MARSEILLE, 23 FEBRUARY 2023

L.COLÒ I2M

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

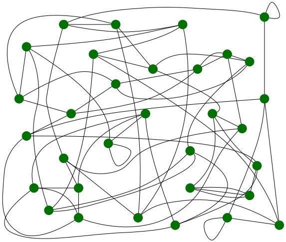
SUPERSINGULAR ISOGENY GRAPHS

L.COLÒ I2M

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 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.



ORIENTATIONS

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

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

A K-*orientation* is an embedding

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

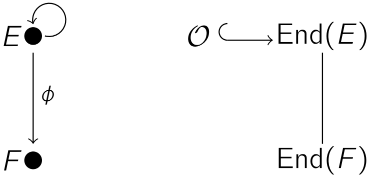
An $\mathcal{O}$-orientation is *primitive* if

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

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.

ORIENTATIONS - ORIENTING ISOGENIES



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

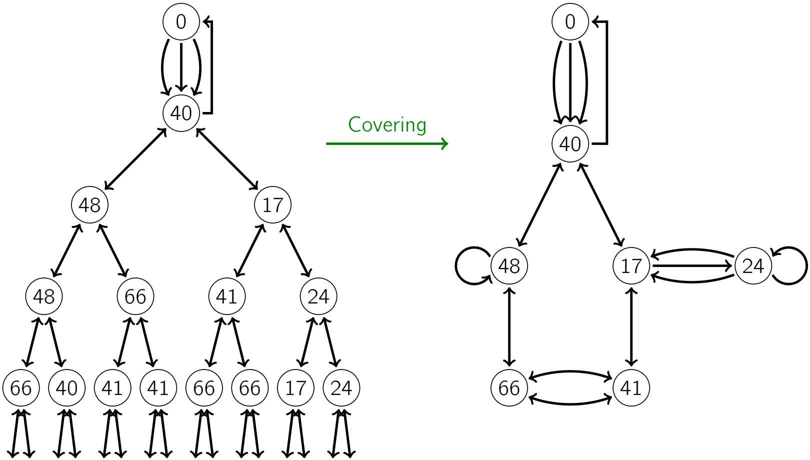
$$\phi_*(\iota)(\alpha) = \frac{1}{\ell}\,\phi \circ \iota(\alpha) \circ \hat{\phi}.$$

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

Oriented isogeny graphs - an example

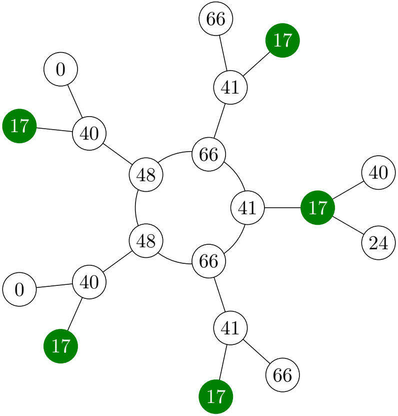
Let $p = 71$ and $E_0/\mathbb{F}_{71}$ be the supersingular elliptic curve with $j(E) = 0$ oriented by the $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega^2 + \omega + 1 = 0$.

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:



Oriented isogeny graphs - yet another example

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



PRIMITIVE ORIENTATIONS

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

An element of $\mathrm{SS}_{\mathcal{O}}^{pr}(p)$ consists of

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

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

- $\mathrm{SS}_{\mathcal{O}}^{pr}(\rho) =$ set of oriented supersingular elliptic curves with ρ induced by ι.

CLASS GROUP ACTION

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

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

Proposition

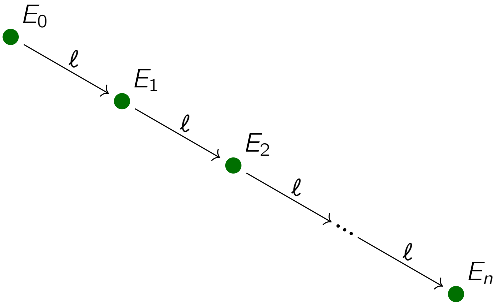
The set $\mathrm{SS}_{\mathcal{O}}^{pr}(\rho)$ is a torsor for the class group $\mathcal{C}\ell(\mathcal{O})$.

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

$$\mathcal{C}\ell(\mathcal{O}) \longrightarrow \mathrm{SS}_{\mathcal{O}}^{pr}(\rho)$$

EFFECTIVE CLASS GROUP ACTIONS

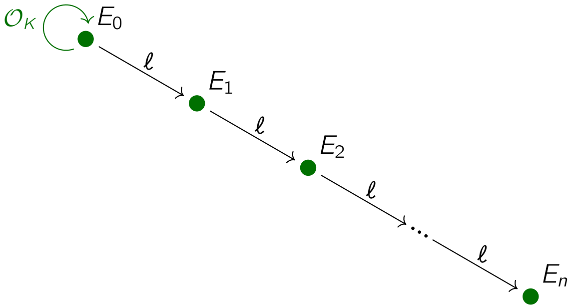
We consider an elliptic curve E_0 with an effective endomorphism ring (eg. $j_0 = 0, 1728$) and a chain of ℓ-isogenies.



