

MARSEILLE, 23 FEBRUARY 2023

# ORIENTED SUPERSINGULAR ELLIPTIC CURVES & CLASS GROUP ACTIONS

LEONARDO COLÒ & DAVID KOHEL

Institut de Mathématiques de Marseille

ALgebraic and combinatorial  
methods for COding and  
CRYPTography



# CONTENTS

- ▶ Orientations and class group actions.
- ▶ OSIDH protocol.
- ▶ Security considerations.

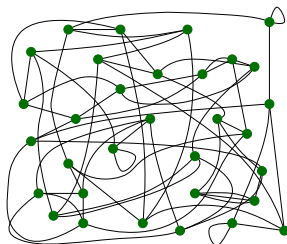
# ORIENTATIONS AND CLASS GROUP ACTIONS



The supersingular isogeny graphs are remarkable because the vertex sets are finite : there are  $(p + 1)/12 + \epsilon_p$  curves. Moreover

- ▶ every supersingular elliptic curve can be defined over  $\mathbb{F}_{p^2}$ ;
- ▶ all  $\ell$ -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.



Let  $\mathcal{O}$  be an order in an imaginary quadratic field  $K$ .

An  $\mathcal{O}$ -orientation on a supersingular elliptic curve  $E$  is an embedding

$$\iota : \mathcal{O} \hookrightarrow \text{End}(E).$$

A  $K$ -orientation is an embedding

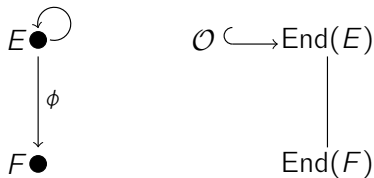
$$\iota : K \hookrightarrow \text{End}^0(E) = \text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

An  $\mathcal{O}$ -orientation is *primitive* if

$$\mathcal{O} \simeq \text{End}(E) \cap \iota(K).$$

## Theorem

The category of  $K$ -oriented supersingular elliptic curves  $(E, \iota)$ , 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  $\ell$ . A  $K$ -orientation  $\iota : K \hookrightarrow \text{End}^0(E)$  determines a  $K$ -orientation  $\phi_*(\iota) : K \hookrightarrow \text{End}^0(F)$  on  $F$ , defined by

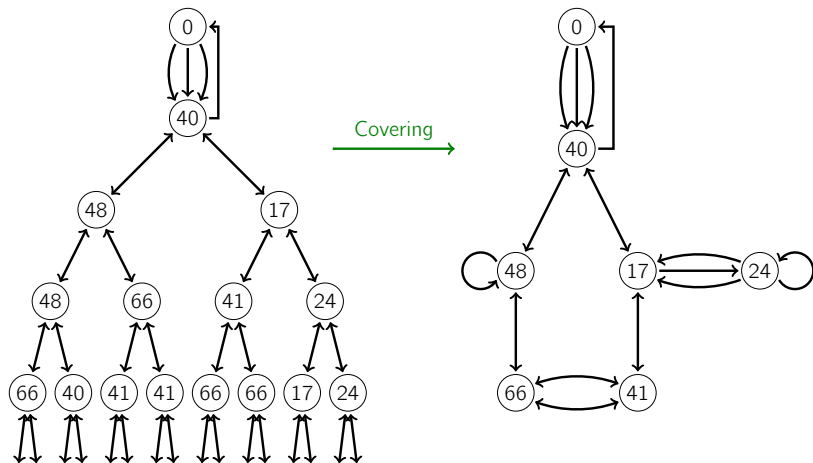
$$\phi_*(\iota)(\alpha) = \frac{1}{\ell} \phi \circ \iota(\alpha) \circ \hat{\phi}.$$

Conversely, given  $K$ -oriented elliptic curves  $(E, \iota_E)$  and  $(F, \iota_F)$  we say that an isogeny  $\phi : E \rightarrow F$  is  $K$ -oriented if  $\phi_*(\iota_E) = \iota_F$ , i.e., if the orientation on  $F$  is induced by  $\phi$ .

