

ORIENTING SUPERSINGULAR ISOGENY GRAPHS

LEONARDO COLÒ & DAVID KOHEL

Institut de Mathématiques de Marseille

Number-Theoretic Methods in Cryptology 2019
Sorbonne Université, Institut de Mathématiques de Jussieu
Paris, 26 June 2019

ISOGENY GRAPHS

Definition

Given an elliptic curve E over k , and a finite set of primes S , we can associate an isogeny graph $\Gamma = (E, S)$

- ▶ whose vertices are elliptic curves isogenous to E over \bar{k} , and
- ▶ whose edges are isogenies of degree $\ell \in S$.

The vertices are defined up to \bar{k} -isomorphism (therefore represented by j -invariants), and the edges from a given vertex are defined up to a \bar{k} -isomorphism of the codomain.

If $S = \{\ell\}$, then we call Γ an ℓ -isogeny graph.

For an elliptic curve E/k and prime $\ell \neq \text{char}(k)$, the full ℓ -torsion subgroup is a 2-dimensional \mathbb{F}_ℓ -vector space. Consequently, the set of cyclic subgroups is in bijection with $\mathbb{P}^1(\mathbb{F}_\ell)$, which in turn are in bijection with the set of ℓ -isogenies from E .

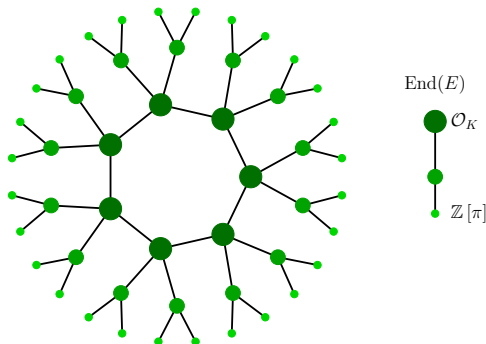
Thus the ℓ -isogeny graph of E is $(\ell + 1)$ -regular (as a directed multigraph). In characteristic 0, if $\text{End}(E) = \mathbb{Z}$, then this graph is a tree.

ORDINARY ISOGENY GRAPHS: VOLCANOES

Let $\text{End}(E) = \mathcal{O} \subseteq K$. The class group $\text{Cl}(\mathcal{O})$ (finite abelian group) acts faithfully and transitively on the set of elliptic curves with endomorphism ring \mathcal{O} :

$$E \longrightarrow E/E[\mathfrak{a}] \quad E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0 \ \forall \alpha \in \mathfrak{a}\}$$

Thus, the CM isogeny graphs can be modelled by an equivalent category of fractional ideals of K .



SUPERSINGULAR ISOGENY GRAPHS

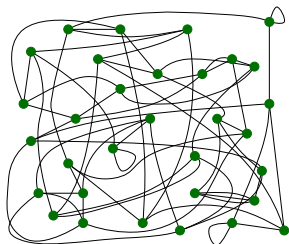
The supersingular isogeny graphs are remarkable because the vertex sets are finite : there are $[p/12] + \epsilon_p$ curves. Moreover

- ▶ every supersingular elliptic curve can be defined over \mathbb{F}_{p^2} ;
- ▶ all ℓ -isogenies are defined over \mathbb{F}_{p^2} ;
- ▶ every endomorphism of E is defined over \mathbb{F}_{p^2} .

The lack of a commutative group acting on the set of supersingular elliptic curves/ \mathbb{F}_{p^2} makes the isogeny graph more complicated.

For this reason, supersingular isogeny graphs have been proposed for

- ▶ cryptographic hash functions (Goren–Lauter),
- ▶ post-quantum SIDH key exchange protocol.



MOTIVATING OSIDH

A new key exchange protocol, CSIDH, analogous to SIDH, uses only \mathbb{F}_p -rational elliptic curves (up to \mathbb{F}_p -isomorphism), and \mathbb{F}_p -rational isogenies.

The constraint to \mathbb{F}_p -rational isogenies can be interpreted as an orientation of the supersingular graph by the subring $\mathbb{Z}[\pi]$ of $\mathbf{End}(E)$ generated by the Frobenius endomorphism π .

We introduce a general notion of orienting supersingular elliptic curves.

Motivation

- ▶ Generalize CSIDH.
- ▶ Key space of SIDH: in order to have the two key spaces of similar size, we need to take $\ell_A^{e_A} \approx \ell_B^{e_B} \approx \sqrt{p}$. This implies that the space of choices for the secret key is limited to a fraction of the whole set of supersingular j -invariants over \mathbb{F}_{p^2} .
- ▶ A feature shared by SIDH and CSIDH is that the isogenies are constructed as quotients of rational torsion subgroups. The need for rational points limits the choice of the prime p

ORIENTATIONS

Let \mathcal{O} be an order in an imaginary quadratic field. An \mathcal{O} -orientation on a supersingular elliptic curve E is an inclusion $\iota : \mathcal{O} \hookrightarrow \mathbf{End}(E)$, and a K -orientation is an inclusion $\iota : K \hookrightarrow \mathbf{End}^0(E) = \mathbf{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. An \mathcal{O} -orientation is *primitive* if $\mathcal{O} \simeq \mathbf{End}(E) \cap \iota(K)$.

Theorem

The category of K -oriented supersingular elliptic curves (E, ι) , whose morphisms are isogenies commuting with the K -orientations, is equivalent to the category of elliptic curves with CM by K .

Let $\phi : E \rightarrow F$ be an isogeny of degree ℓ . A K -orientation $\iota : K \hookrightarrow \mathbf{End}^0(E)$ determines a K -orientation $\phi_*(\iota) : K \hookrightarrow \mathbf{End}^0(F)$ on F , defined by

$$\phi_*(\iota)(\alpha) = \frac{1}{\ell} \phi \circ \iota(\alpha) \circ \hat{\phi}.$$

CLASS GROUP ACTION

- ▶ $\mathbf{SS}(p) = \{\text{supersingular elliptic curves over } \overline{\mathbb{F}}_p \text{ up to isomorphism}\}.$
- ▶ $\mathbf{SS}_{\mathcal{O}}(p) = \{\mathcal{O}\text{-oriented s.s. elliptic curves over } \overline{\mathbb{F}}_p \text{ up to } K\text{-isomorphism}\}.$
- ▶ $\mathbf{SS}_{\mathcal{O}}^{pr}(p) = \text{subset of primitive } \mathcal{O}\text{-oriented curves}.$

The set $\mathbf{SS}_{\mathcal{O}}(p)$ admits a transitive group action:

$$\mathcal{C}l(\mathcal{O}) \times \mathbf{SS}_{\mathcal{O}}(p) \longrightarrow \mathbf{SS}_{\mathcal{O}}(p) \quad ([\mathbf{a}], E) \longmapsto [\mathbf{a}] \cdot E = E/E[\mathbf{a}]$$

Proposition

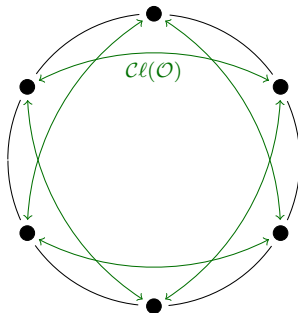
The class group $\mathcal{C}l(\mathcal{O})$ acts faithfully and transitively on the set of \mathcal{O} -isomorphism classes of primitive \mathcal{O} -oriented elliptic curves.

