On the security of OSIDH

Pierrick Dartois and Luca De Feo

IBM Research Zurich, Corps des Mines, Université de Rennes 1

March 9 2022

Cryptographic group actions

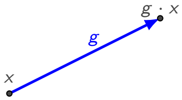
Cryptographic group action[1]

- G: an abelian group.
- X: a set ($|X| = |G|$).

[1] Brassard and Yung (1991), Couveignes (2006).

Cryptographic group action[1]

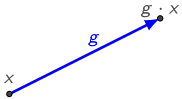
- G: an abelian group.
- X: a set ($|X| = |G|$).
- $\cdot : G \times X \longrightarrow X$ a group action that is:
  - Transitive : $\forall x, \in X, \quad G \cdot x = X$.
  - Faithful : $g \cdot x = x \Longrightarrow g = e$.



[1] Brassard and Yung (1991), Couveignes (2006).

Cryptographic group action[1]

- G: an abelian group.
- X: a set ($|X| = |G|$).
- $\cdot : G \times X \longrightarrow X$ a group action that is:
  - Transitive : $\forall x, \in X, \quad G \cdot x = X$.
  - Faithful : $g \cdot x = x \Longrightarrow g = e$.
- Easy to compute $g \cdot x$.



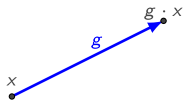
[1] Brassard and Yung (1991), Couveignes (2006).

Cryptographic group action[1]

- G: an abelian group.
- X: a set ($|X| = |G|$).
- $\cdot : G \times X \longrightarrow X$ a group action that is:
  - Transitive : $\forall x, \in X, \quad G \cdot x = X$.
  - Faithful : $g \cdot x = x \Longrightarrow g = e$.
- Easy to compute $g \cdot x$.
- One way group action:

$$\underset{known}{y} = \underset{?}{g} \cdot \underset{known}{x}$$

Finding g is hard.



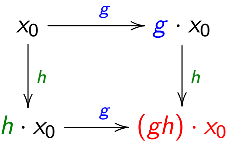
[1]Brassard and Yung (1991), Couveignes (2006).

Diffie-Hellman key exchange

- Public parameter: $x_0 \in X$.
- Alice's secret: $g \in G$.
- Bob's secret: $h \in G$.

Diffie-Hellman key exchange

- Public parameter: $x_0 \in X$.
- Alice's secret: $g \in G$.
- Bob's secret: $h \in G$.



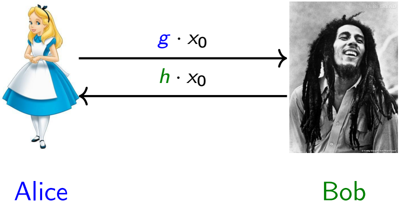


Photo credits: Gallery Yopriceville and Michael Ochs.

The OSIDH group action

The ideal class group

The ideal class group

- Quadratic imaginary field $K := \mathbb{Q}(\sqrt{-d})$, $d \in \mathbb{N}^*$.

The ideal class group

- Quadratic imaginary field $K := \mathbb{Q}(\sqrt{-d})$, $d \in \mathbb{N}^*$.
- An order $\mathcal{O} \subseteq K$ is a subring and full-rank lattice.

The ideal class group

- Quadratic imaginary field $K := \mathbb{Q}(\sqrt{-d})$, $d \in \mathbb{N}^*$.
- An order $\mathcal{O} \subseteq K$ is a subring and full-rank lattice.
- An $\mathcal{O}$-ideal $\mathfrak{a} \subseteq K$ is a lattice s.t. $\mathcal{O} \cdot \mathfrak{a} \subseteq \mathfrak{a}$.

The ideal class group

- Quadratic imaginary field $K := \mathbb{Q}(\sqrt{-d})$, $d \in \mathbb{N}^*$.
- An order $\mathcal{O} \subseteq K$ is a subring and full-rank lattice.
- An $\mathcal{O}$-ideal $\mathfrak{a} \subseteq K$ is a lattice s.t. $\mathcal{O} \cdot \mathfrak{a} \subseteq \mathfrak{a}$.
- Group of invertible ideals:

$$I(\mathcal{O}) := \{\mathfrak{a} \mid \exists \mathfrak{b}, \quad \mathfrak{a} \cdot \mathfrak{b} = \mathcal{O}\}$$