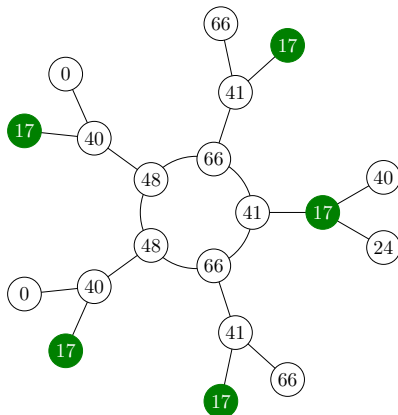
# ORIENTED ISOGENY GRAPHS - AN EXAMPLE

Let  $p = 71$  and  $E_0/\mathbb{F}_{71}$  be the supersingular elliptic curve with  $j(E) = 0$  oriented by the  $\mathcal{O}_K = \mathbb{Z}[\omega]$ , where  $\omega^2 + \omega + 1 = 0$ .

The orientation by  $K = \mathbb{Q}[\omega]$  differentiates vertices in the descending paths from  $E_0$ , determining an infinite graph shown here to depth 4:



We let again  $p = 71$  and we consider the isogeny graph oriented by  $\mathbb{Z}[\omega_{79}]$  where  $\omega_{79}$  generates the ring of integers of  $\mathbb{Q}(\sqrt{-79})$ .





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

An element of  $SS_{\mathcal{O}}^{pr}(\rho)$  consists of

- ▶ A supersingular elliptic curve  $E/\overline{\mathbb{F}}_p$ ;
- ▶ a primitive orientation  $\iota : \mathcal{O} \hookrightarrow \text{End}(E)$ ;
- ▶ a structure of a  $p$ -orientation which is a homomorphism  $\rho : \mathcal{O} \rightarrow \overline{\mathbb{F}}_p$ .

$$\rho : \mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p} \xrightarrow{\iota} \text{End}(E)/\mathfrak{P} \hookrightarrow \overline{\mathbb{F}}_p$$

- ▶  $SS_{\mathcal{O}}^{pr}(\rho) = \text{set of oriented supersingular elliptic curves with } \rho \text{ induced by } \iota.$

The set  $SS_{\mathcal{O}}(\rho)$  admits a transitive group action:

$$\begin{aligned}\mathcal{C}(\mathcal{O}) \times SS_{\mathcal{O}}(\rho) &\longrightarrow SS_{\mathcal{O}}(\rho) \\ ([\mathfrak{a}], E) &\longmapsto [\mathfrak{a}] \cdot E = E/E[\mathfrak{a}]\end{aligned}$$

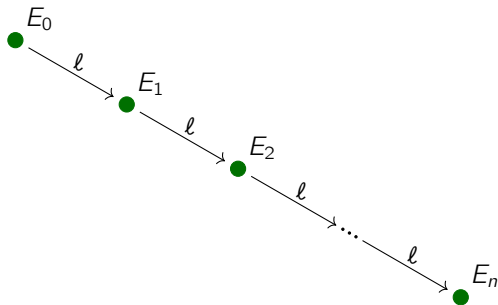
## Proposition

The set  $SS_{\mathcal{O}}^{pr}(\rho)$  is a torsor for the class group  $\mathcal{C}(\mathcal{O})$ .

For fixed primitive  $p$ -oriented supersingular curve  $E$ , we get bijection of sets:

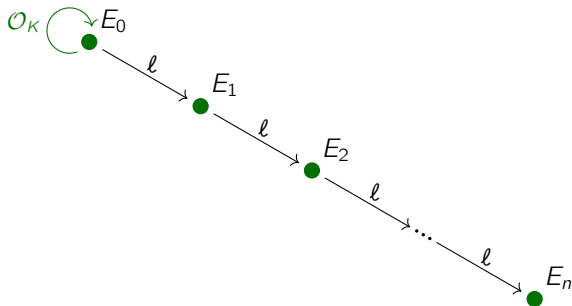
$$\mathcal{C}(\mathcal{O}) \longrightarrow SS_{\mathcal{O}}^{pr}(\rho)$$