In particular, for fixed primitive \mathcal{O} -oriented E , we obtain a bijection of sets:

$$\mathcal{C}l(\mathcal{O}) \longrightarrow \mathbf{SS}_{\mathcal{O}}^{pr}(p) \quad [\mathbf{a}] \longmapsto [\mathbf{a}] \cdot E$$

VORTEX

We define a vortex to be the ℓ -isogeny subgraph whose vertices are isomorphism classes of \mathcal{O} -oriented elliptic curves with ℓ -maximal endomorphism ring, equipped with an action of $\mathcal{C}\ell(\mathcal{O})$.

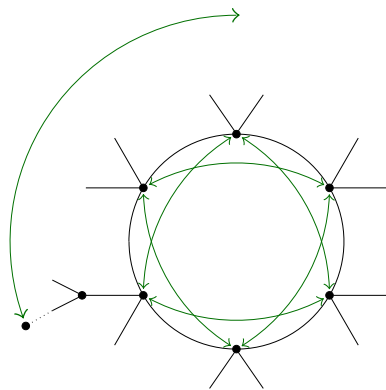


Instead of considering the union of different isogeny graphs, we focus on one single crater and we think of all the other primes as acting on it: the resulting object is a single isogeny circle rotating under the action of $\mathcal{C}\ell(\mathcal{O})$.

WHIRLPOOL

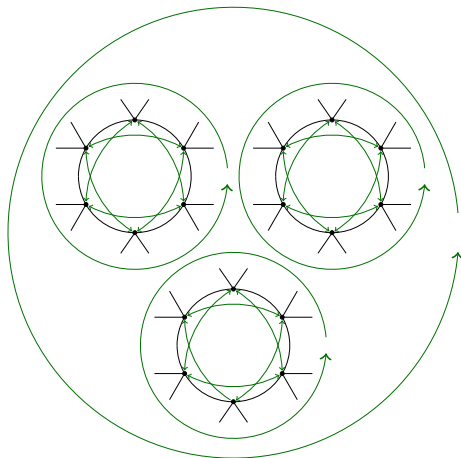
The action of $\mathcal{C}l(\mathcal{O})$ extends to the union $\bigcup_i SS_{\mathcal{O}_i}(p)$ over all superorders \mathcal{O}_i containing \mathcal{O} via the surjections $\mathcal{C}l(\mathcal{O}) \rightarrow \mathcal{C}l(\mathcal{O}_i)$.

We define a *whirlpool* to be a complete isogeny volcano acted on by the class group. We would like to think at isogeny graphs as moving objects.



WHIRLPOOL

Actually, we would like to take the ℓ -isogeny graph on the full $\mathcal{Cl}(\mathcal{O}_K)$ -orbit. This might be composed of several ℓ -isogeny orbits (craters), although the class group is transitive.



ISOGENY CHAINS

Definition

An ℓ -isogeny chain of length n from E_0 to E is a sequence of isogenies of degree ℓ :

$$E_0 \xrightarrow{\phi_0} E_1 \xrightarrow{\phi_1} E_2 \xrightarrow{\phi_2} \dots \xrightarrow{\phi_{n-1}} E_n = E.$$

The ℓ -isogeny chain is without backtracking if $\ker(\phi_{i+1} \circ \phi_i) \neq E_i[\ell]$, $\forall i$.
The isogeny chain is descending (or ascending, or horizontal) if each ϕ_i is descending (or ascending, or horizontal, respectively).

Suppose that (E_i, ϕ_i) is a descending ℓ -isogeny chain with

$$\mathcal{O}_K \subseteq \mathbf{End}(E_0), \dots, \mathcal{O}_n = \mathbb{Z} + \ell^n \mathcal{O}_K \subseteq \mathbf{End}(E_n)$$

If \mathfrak{q} is a split prime in \mathcal{O}_K over $q \neq \ell, p$, and then the isogeny $\psi_0 : E_0 \rightarrow F_0 = E_0/E_0[\mathfrak{q}]$, can be extended to the ℓ -isogeny chain by pushing forward the cyclic group $C_0 = E_0[\mathfrak{q}]$:

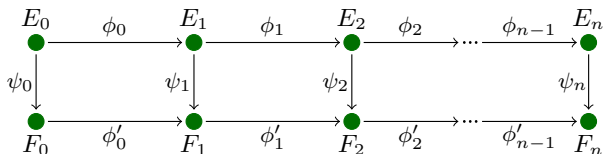
$$C_0 = E_0[\mathfrak{q}], C_1 = \phi_0(C_0), \dots, C_n = \phi_{n-1}(C_{n-1})$$

and defining $F_i = E_i/C_i$.

LADDERS

Definition

An ℓ -ladder of length n and degree q is a commutative diagram of ℓ -isogeny chains (E_i, ϕ_i) , (F_i, ϕ'_i) of length n connected by q -isogenies $\psi_i : E_i \rightarrow F_i$



We also refer to an ℓ -ladder of degree q as a q -isogeny of ℓ -isogeny chains.

We say that an ℓ -ladder is ascending (or descending, or horizontal) if the ℓ -isogeny chain (E_i, ϕ_i) is ascending (or descending, or horizontal, respectively).

We say that the ℓ -ladder is level if ψ_0 is a horizontal q -isogeny. If the ℓ -ladder is descending (or ascending), then we refer to the length of the ladder as its depth (or, respectively, as its height).

EFFECTIVE ENDOMORPHISM RINGS AND ISOGENIES

We say that a subring of $\text{End}(E)$ is effective if we have explicit polynomials or rational functions which represent its generators.

Examples. \mathbb{Z} in $\text{End}(E)$ is effective. Effective imaginary quadratic subrings $\mathcal{O} \subset \text{End}(E)$, are the subrings $\mathcal{O} = \mathbb{Z}[\pi]$ generated by Frobenius

In the Couveignes-Rostovtsev-Stolbunov constructions, or in the CSIDH protocol, one works with $\mathcal{O} = \mathbb{Z}[\pi]$.

- ▶ For large finite fields, the class group of \mathcal{O} is large and the primes \mathfrak{q} in \mathcal{O} have no small generators.

Factoring the division polynomial $\psi_q(x)$ to find the kernel polynomial of degree $(q-1)/2$ for $E[\mathfrak{q}]$ becomes relatively expensive.

