domain $E$ defined over $\mathbb{F}_q$.

# CRS: Volcanology

What is the relationship between two isogenous curves?

## Proposition (Horizontal and vertical isogenies)

Let $\varphi : E \to E'$ be an isogeny of prime degree , and let $\mathcal{O}, \mathcal{O}'$ be the orders corresponding to $E, E'$. Then, either $\mathcal{O} \subseteq \mathcal{O}'$ or $\mathcal{O}' \subseteq \mathcal{O}$, and one of the following is true:

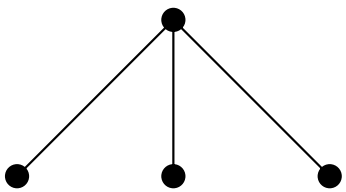
- $\mathcal{O} = \mathcal{O}'$, in this case $\varphi$ is said to *horizontal*.
- $[\mathcal{O}' : \mathcal{O}] = l$, in this case $\varphi$ is said to be *ascending*.
- $[\mathcal{O} : \mathcal{O}'] = l$, in this case $\varphi$ is said to be *descending*.

# CRS: Volcanology

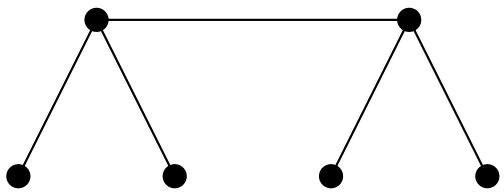
Global stucture: how many horizontal and vertical $l$-isogenies does a given curve have?

| | | $\rightarrow$ | $\uparrow$ | $\downarrow$ |
|---|---|---|---|---|
| $\mathbb{Z}[\pi] = \mathcal{O}_K$ | Surface = Middle = Floor | $1 + \left(\frac{\Delta_K}{l}\right)$ | | |
| $\mathbb{Z}[\pi] \subsetneq \mathcal{O}_K$ | Surface | $1 + \left(\frac{\Delta_K}{l}\right)$ | | $l - \left(\frac{\Delta_K}{l}\right)$ |
| | Middle | | 1 | $l$ |
| | Floor | | 1 | |

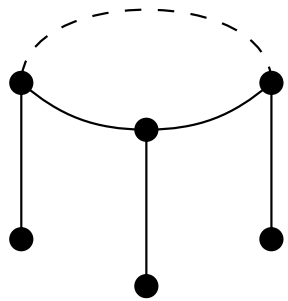
Table: Number and types of $l$-isogenies



Atkin: $\left(\frac{\Delta_K}{l}\right) = -1$



Ramified: $\left(\frac{\Delta_K}{l}\right) = 0$



Elkies: $\left(\frac{\Delta_K}{l}\right) = +1$

# CSIDH: Classical security

## Exhaustive key search

## Meet-in-the-middle attack

## Pohlig-Hellman style attack

# CSIDH: Quantum security

## Observation (The query model)

Given a black-box function $f$, we have to answer a question about it. Instead of measuring the time complexity of our algorithm, we measure the query complexity: the number of queries it makes to $f$.

### Why do we use the query model?

- Often the function $f$ is efficient to implement.
- All known interesting quantum algorithm fit in the query paradigm.

# Quantum attacks based on the abelian hidden shift problem

## Definition (A-HSP)

Let $A$ be a finite abelian group, $T$ a finite set and let $f_1, f_2 : A \to T$ be black-box functions. The functions $f_1, f_2$ are said to hide a shift $s \in A$ if $f_1$ is injective and $f_2(x) = f_1(xs)$ for all $x \in A$. The goal is then to recover $s$ by evaluating the functions $f_1$ and $f_2$.