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



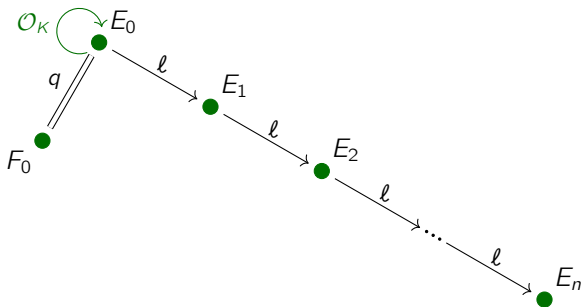
We consider an elliptic curve  $E_0$  with an effective endomorphism ring (eg.  $j_0 = 0, 1728$ ) and a chain of  $\ell$ -isogenies.

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



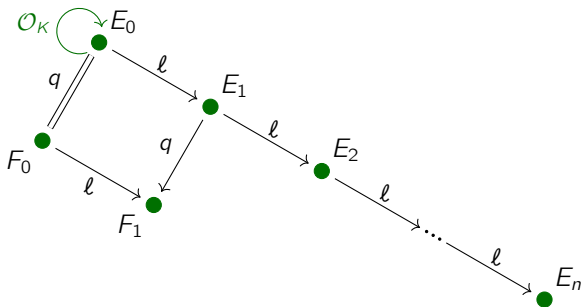
We consider an elliptic curve  $E_0$  with an effective endomorphism ring (eg.  $j_0 = 0, 1728$ ) and a chain of  $\ell$ -isogenies.

- Horizontal isogenies must be endomorphisms



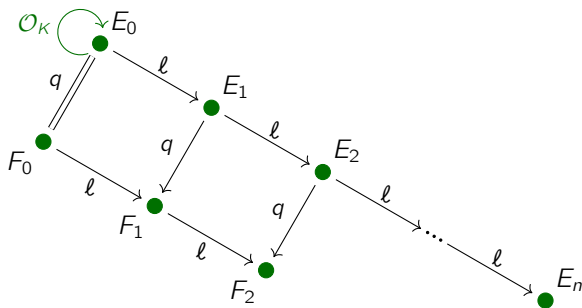
We consider an elliptic curve  $E_0$  with an effective endomorphism ring (eg.  $j_0 = 0, 1728$ ) and a chain of  $\ell$ -isogenies.

- We push forward our  $q$ -orientation obtaining  $F_1$ .



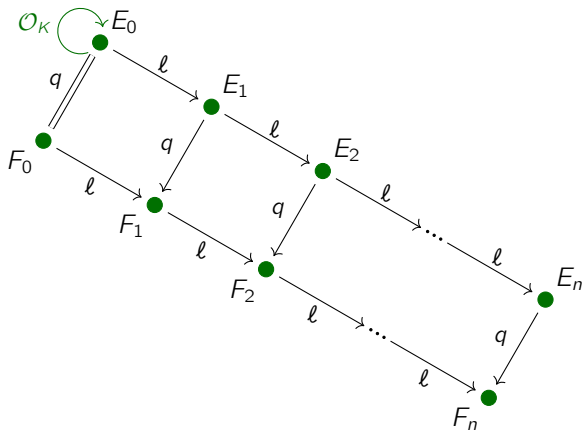
We consider an elliptic curve  $E_0$  with an effective endomorphism ring (eg.  $j_0 = 0, 1728$ ) and a chain of  $\ell$ -isogenies.

- We repeat the process for  $F_2$ .



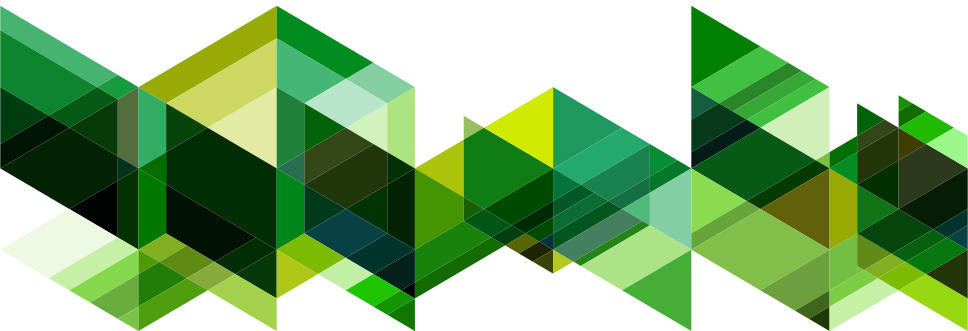
We consider an elliptic curve  $E_0$  with an effective endomorphism ring (eg.  $j_0 = 0, 1728$ ) and a chain of  $\ell$ -isogenies.