- ▶ In SIDH, the ordinary protocol of De Feo, Smith, and Kieffer, or CSIDH, the curves are chosen such that the points of $E[\mathfrak{q}]$ are defined over a small degree extension κ/k , and working with rational points in $E(\kappa)$.
- ▶ We propose the use of an effective CM order \mathcal{O}_K of class number 1. The kernel polynomial can be computed directly without need for a splitting field for $E[\mathfrak{q}]$, and the computation of a generator isogeny is a one-time precomputation.

MODULAR APPROACH

The use of modular curves for efficient computation of isogenies has an established history (see Elkies)

Modular Curve

The modular curve $\mathbf{X}(1) \simeq \mathbb{P}^1$ classifies elliptic curves up to isomorphism, and the function j generates its function field.

The modular polynomial $\Phi_m(X, Y)$ defines a correspondence in $\mathbf{X}(1) \times \mathbf{X}(1)$ such that $\Phi_m(j(E), j(E')) = 0$ if and only if there exists a cyclic m -isogeny ϕ from E to E' , possibly over some extension field.

Definition

A *modular ℓ -isogeny chain* of length n over k is a finite sequence (j_0, j_1, \dots, j_n) in k such that $\Phi_\ell(j_i, j_{i+1}) = 0$ for $0 \leq i < n$.

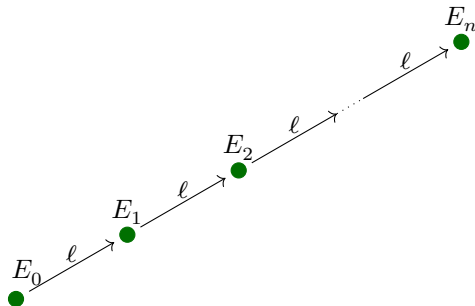
A *modular ℓ -ladder* of length n and degree q over k is a pair of modular ℓ -isogeny chains

$$(j_0, j_1, \dots, j_n) \text{ and } (j'_0, j'_1, \dots, j'_n),$$

such that $\Phi_q(j_i, j'_i) = 0$.

OSIDH - INTRODUCTION

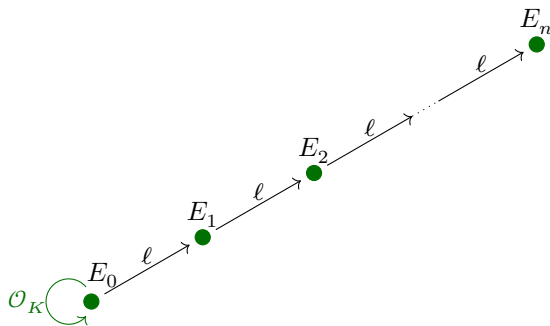
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ -isogenies.



OSIDH - INTRODUCTION

We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ -isogenies.

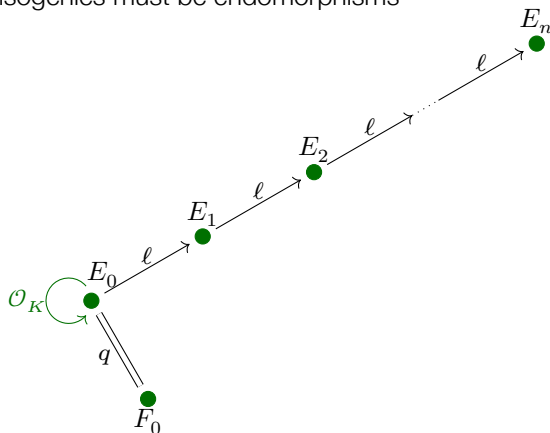
- For $\ell = 2$ (or 3) a suitable candidate for \mathcal{O}_K could be the Gaussian integers $\mathbb{Z}[i]$ or the Eisenstein integers $\mathbb{Z}[\omega]$.



OSIDH - INTRODUCTION

We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ -isogenies.

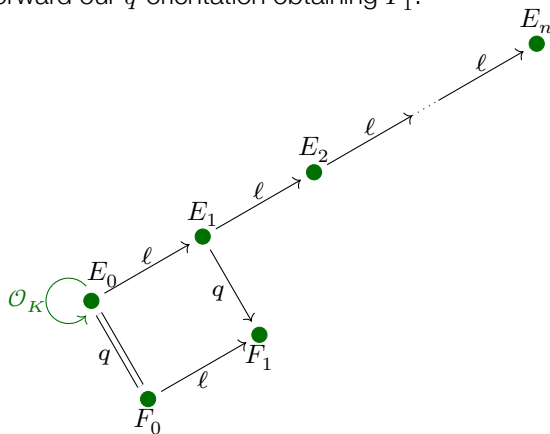
- Horizontal isogenies must be endomorphisms



OSIDH - INTRODUCTION

We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ -isogenies.

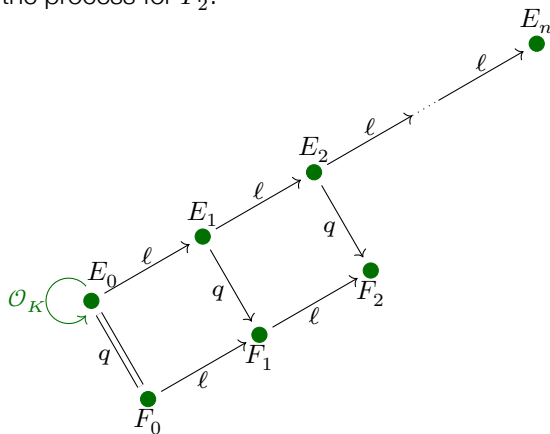
- We push forward our q -orientation obtaining F_1 .



OSIDH - INTRODUCTION

We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ -isogenies.

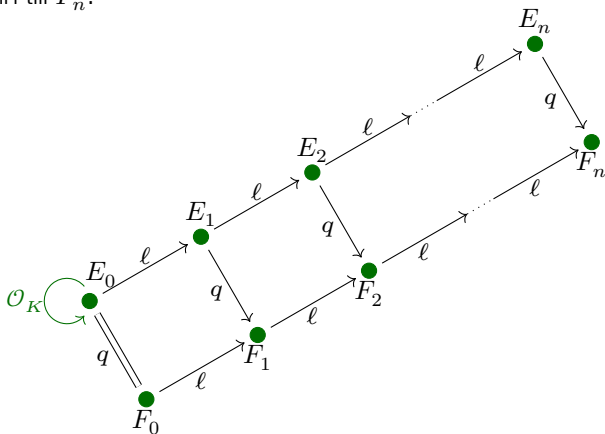
- We repeat the process for F_2 .



OSIDH - INTRODUCTION

We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ -isogenies.

- And again till F_n .



HOW FAR SHOULD WE GO?

In order to have the action of $\mathcal{C}\ell(\mathcal{O})$ cover a large portion of the supersingular elliptic curves, we require $\ell^n \sim p$, i.e., $n \sim \log_\ell(p)$.