- Subgroup of principal ideals $P(\mathcal{O}) \subseteq I(\mathcal{O})$:

$$P(\mathcal{O}) := \{\alpha \cdot \mathcal{O} \mid \alpha \in K\}$$

The ideal class group

- Quadratic imaginary field $K := \mathbb{Q}(\sqrt{-d})$, $d \in \mathbb{N}^*$.
- An order $\mathcal{O} \subseteq K$ is a subring and full-rank lattice.
- An $\mathcal{O}$-ideal $\mathfrak{a} \subseteq K$ is a lattice s.t. $\mathcal{O} \cdot \mathfrak{a} \subseteq \mathfrak{a}$.
- Group of invertible ideals:

$$I(\mathcal{O}) := \{\mathfrak{a} \mid \exists \mathfrak{b}, \quad \mathfrak{a} \cdot \mathfrak{b} = \mathcal{O}\}$$

- Subgroup of principal ideals $P(\mathcal{O}) \subseteq I(\mathcal{O})$:

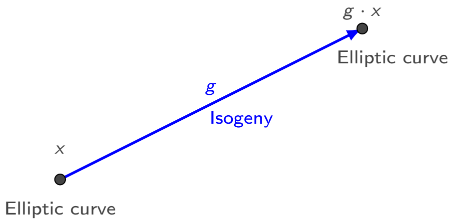
$$P(\mathcal{O}) := \{\alpha \cdot \mathcal{O} \mid \alpha \in K\}$$

- The ideal class group of $\mathcal{O}$:

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

It is a finite abelian group.

Sketch of the cryptographic group action



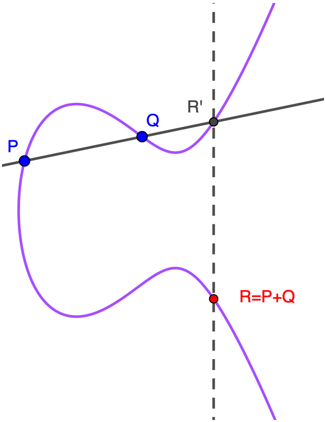
Elliptic curves

- An elliptic curve $E/\mathbb{F}_q$ is defined by:

$$y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{F}_q$.

- $E(\overline{\mathbb{F}_q})$ is an abelian group.



Isogenies

Definition

An isogeny $\varphi : E \longrightarrow F$ is:

- A morphism of algebraic varieties (given by rational fractions).
- A group homomorphism:

$$\forall P, Q \in E, \quad \varphi(P+Q) = \varphi(P) + \varphi(Q).$$

Isogenies are surjective and have finite kernel.

Isogenies

Definition

An isogeny $\varphi : E \longrightarrow F$ is:

- A morphism of algebraic varieties (given by rational fractions).
- A group homomorphism:

$$\forall P, Q \in E, \quad \varphi(P+Q) = \varphi(P) + \varphi(Q).$$

Isogenies are surjective and have finite kernel.

Examples:

1. The multiplication by $n \in \mathbb{N}$:

$$[n] : P \in E \longmapsto n \cdot P \in E$$

2. The Frobenius (if $\mathrm{char}(k) = p$):

$$\phi_p : (x, y) \in E \longmapsto (x^p, y^p) \in E^{(p)}$$

with $E^{(p)} : \; y^2 = x^3 + a^p x + b^p$ if $E : y^2 = x^3 + ax + b$.

Endomorphism rings

Definition

$$\mathrm{End}(E) = \{\text{isogenies} \quad E \longrightarrow E\}$$

Endomorphism rings

Definition

$$\mathrm{End}(E) = \{\text{isogenies} \quad E \longrightarrow E\}$$

Theorem

Let $E/\mathbb{F}_q$. Then $\mathrm{End}(E)$ is isomorphic to either:

1. *An order in a quadratic imaginary field (ordinary case).*
2. *Or a maximal order in a quaternion algebra (supersingular case).*

Oriented elliptic curves

- K: quadratic imaginary field.
- $\mathcal{O}$: order of K.
- $E/\mathbb{F}_q$: supersingular elliptic curve.

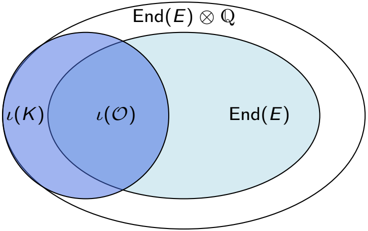
Definition (Colò and Kohel)

- K-orientation of E:

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

- ι is a (primitive) $\mathcal{O}$-orientation if

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



K-oriented isogenies

Definition (Colò and Kohel)

A K-oriented isogeny $\varphi : (E, \iota_E) \longrightarrow (F, \iota_F)$ satisfies:

$$\forall \alpha \in K, \quad \iota_F(\alpha) = \frac{1}{\deg(\varphi)} \varphi \circ \iota_E(\alpha) \circ \widehat{\varphi}.$$

where $\deg(\varphi) = \# \ker(\varphi)$ in most cases and $\widehat{\varphi}$ is the dual isogeny.