- And again till  $F_n$ .





OSIDH



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

ALICE

BOB

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

	<b>ALICE</b>	<b>BOB</b>
Choose integers in a bound $[-r, r]$	$(e_1, \dots, e_t)$	$(d_1, \dots, d_t)$

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

	ALICE	BOB
Choose integers in a bound $[-r, r]$	$(e_1, \dots, e_t)$	$(d_1, \dots, d_t)$
Construct an isogenous curve	$F_n = E_n/E_n[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}]$	$G_n = E_n/E_n[\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_t^{d_t}]$

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

	ALICE	BOB
Choose integers in a bound $[-r, r]$	$(e_1, \dots, e_t)$	$(d_1, \dots, d_t)$
Construct an isogenous curve	$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}]$	$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_t^{d_t}]$
Precompute all directions $\forall i$	$F_{n,i}^{(-r)} \leftarrow F_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow F_{n,i}^{(1)} \leftarrow F_n$	$G_{n,i}^{(-r)} \leftarrow G_{n,i}^{(-r+1)} \leftarrow \dots \leftarrow G_{n,i}^{(1)} \leftarrow G_n$

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

	ALICE	BOB
Choose integers in a bound $[-r, r]$	$(e_1, \dots, e_t)$	$(d_1, \dots, d_t)$
Construct an isogenous curve	$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}]$	$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_t^{d_t}]$
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	$F_n \rightarrow F_{n,i}^{(1)} \rightarrow \dots \rightarrow F_{n,i}^{(r-1)} \rightarrow F_{n,i}^{(r)}$	$G_n \rightarrow G_{n,i}^{(1)} \rightarrow \dots \rightarrow G_{n,i}^{(r-1)} \rightarrow G_{n,i}^{(r)}$

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

	ALICE	BOB
Choose integers in a bound $[-r, r]$	$(e_1, \dots, e_t)$	$(d_1, \dots, d_t)$
Construct an isogenous curve	$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}]$	$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_t^{d_t}]$
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	$F_n \rightarrow F_{n,i}^{(1)} \rightarrow \dots \rightarrow F_{n,i}^{(r-1)} \rightarrow F_{n,i}^{(r)}$	$G_n \rightarrow G_{n,i}^{(1)} \rightarrow \dots \rightarrow G_{n,i}^{(r-1)} \rightarrow G_{n,i}^{(r)}$
Exchange data		
	$G_n + \text{directions}$	$F_n + \text{directions}$

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

	ALICE	BOB
Choose integers in a bound $[-r, r]$	$(e_1, \dots, e_t)$	$(d_1, \dots, d_t)$
Construct an isogenous curve	$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}]$	$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_t^{d_t}]$
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	$G_n + \text{directions}$	$F_n + \text{directions}$
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 $j > i$ .



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

	ALICE	BOB
Choose integers in a bound $[-r, r]$	$(e_1, \dots, e_t)$	$(d_1, \dots, d_t)$
Construct an isogenous curve	$F_n = E_n / E_n [\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}]$	$G_n = E_n / E_n [\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_t^{d_t}]$
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	$G_n + \text{directions}$	$F_n + \text{directions}$
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  $H_n = E_n / E_n [\mathfrak{p}_1^{e_1+d_1} \cdots \mathfrak{p}_t^{e_t+d_t}]$