- ▶ $\#SS_{\mathcal{O}}^{pr}(p) = h(\mathcal{O}_n) = \text{class number of } \mathcal{O}_n = \mathbb{Z} + \ell^n \mathcal{O}_K$.
- ▶ Class Number Formula

$$h(\mathbb{Z} + m\mathcal{O}_K) = \frac{h(\mathcal{O}_K)m}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{p|m} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right)$$

- ▶ Units

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1\} & \text{if } \Delta_K < -4 \\ \{\pm 1, \pm i\} & \text{if } \Delta_K = -4 \\ \{\pm 1, \pm \omega, \pm \omega^2\} & \text{if } \Delta_K = -3 \end{cases} \Rightarrow [\mathcal{O}_K^\times : \mathcal{O}^\times] = \begin{cases} 1 & \text{if } \Delta_K < -4 \\ 2 & \text{if } \Delta_K = -4 \\ 3 & \text{if } \Delta_K = -3 \end{cases}$$

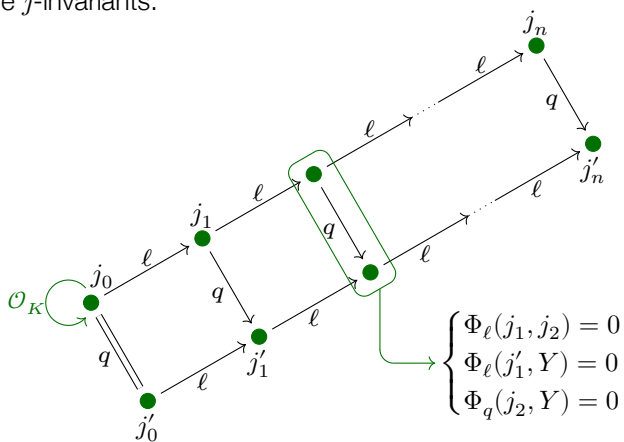
- ▶ Number of Supersingular curves

$$\#\text{SS}(p) = \left[\frac{p}{12}\right] + \epsilon_p \quad \epsilon_p \in \{0, 1, 2\}$$

$$\text{Therefore, } h(\ell^n \mathcal{O}_K) = \frac{1 \cdot \ell^n}{2 \text{ or } 3} \left(1 - \left(\frac{\Delta_K}{\ell}\right) \frac{1}{\ell}\right) = \left[\frac{p}{12}\right] + \epsilon_p \implies p \sim \ell^n$$

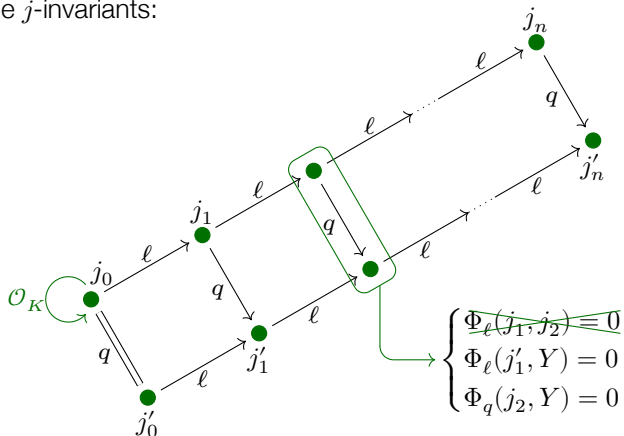
OSIDH - INTRODUCTION & MODULAR APPROACH

If we look at modular polynomials $\Phi_\ell(X, Y)$ and $\Phi_q(X, Y)$ we realize that all we need are the j -invariants:



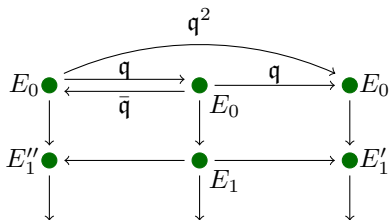
OSIDH - INTRODUCTION & MODULAR APPROACH

If we look at modular polynomials $\Phi_\ell(X, Y)$ and $\Phi_q(X, Y)$ we realize that all we need are the j -invariants:



Since j_2 is given (the initial chain is known) and supposing that j'_1 has already been constructed, j'_2 is determined by a system of two equations

HOW MANY STEPS BEFORE THE IDEALS ACT DIFFERENTLY?



$E'_i \neq E''_i$ if and only if $\mathfrak{q}^2 \cap \mathcal{O}_i$ is not principal and the probability that a random ideal in \mathcal{O}_i is principal is $1/h(\mathcal{O}_i)$. In fact, we can do better; we write $\mathcal{O}_K = \mathbb{Z}[\omega]$ and we observe that if \mathfrak{q}^2 was principal, then

$$\mathfrak{q}^2 = \mathbf{N}(\mathfrak{q}^2) = \mathbf{N}(a + b\ell^i\omega)$$

since it would be generated by an element of $\mathcal{O}_i = \mathbb{Z} + \ell^i\mathcal{O}_K$. Now

$$\mathbf{N}(a + b\ell^i) = a^2 \pm abt\ell^i + b^2s\ell^{2i} \quad \text{where} \quad \omega^2 + t\omega + s = 0$$

Thus, as soon as $\ell^{2i} \gg \mathfrak{q}^2$, we are guaranteed that \mathfrak{q}^2 is not principal.

A FIRST NAIVE PROTOCOL

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$

ALICE

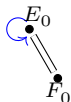
BOB

A FIRST NAIVE PROTOCOL

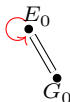
PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$

Choose a primitive
 \mathcal{O}_K -orientation of
 E_0

ALICE



BOB



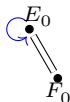
A FIRST NAIVE PROTOCOL

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$

Choose a primitive
 \mathcal{O}_K -orientation of
 E_0

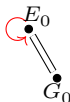
Push it forward to
depth n

ALICE



$$\underbrace{E_0 = F_0 \rightarrow F_1 \rightarrow \dots \rightarrow F_n}_{\phi_A}$$

BOB



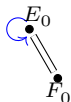
$$\underbrace{E_0 = G_0 \rightarrow G_1 \rightarrow \dots \rightarrow G_n}_{\phi_B}$$

A FIRST NAIVE PROTOCOL

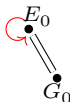
PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$

Choose a primitive
 \mathcal{O}_K -orientation of
 E_0

ALICE



BOB



Push it forward to
depth n

$$\underbrace{E_0 = F_0 \rightarrow F_1 \rightarrow \dots \rightarrow F_n}_{\phi_A}$$

$$\underbrace{E_0 = G_0 \rightarrow G_1 \rightarrow \dots \rightarrow G_n}_{\phi_B}$$

Exchange data

$$\{G_i\}_{i=1}^n$$

$$\{F_i\}_{i=1}^n$$

A FIRST NAIVE PROTOCOL

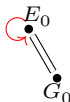
PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$

Choose a primitive
 \mathcal{O}_K -orientation of
 E_0

ALICE



BOB



Push it forward to
depth n

$$\underbrace{E_0 = F_0 \rightarrow F_1 \rightarrow \dots \rightarrow F_n}_{\phi_A}$$

$$\underbrace{E_0 = G_0 \rightarrow G_1 \rightarrow \dots \rightarrow G_n}_{\phi_B}$$