K-oriented isogenies

Definition (Colò and Kohel)

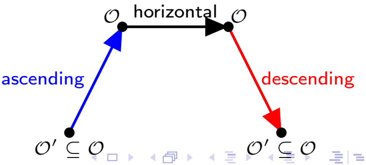
A K-oriented isogeny $\varphi : (E, \iota_E) \longrightarrow (F, \iota_F)$ satisfies:

$$\forall \alpha \in K, \quad \iota_F(\alpha) = \frac{1}{\deg(\varphi)} \varphi \circ \iota_E(\alpha) \circ \widehat{\varphi}.$$

where $\deg(\varphi) = \#\ker(\varphi)$ in most cases and $\widehat{\varphi}$ is the dual isogeny.

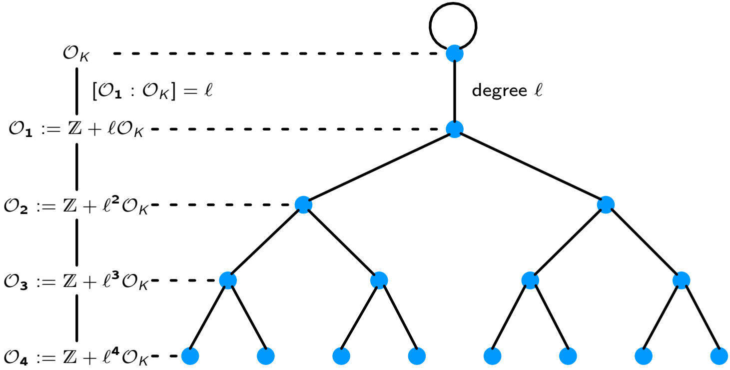
Let $\mathcal{O} := \iota_E^{-1}(\mathrm{End}(E))$ and $\mathcal{O}' := \iota_F^{-1}(\mathrm{End}(F))$:

- If $\mathcal{O} \subseteq \mathcal{O}'$, then φ is ascending.
- If $\mathcal{O} = \mathcal{O}'$, then φ is horizontal.
- If $\mathcal{O} \supseteq \mathcal{O}'$, then φ is descending.



K-oriented supersingular ℓ-isogeny graphs

Example: $K = \mathbb{Q}(i)$, $\ell = 2$, $p = 79$.



Action of $\mathrm{Cl}(\mathcal{O})$ on the primitively $\mathcal{O}$-oriented elliptic curves

Order $\mathcal{O}$	Primitively $\mathcal{O}$-oriented elliptic curves
$\mathcal{O}$-ideal $\mathfrak{a} \subseteq \mathcal{O}$	Horizontal K-oriented isogeny $(E, \iota) \longrightarrow \mathfrak{a} \cdot (E, \iota)$
Conjugate ideal $\overline{\mathfrak{a}} \equiv \mathfrak{a}^{-1}$	Dual isogeny $\mathfrak{a} \cdot (E, \iota) \longrightarrow (E, \iota)$
Principal ideal	K-oriented endomorphism
$\mathfrak{a} \equiv \mathfrak{b}$ in $\mathrm{Cl}(\mathcal{O})$	$\mathfrak{a} \cdot (E, \iota) \simeq \mathfrak{b} \cdot (E, \iota)$
Ideal multiplication	Composition of isogenies

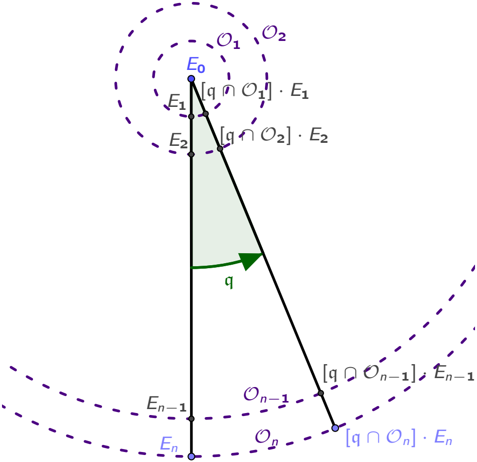
Action of $\mathrm{Cl}(\mathcal{O})$ on the primitively $\mathcal{O}$-oriented elliptic curves

Order $\mathcal{O}$	Primitively $\mathcal{O}$-oriented elliptic curves
$\mathcal{O}$-ideal $\mathfrak{a} \subseteq \mathcal{O}$	Horizontal K-oriented isogeny $(E,\iota) \longrightarrow \mathfrak{a}\cdot(E,\iota)$
Conjugate ideal $\overline{\mathfrak{a}} \equiv \mathfrak{a}^{-1}$	Dual isogeny $\mathfrak{a}\cdot(E,\iota) \longrightarrow (E,\iota)$
Principal ideal	K-oriented endomorphism
$\mathfrak{a} \equiv \mathfrak{b}$ in $\mathrm{Cl}(\mathcal{O})$	$\mathfrak{a}\cdot(E,\iota) \simeq \mathfrak{b}\cdot(E,\iota)$
Ideal multiplication	Composition of isogenies

How do we compute this cryptographic group action?