# SECURITY CONSIDERATIONS



For an order  $\mathcal{O}$  of conductor  $\ell^n M$ , we note that  $\mathcal{C}(\mathcal{O}) \simeq \text{SS}_{\mathcal{O}}^{\text{pr}}(\rho)$  and define

$$I = I_1 \times \dots \times I_t \subseteq \mathbb{Z}^t \quad \text{where } I_j = [-r_j, r_j].$$

The security of OSIDH depends on the following maps

$$I = \prod_{i=1}^t [-r_i, r_i] \longrightarrow \text{SS}_{\mathcal{O}}^{\text{pr}}(\rho) \longrightarrow \text{SS}(p)$$

### Supersingular covering bound

We say that the map  $\mathcal{C}(\mathcal{O}) \simeq \text{SS}_{\mathcal{O}}^{\text{pr}}(\rho) \longrightarrow \text{SS}(p)$  is  $\lambda$ -surjective if

$$p^\lambda \leq \#\mathcal{C}(\mathcal{O})$$

where  $\lambda$  is the *logarithmic covering radius*. We get

$$\lambda \log_\ell(p) \leq n + \log_\ell(M) + \log_\ell(h(\mathcal{O}_K))$$

For an order  $\mathcal{O}$  of conductor  $\ell^n M$ , we note that  $\mathcal{A}(\mathcal{O}) \simeq \text{SS}_{\mathcal{O}}^{pr}(\rho)$  and define

$$I = I_1 \times \dots \times I_t \subseteq \mathbb{Z}^t \quad \text{where } I_j = [-r_j, r_j].$$

The security of OSIDH depends on the following maps

$$I = \prod_{i=1}^t [-r_i, r_i] \longrightarrow \text{SS}_{\mathcal{O}}^{pr}(\rho) \longrightarrow \text{SS}(\rho)$$

### Supersingular injectivity bound

How can one insure the injectivity of the map  $\text{SS}_{\mathcal{O}}^{pr}(\rho) \rightarrow \text{SS}(\rho)$ ? We set

$$n + \log_{\ell}(M) + \frac{1}{2} \log_{\ell}(|\Delta_K|) \leq \frac{1}{2} \log_{\ell}(\rho)$$

If (SIB) holds, then the map  $\text{SS}_{\mathcal{O}}^{pr}(\rho) \rightarrow \text{SS}(\rho)$  is injective.

For an order  $\mathcal{O}$  of conductor  $\ell^n M$ , we note that  $\mathcal{C}(\mathcal{O}) \simeq \text{SS}_{\mathcal{O}}^{\text{pr}}(\rho)$  and define

$$I = I_1 \times \dots \times I_t \subseteq \mathbb{Z}^t \quad \text{where } I_j = [-r_j, r_j].$$

The security of OSIDH depends on the following maps

$$I = \prod_{i=1}^t [-r_i, r_i] \longrightarrow \text{SS}_{\mathcal{O}}^{\text{pr}}(\rho) \longrightarrow \text{SS}(\rho)$$

## Class group covering bound

In order to have a uniform element of  $\mathcal{C}(\mathcal{O})$  it is desirable to be able to reach all elements of  $\mathcal{C}(\mathcal{O})$ .

$$\sum_{i=1}^t \log_{\ell}(2r_i + 1) \geq \lambda(n + \log_{\ell}(M) + \log_{\ell}(h(\mathcal{O}_K)))$$

For an order  $\mathcal{O}$  of conductor  $\ell^n M$ , we note that  $\mathcal{A}(\mathcal{O}) \simeq \text{SS}_{\mathcal{O}}^{\text{pr}}(\rho)$  and define

$$I = I_1 \times \dots \times I_t \subseteq \mathbb{Z}^t \quad \text{where } I_j = [-r_j, r_j].$$

The security of OSIDH depends on the following maps

$$I = \prod_{i=1}^t [-r_i, r_i] \longrightarrow \text{SS}_{\mathcal{O}}^{\text{pr}}(\rho) \longrightarrow \text{SS}(\rho)$$

### Minkowski norm bound

The set of elements obtained by random walks should contain no cycle; thus,

$$\sum_{i=1}^t r_i \log_{\ell}(q_i) \leq n + \log_{\ell}(M) + \frac{1}{2} \log_{\ell}(|\Delta_K|/4)$$

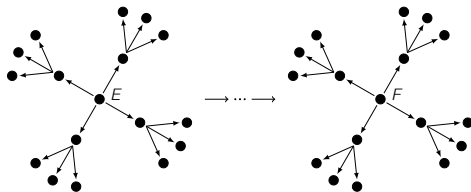
The attack of Dartois and De Feo exploits the non-injectivity of the map  $I \rightarrow \text{SS}_{\mathcal{O}}^{\text{pr}}(\rho)$  to recover an endomorphism of  $E$ .