Exchange data

$$\{G_i\}_{i=1}^n$$

$$\{F_i\}_{i=1}^n$$

Compute shared
secret

$$\text{Compute } \phi_A \cdot \{G_i\}$$

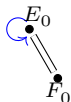
$$\text{Compute } \phi_B \cdot \{F_i\}$$

A FIRST NAIVE PROTOCOL

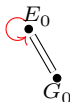
PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$

Choose a primitive
 \mathcal{O}_K -orientation of
 E_0

ALICE



BOB



Push it forward to
depth n

$$\underbrace{E_0 = F_0 \rightarrow F_1 \rightarrow \dots \rightarrow F_n}_{\phi_A}$$

$$\underbrace{E_0 = G_0 \rightarrow G_1 \rightarrow \dots \rightarrow G_n}_{\phi_B}$$

Exchange data

$$\{G_i\}_{i=1}^n$$

$$\{F_i\}_{i=1}^n$$

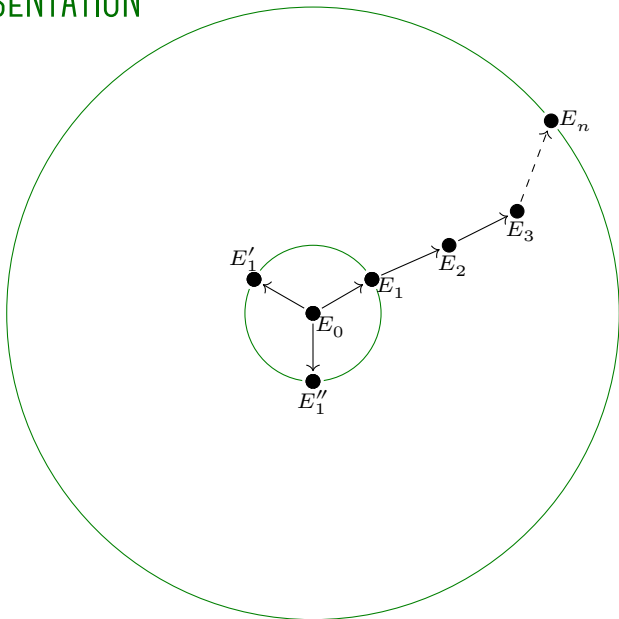
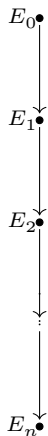
Compute shared
secret

$$\text{Compute } \phi_A \cdot \{G_i\}$$

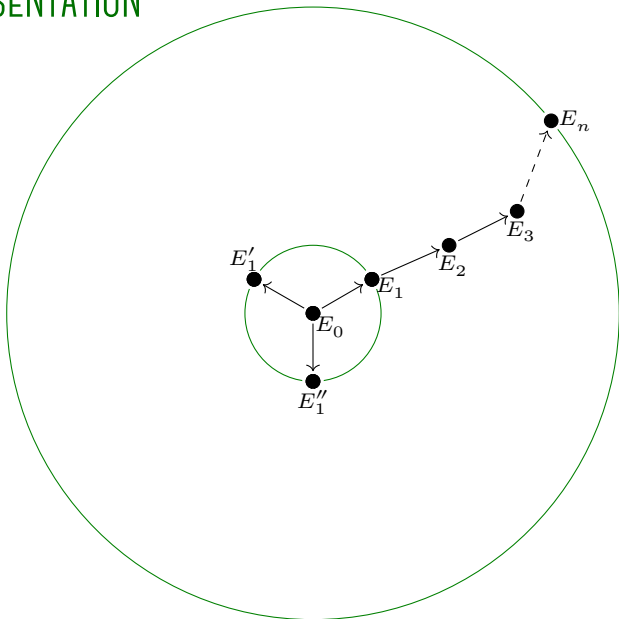
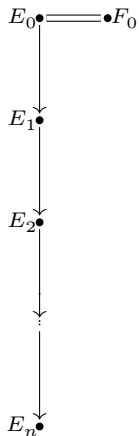
$$\text{Compute } \phi_B \cdot \{F_i\}$$

In the end, Alice and Bob will share a new chain $E_0 \rightarrow H_1 \rightarrow \dots \rightarrow H_n$

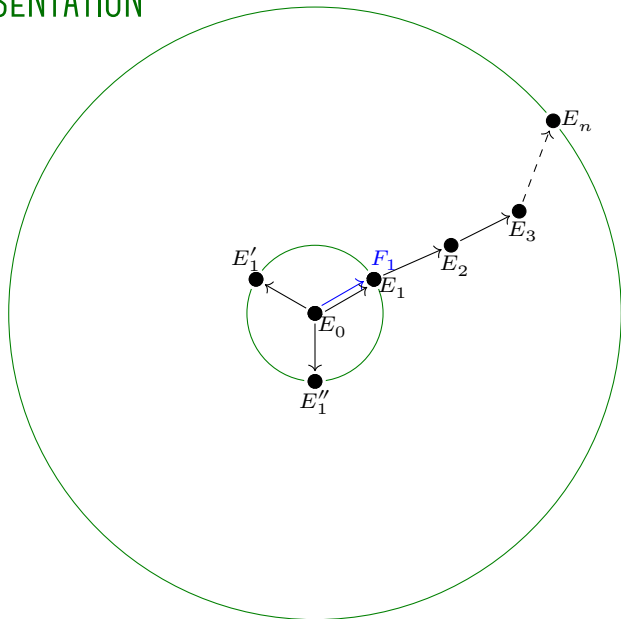
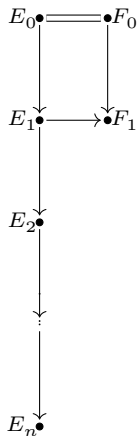
GRAPHIC REPRESENTATION



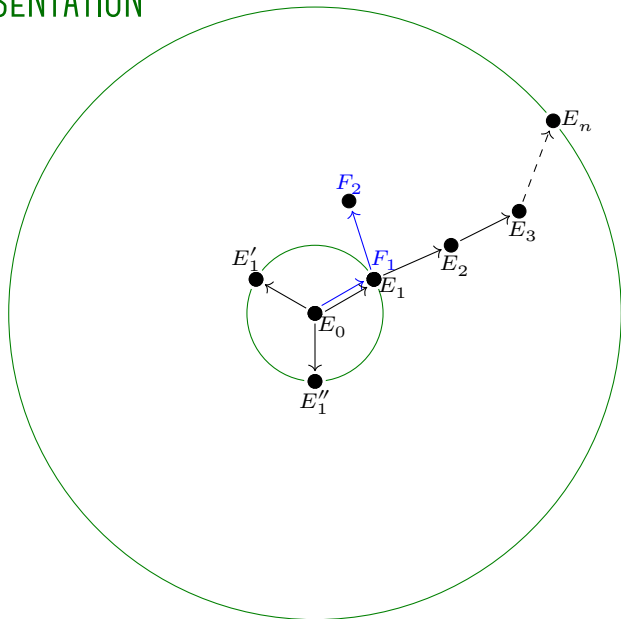
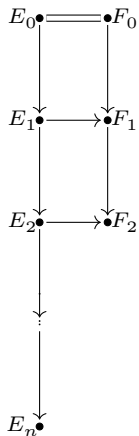
GRAPHIC REPRESENTATION