$$\begin{aligned} f_1 : \mathrm{Cl}(\mathcal{O}) &\longrightarrow \mathrm{Ell}(\mathcal{O}) \\ \mathfrak{b} &\longmapsto [\mathfrak{b}]\, E_0 \end{aligned} \qquad \begin{aligned} f_2 : \mathrm{Cl}(\mathcal{O}) &\longrightarrow \mathrm{Ell}(\mathcal{O}) \\ \mathfrak{b} &\longmapsto [\mathfrak{b}]\, E_A \end{aligned}$$

These function hide the private key $\mathfrak{a}$ as a shift:

$$\begin{aligned} f_1(x \cdot \mathfrak{a}) &= [x \cdot \mathfrak{a}]\, E_A \\ &= [x]\, [\mathfrak{a}]\, E_A \\ &= [x]\, E_B \\ &= f_2(x) \end{aligned}$$

# Quantum attacks on the A-HSP

## Kuperberg

space and query complexity: $2^{O(\sqrt{\log n})}$

## Regev

query complexity: $2^{O(\sqrt{\log n \log\log n})}$
space complexity: polynomial

## Kuperberg

classical space and query complexity: $2^{O(\sqrt{\log n})}$
quantum space: $O(\log n)$

- These algorithms are shown to have subexponential complexity in the limit.
- In a generic group the query complexity coincides with the time complexity,

BUT

in our case the evaluation of $f_1, f_2$ means evaluating the action $[\mathfrak{a}]\,E_0, [\mathfrak{a}]\,E_A$, which is non-trivial.

$$\Downarrow$$

The time complexity must take into account this important factor.

- Regev: $L_N[1/2, \sqrt{2}] = \exp\left[(\sqrt{2}+1)\sqrt{\ln N \ln\ln N}\right]$ where $N = \#\,\mathrm{Cl}(\mathcal{O})$.
- Bisson: $L_p[1/2, 1/\sqrt{2}] = \exp\left[(1/\sqrt{2}+1)\sqrt{\ln p \ln\ln p}\right]$
- Regev + Bisson: $L_p[1/2, 3/\sqrt{2}] \Longrightarrow L_p[1/2, 1+\sqrt{2}]$.

- Kuperberg + Bisson: $L_p[1/2, 1/\sqrt{2}]$.

- Regev: $L_N[1/2, \sqrt{2}] = \exp\left[(\sqrt{2}+1)\sqrt{\ln N \ln\ln N}\right]$ where $N = \#\,\mathrm{Cl}(\mathcal{O})$.
- Bisson: $L_p[1/2, 1/\sqrt{2}] = \exp\left[(1/\sqrt{2}+1)\sqrt{\ln p \ln\ln p}\right]$
- Regev + Bisson: $L_p[1/2, 3/\sqrt{2}] \Longrightarrow L_p[1/2, 1+\sqrt{2}]$.

- Kuperberg + Bisson: $L_p[1/2, 1/\sqrt{2}]$.

# CSIDH: Security Estimates

| | Classical $\log \sqrt[4]{p}$ | Regev $\log L_N[1/2, \sqrt{2}]$ | Kuperberg $3\sqrt{\log N}$ | Kuperberg $1.8\sqrt{\log N}$ | Regev $\log L_p[1/2, 3/\sqrt{2}]$ | Kuperberg $\log L_p[1/2, 1/\sqrt{2}]$ |
|---|---|---|---|---|---|---|
| CSIDH-512 | 128 | 62 | 48 | 29 | 139 | 47 |
| CSIDH-1024 | 256 | 94 | 68 | 41 | 209 | 70 |
| CSIDH-1792 | 448 | 129 | 90 | 54 | 288 | 96 |

# CSIDH: Instantiations

| | **Clock cycles** | **Wall-clock time** | **Stack Memory** |
|---|---|---|---|
| Key validation | $5.5 \cdot 10^6$ cc | 2.1 ms | 4368 bytes |
| Group action | $106 \cdot 10^6$ cc | 40.8 ms | 2464 bytes |

Table: Performance number for the described proof-of-concept implementation, averaged over 10000 runs on an Intel Skylake i5 processor clocked at 3.5 GHz.