## Key generation

On one side,  $A$  begins with  $F = E$ .

- ▶ Split primes: for each prime  $q_i$  in  $\mathcal{P}_S$ , choose a random  $s_i \in I_i$ , constructs the  $q_i$ -isogeny walk of length  $s_i$  while pushing forward the other direction as well as the  $q$ -clouds at each prime  $q$  in  $\mathcal{P}_A$  and  $\mathcal{P}_B$ .
- ▶ Non-split primes: for each prime choose a random walk in the cloud to a new curve  $F$  and push forward the remaining unused  $q$ -clouds.

The data  $F$  and  $q$ -isogeny chains at primes  $q$  in  $\mathcal{P}_S$  and  $q$ -clouds at primes  $q$  in  $\mathcal{P}_B$  constitute  $A$ 's public key.



# PARAMETER SELECTION - AN EXAMPLE

We set  $\Delta_K = -3$  and  $\ell = 2$ .

We begin with  $t = 10$  and a bit Bound  $B_s = 32$ .

## Split Primes

	$q$ :	7	13	19	31	37	43	61	67	73	79
$\mathcal{P}_s$ :	$r$ :	11	8	7	6	6	6	5	5	5	5
	$\#$ :	23	17	15	13	13	13	11	11	11	11

This gives a logarithmic contribution of

$$\sum_{j=1}^{10} \log_2(2r_j + 1) = 37.4569\dots$$

to the entropy of the random walk.

The logarithmic norm, which we must bound is:

$$\sum_{j=1}^{10} r_j \log_2(q_j) = 306.2115\dots (< 320 = 32 \cdot 10).$$



We set  $\Delta_K = -3$  and  $\ell = 2$ .

We begin with  $t = 10$  and a bit Bound  $B_s = 32$ .

## Non-Split Primes

We partition the remaining primes up to 163 into sets  $\mathcal{P}_A$  and  $\mathcal{P}_B$ , with a radius for the cloud (or eddy), as follows:

	$q$ :	2	11	17	41	47	59	83	101	103	109	131	149	151	157
$\mathcal{P}_A$ :	$r$ :	7	2	1	1	1	1	1	1	1	1	1	1	1	1
	$\#$ :	128	132	18	42	48	60	84	102	102	108	132	150	150	156
	$q$ :	3	5	23	29	53	71	89	97	107	113	127	137	139	163
$\mathcal{P}_B$ :	$r$ :	4	3	1	1	1	1	1	1	1	1	1	1	1	1
	$\#$ :	81	150	24	30	54	72	90	96	108	114	126	138	138	162

Both sets leak the horizontal directions for these primes, giving an additional contribution of  $\approx 28$  bits to the logarithmic norm.

These prime sets each contribute a  $\log_2(M)$  of 90 bits, such that  $n$  must be at least 244 to defeat the lattice-based class group attack.

The norm bound suggests using a uniform bound  $B_s$  on  $r_j \log_\ell(q_j)$  rather than the exponents  $r_j$ . This gives

$$\lambda \log_\ell(p) \leq \sum_{i=1}^t \log_\ell(2r_i + 1) \leq \sum_{j=1}^t r_j \log_\ell(q_j) \leq tB_s < n + \log_\ell(M)$$

for which ( $t = 64$ ,  $B_s = 16$ ,  $n = 1024$ ) represent a choice of parameters ensuring injectivity of  $l \rightarrow \mathcal{A}(\mathcal{O})$ .

THANK YOU FOR YOUR ATTENTION