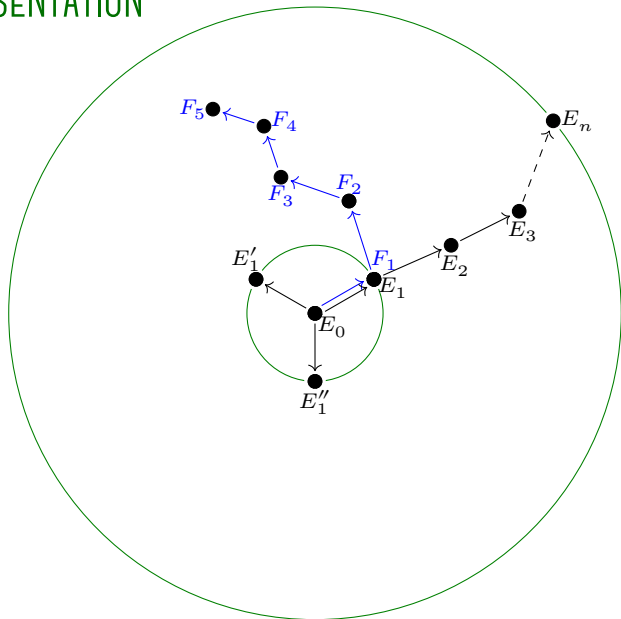
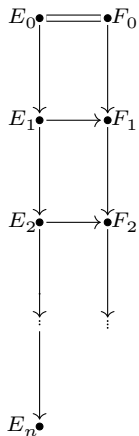
GRAPHIC REPRESENTATION



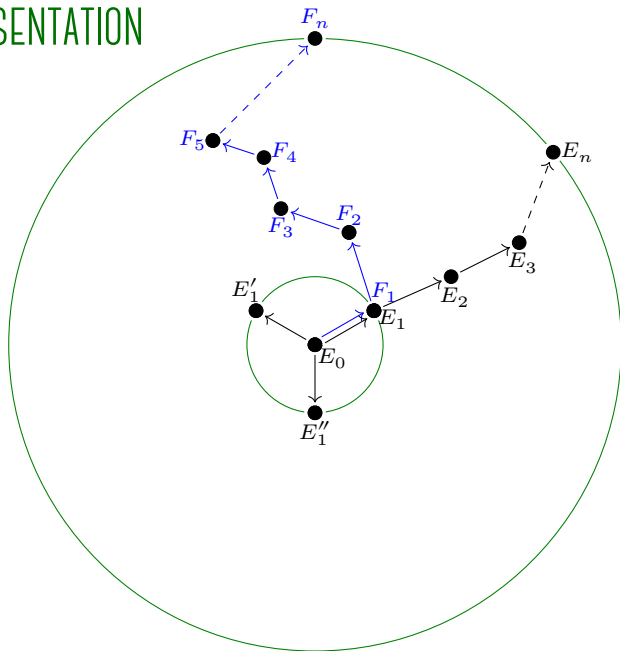
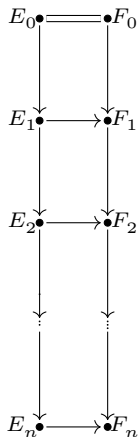
GRAPHIC REPRESENTATION



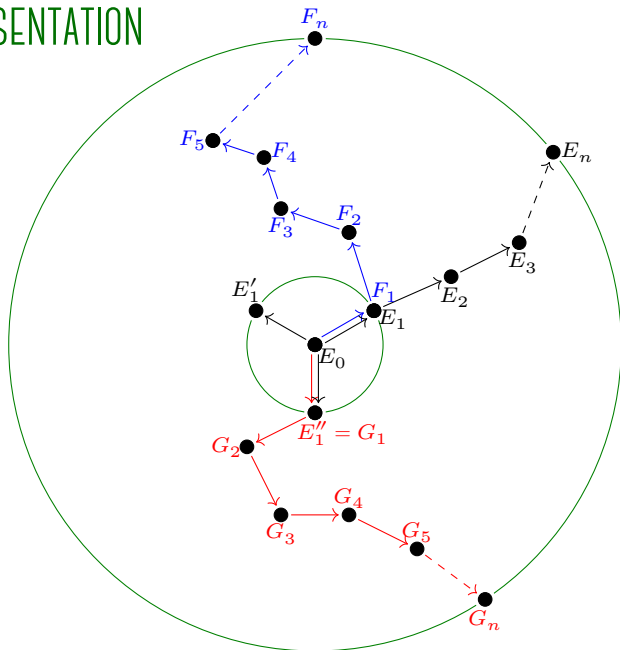
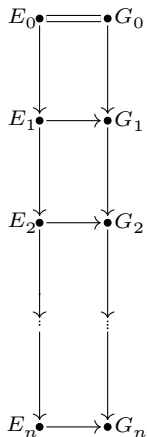
GRAPHIC REPRESENTATION



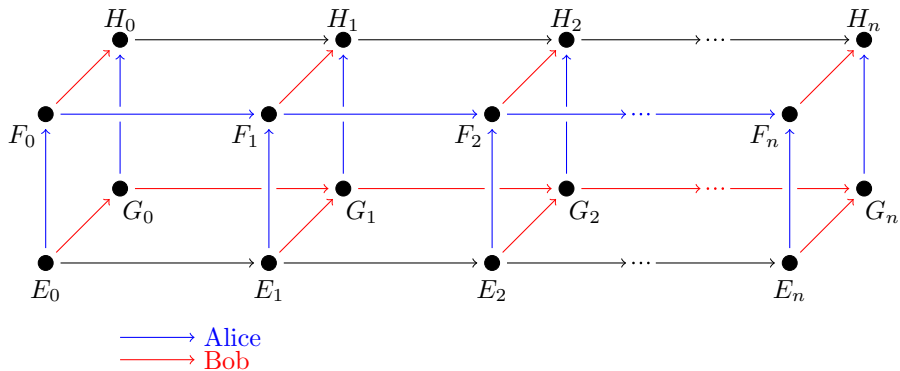
GRAPHIC REPRESENTATION



GRAPHIC REPRESENTATION



GRAPHIC REPRESENTATION



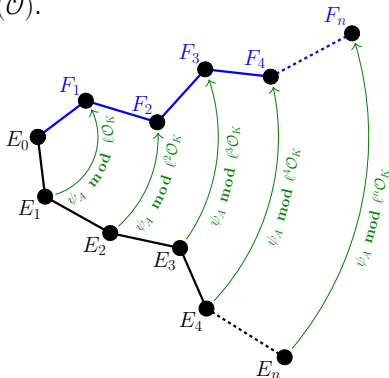
A FIRST NAIVE PROTOCOL - WEAKNESS

In reality, sharing (F_i) and (G_i) reveals too much of the private data.