EFFECTIVE CLASS GROUP ACTIONS

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

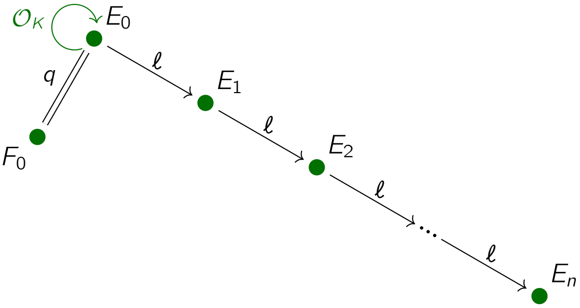
- For $\ell = 2$ (or 3) a suitable candidate for $\mathcal{O}_K$ could be the Gaussian integers $\mathbb{Z}[i]$ or the Eisenstein integers $\mathbb{Z}[\omega]$.



Effective Class Group Actions

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

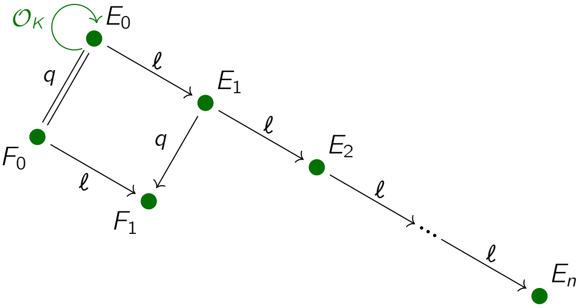
- Horizontal isogenies must be endomorphisms



Effective class group actions

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

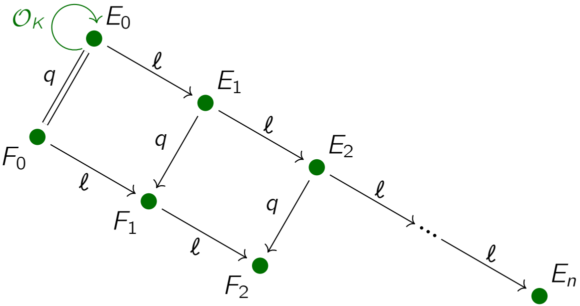
- We push forward our q-orientation obtaining F_1.



EFFECTIVE CLASS GROUP ACTIONS

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

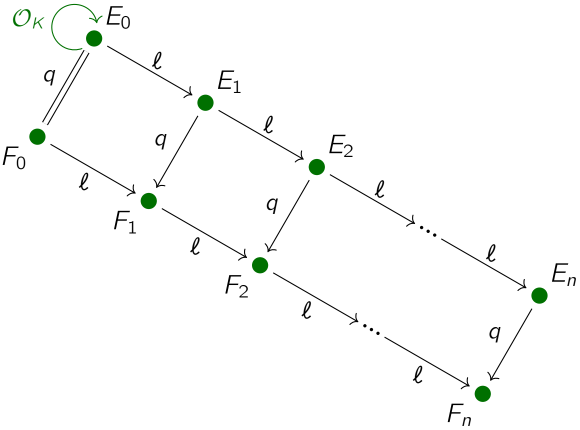
- We repeat the process for F_2.



EFFECTIVE CLASS GROUP ACTIONS

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.



OSIDH

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

ALICE	BOB

OSIDH PROTOCOL

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

	ALICE	**BOB**
Choose integers in a bound $[-r, r]$	$(e_1, \ldots, e_t)$	$(d_1, \ldots, d_t)$

OSIDH PROTOCOL

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

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

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

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

L.COLÒ I2M

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

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

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

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

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

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

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

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

SECURITY CONSIDERATIONS

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

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

The security of OSIDH depends on the following maps

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

Supersingular covering bound

We say that the map $\mathcal{C}\ell(\mathcal{O}) \simeq \mathrm{SS}^{pr}_{\mathcal{O}}(p) \longrightarrow \mathrm{SS}(p)$ is λ-*surjective* if

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

where λ is the *logarithmic covering radius*. We get

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

OSIDH PROTOCOL - SECURITY CONSIDERATIONS

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

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

The security of OSIDH depends on the following maps

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

Supersingular injectivity bound

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

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

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

OSIDH PROTOCOL - SECURITY CONSIDERATIONS

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

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

The security of OSIDH depends on the following maps

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

Class group covering bound

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

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

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

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

The security of OSIDH depends on the following maps

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

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 $I \to \mathrm{SS}_{\mathcal{O}}^{pr}(p)$ to recover an endomorphism of E.

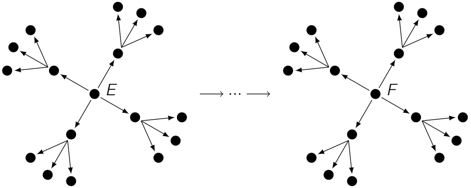
Countermeasures - the use of non-split prime

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

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

to the entropy of the random walk.

The logarithmic norm, which we must bound is:

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

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:

$\mathcal{P}_A$:	q :	2	11	17	41	47	59	83	101	103	109	131	149	151	157
	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

$\mathcal{P}_B$:	q :	3	5	23	29	53	71	89	97	107	113	127	137	139	163
	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 ≈ 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.

PARAMETER SELECTION - CONCLUSION

L.COLÒ I2M

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

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

for which $(t = 64, B_s = 16, n = 1024)$ represent a choice of parameters ensuring injectivity of $I \to \mathcal{C}\ell(\mathcal{O})$.

THANK YOU FOR YOUR ATTENTION