From the short exact sequence of class groups:

$$1 \rightarrow \frac{(\mathcal{O}_K/\ell^n \mathcal{O}_K)^\times}{\mathcal{O}_K^\times (\mathbb{Z}/\ell^n \mathbb{Z})^\times} \rightarrow \mathcal{Cl}(\mathcal{O}) \rightarrow \mathcal{Cl}(\mathcal{O}_K) \rightarrow 1$$

an adversary can compute successive approximations (mod ℓ^i) to ϕ_A and ϕ_B modulo ℓ^n hence in $\mathcal{Cl}(\mathcal{O})$.



OSIDH PROTOCOL

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O}_n \subseteq \text{End}(E_n) \cap K \subseteq \mathcal{O}_K$

ALICE

BOB

OSIDH PROTOCOL

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O}_n \subseteq \text{End}(E_n) \cap K \subseteq \mathcal{O}_K$

ALICE

Choose integers
in a bound $[-r, r]$

(e_1, \dots, e_t)

BOB

(d_1, \dots, d_t)

OSIDH PROTOCOL

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O}_n \subseteq \text{End}(E_n) \cap K \subseteq \mathcal{O}_K$

ALICE

Choose integers
in a bound $[-r, r]$
Construct an
isogenous curve

$$(e_1, \dots, e_t)$$

$$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}]$$

BOB

$$(d_1, \dots, d_t)$$

$$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \dots \mathfrak{p}_t^{d_t}]$$

OSIDH PROTOCOL

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O}_n \subseteq \text{End}(E_n) \cap K \subseteq \mathcal{O}_K$

ALICE

Choose integers
in a bound $[-r, r]$
Construct an
isogenous curve
Precompute all
directions $\forall i$

$$(e_1, \dots, e_t)$$

$$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}]$$

$$F_{n,i}^{(-r)} \leftarrow F_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow F_{n,i}^{(1)} \leftarrow F_n$$

BOB

$$(d_1, \dots, d_t)$$

$$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \dots \mathfrak{p}_t^{d_t}]$$

$$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$$

OSIDH PROTOCOL

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O}_n \subseteq \text{End}(E_n) \cap K \subseteq \mathcal{O}_K$

Choose integers
in a bound $[-r, r]$
Construct an
isogenous curve
Precompute all
directions $\forall i$
... and their
conjugates

ALICE

$$(e_1, \dots, e_t)$$

$$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}]$$

$$F_{n,i}^{(-r)} \leftarrow F_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow F_{n,i}^{(1)} \leftarrow F_n$$

$$F_n \rightarrow F_{n,i}^{(1)} \rightarrow \dots \rightarrow F_{n,i}^{(r-1)} \rightarrow F_{n,i}^{(r)}$$

BOB

$$(d_1, \dots, d_t)$$

$$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \dots \mathfrak{p}_t^{d_t}]$$

$$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$$

$$G_n \rightarrow G_{n,i}^{(1)} \rightarrow \dots \rightarrow G_{n,i}^{(r-1)} \rightarrow G_{n,i}^{(r)}$$

OSIDH PROTOCOL

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O}_n \subseteq \text{End}(E_n) \cap K \subseteq \mathcal{O}_K$

Choose integers
in a bound $[-r, r]$
Construct an
isogenous curve
Precompute all
directions $\forall i$
... and their
conjugates
Exchange data

ALICE

$$(e_1, \dots, e_t)$$

$$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}]$$

$$F_{n,i}^{(-r)} \leftarrow F_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow F_{n,i}^{(1)} \leftarrow F_n$$

$$F_n \rightarrow F_{n,i}^{(1)} \rightarrow \dots \rightarrow F_{n,i}^{(r-1)} \rightarrow F_{n,i}^{(r)}$$

BOB

$$(d_1, \dots, d_t)$$

$$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \dots \mathfrak{p}_t^{d_t}]$$

$$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$$

$$G_n \rightarrow G_{n,i}^{(1)} \rightarrow \dots \rightarrow G_{n,i}^{(r-1)} \rightarrow G_{n,i}^{(r)}$$

G_n + directions

F_n + directions

OSIDH PROTOCOL

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O}_n \subseteq \text{End}(E_n) \cap K \subseteq \mathcal{O}_K$

Choose integers
in a bound $[-r, r]$

Construct an
isogenous curve

Precompute all
directions $\forall i$

... and their
conjugates

Exchange data

Compute shared
data

ALICE

$$(e_1, \dots, e_t)$$

$$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}]$$

$$F_{n,i}^{(-r)} \leftarrow F_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow F_{n,i}^{(1)} \leftarrow F_n$$

$$F_n \rightarrow F_{n,i}^{(1)} \rightarrow \dots \rightarrow F_{n,i}^{(r-1)} \rightarrow F_{n,i}^{(r)}$$

BOB

$$(d_1, \dots, d_t)$$

$$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \dots \mathfrak{p}_t^{d_t}]$$

$$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$$

$$G_n \rightarrow G_{n,i}^{(1)} \rightarrow \dots \rightarrow G_{n,i}^{(r-1)} \rightarrow G_{n,i}^{(r)}$$

G_n + directions

Takes e_i steps in

\mathfrak{p}_i -isogeny chain & push
forward information for

$$j > i.$$

F_n + directions

Takes d_i steps in

\mathfrak{p}_i -isogeny chain & push
forward information for

$$j > i.$$

OSIDH PROTOCOL

PUBLIC DATA: A chain of ℓ -isogenies $E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n$ and a set of splitting primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t \subseteq \mathcal{O}_n \subseteq \text{End}(E_n) \cap K \subseteq \mathcal{O}_K$

	ALICE	BOB
Choose integers in a bound $[-r, r]$	(e_1, \dots, e_t)	(d_1, \dots, d_t)
Construct an isogenous curve	$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}]$	$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \dots \mathfrak{p}_t^{d_t}]$
Precompute all directions $\forall i$	$F_{n,i}^{(-r)} \leftarrow F_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow F_{n,i}^{(1)} \leftarrow F_n$	$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$
... and their conjugates	$F_n \rightarrow F_{n,i}^{(1)} \rightarrow \dots \rightarrow F_{n,i}^{(r-1)} \rightarrow F_{n,1}^{(r)}$	$G_n \rightarrow G_{n,i}^{(1)} \rightarrow \dots \rightarrow G_{n,i}^{(r-1)} \rightarrow G_{n,1}^{(r)}$
Exchange data	G_n + directions	F_n + directions
Compute shared data	Takes e_i steps in \mathfrak{p}_i -isogeny chain & push forward information for $j > i$.	Takes d_i steps in \mathfrak{p}_i -isogeny chain & push forward information for $j > i$.

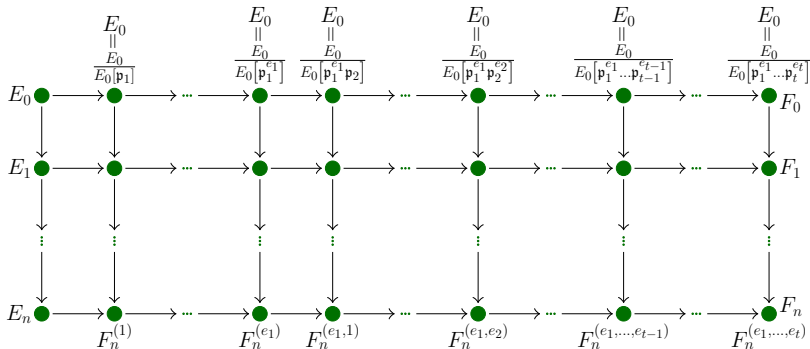
In the end, they share $H_n = E_n / E_n [\mathfrak{p}_1^{e_1+d_1} \cdot \dots \cdot \mathfrak{p}_t^{e_t+d_t}]$

OSIDH PROTOCOL - GRAPHIC REPRESENTATION I

The first step consists of choosing the secret keys; these are represented by a sequence of integers (e_1, \dots, e_t) such that $|e_i| \leq r$. The bound r is taken so that the number $(2r + 1)^t$ of curves that can be reached is sufficiently large. This choice of integers enables Alice to compute a new elliptic curve

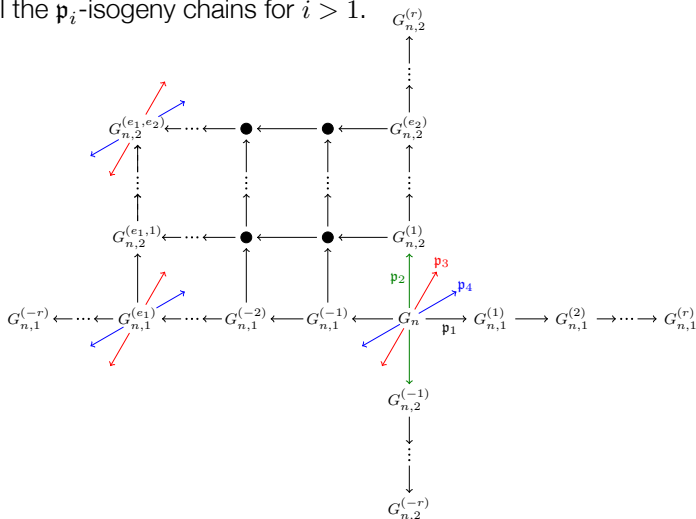
$$F_n = \frac{E_n}{E_n[\mathbf{p}_1^{e_1} \dots \mathbf{p}_t^{e_t}]}$$

by means of constructing the following commutative diagram



OSIDH PROTOCOL - GRAPHIC REPRESENTATION II

Once that Alice obtain from Bob the curve G_n together with the collection of data encoding the directions, she takes e_1 steps in the \mathfrak{p}_1 -isogeny chain and push forward all the \mathfrak{p}_i -isogeny chains for $i > 1$.



HARD PROBLEMS

Endomorphism ring problem

Given a supersingular elliptic curve E/\mathbb{F}_{p^2} and $\pi = [p]$, determine $\mathbf{End}(E)$ as an abstract ring or an explicit basis for it over \mathbb{Z} (or for $\mathbf{End}^0(E)$ over \mathbb{Q}).

Endomorphism Generators Problem

Given a supersingular elliptic curve E/\mathbb{F}_{p^2} , $\pi = [p]$, an imaginary quadratic order \mathcal{O} admitting an embedding in $\mathbf{End}(E)$ and a collection of compatible $(\mathcal{O}, \mathfrak{q}^n)$ -orientations of E for $(\mathfrak{q}, n) \in S$, determine

1. An explicit endomorphism $\phi \in \mathcal{O} \subseteq \mathbf{End}(E)$
2. A generator ϕ of $\mathcal{O} \subseteq \mathbf{End}(E)$

Suppose $S = \{(\mathfrak{q}, n)\} = \{(\mathfrak{q}_1, n_1), \dots, (\mathfrak{q}_t, n_t)\}$ where $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ are pairwise distinct primes such that

$$\begin{aligned} [0, \dots, n_1] \times \dots \times [0, \dots, n_t] &\longrightarrow \mathcal{C}\ell(\mathcal{O}) \\ (e_1, \dots, e_t) &\longrightarrow [\mathfrak{q}_1^{e_1} \cdot \dots \cdot \mathfrak{q}_t^{e_t}] \end{aligned}$$

is injective. Then, the problem should remain difficult.

SECURITY PARAMETERS - FIRST CHOICE

Consider an arbitrary supersingular endomorphism ring $\mathcal{O}_{\mathfrak{B}} \subset \mathfrak{B}$ with discriminant p^2 . There is a positive definite rank 3 quadratic form

$$\begin{array}{ccc} \text{disc} : \mathcal{O}_{\mathfrak{B}}/\mathbb{Z} & \longrightarrow & \mathbb{Z} \\ \wedge^2(\mathcal{O}_{\mathfrak{B}}) \supseteq \mathbb{Z} \wedge \mathcal{O}_{\mathfrak{B}} & \xrightarrow{\alpha} & |\text{disc}(\alpha)| = |\text{disc}(\mathbb{Z}[\alpha])| \end{array}$$

representing discriminants of orders embedding in $\mathcal{O}_{\mathfrak{B}}$.

The general order $\mathcal{O}_{\mathfrak{B}}$ has a reduced basis $1 \wedge \alpha_1, 1 \wedge \alpha_2, 1 \wedge \alpha_3$ satisfying

$$|\text{disc}(1 \wedge \alpha_i)| = \Delta_i \text{ where } \Delta_i \sim p^{2/3}$$

(Minkowski bound: $c_1 p^2 \leq \Delta_1 \Delta_2 \Delta_3 \leq c_2 p^2$).

In order to hide \mathcal{O}_n in $\mathcal{O}_{\mathfrak{B}}$ we impose

$$\ell^{2n} |\Delta_K| > c p^{2/3} \quad \Rightarrow \quad n \sim \frac{\log_{\ell}(p)}{3}$$

so that there is no special imaginary quadratic subring in $\mathcal{O}_{\mathfrak{B}} = \text{End}(E_n)$.

Future work:

- ▶ Security analysis and setting security parameters.
- ▶ Implementation and algorithmic optimization.
- ▶ Use of canonical liftings.

Future work:

- ▶ Security analysis and setting security parameters.
- ▶ Implementation and algorithmic optimization.
- ▶ Use of canonical liftings.

THANK YOU FOR YOUR ATTENTION