Computing the ideal class group action in OSIDH

Here $\mathcal{O} = \mathcal{O}_n = \mathbb{Z} + \ell^n \mathcal{O}_K$.



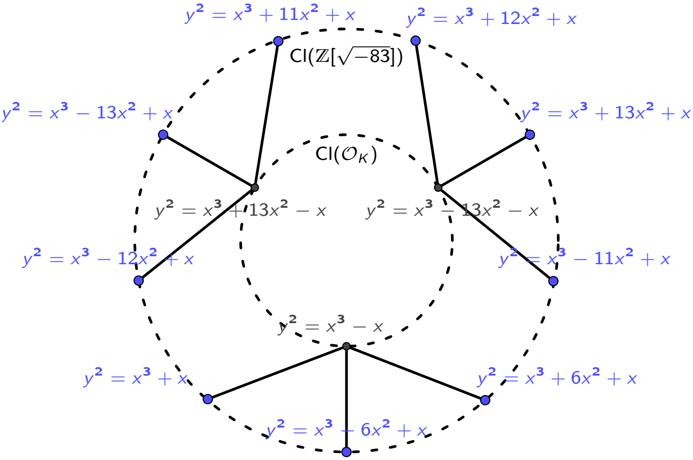
Restricted cryptographic group action

- $\mathfrak{q}_1, \cdots, \mathfrak{q}_t$ primes of $\mathcal{O}_K$ such that the $[\mathfrak{q}_j \cap \mathcal{O}_n]$ generate $\mathrm{Cl}(\mathcal{O}_n)$.
- We know how to act by $\mathfrak{q}_1, \cdots, \mathfrak{q}_t$.
- The, we can compute

$$\left(\prod_{j=1}^{t} \mathfrak{q}_j^{e_j}\right) \cdot F_n.$$

What about CSIDH?

Example: $K = \mathbb{Q}(\sqrt{-83})$, $\ell = 2$, $p = 83$, $\mathcal{O} = \mathbb{Z}[\sqrt{-83}] = \mathbb{Z} + 2\mathcal{O}_K$.



The OSIDH protocol

Naive Diffie-Hellman-like key exchange:

Public parameters:

- $\mathfrak{q}_1, \cdots, \mathfrak{q}_t$ primes of $\mathcal{O}_K$ such that the $[\mathfrak{q}_j \cap \mathcal{O}_n]$ generate $\mathrm{Cl}(\mathcal{O}_n)$.
- $(E_i)_{0 \le i \le n}$ a public descending ℓ-isogeny chain.

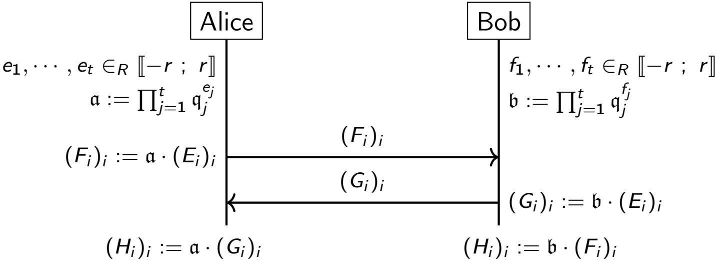
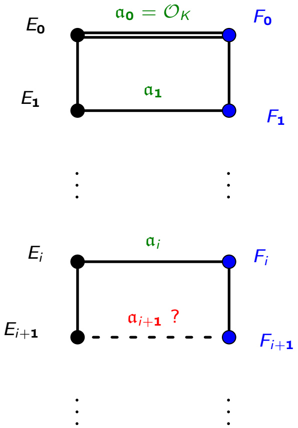


Figure: Naive protocol.

Attack on the straw man key exchange (Colò and Kohel)

Goal: Find $\mathfrak{a}_n \subseteq \mathcal{O}_n$ s.t. $[\mathfrak{a}_n] \cdot E_n = F_n$.

$$\mathfrak{a}_{i+1} \cdot \mathcal{O}_i \equiv \mathfrak{a}_i \text{ in } \mathrm{Cl}(\mathcal{O}_i)$$

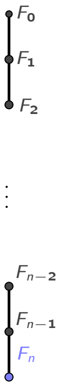


Trick of the real OSIDH protocol:

- Keep the chain $(F_i)_{0\leq i\leq n} := \mathfrak{a}\cdot(E_i)_{0\leq i\leq n}$ secret, only F_n matters.

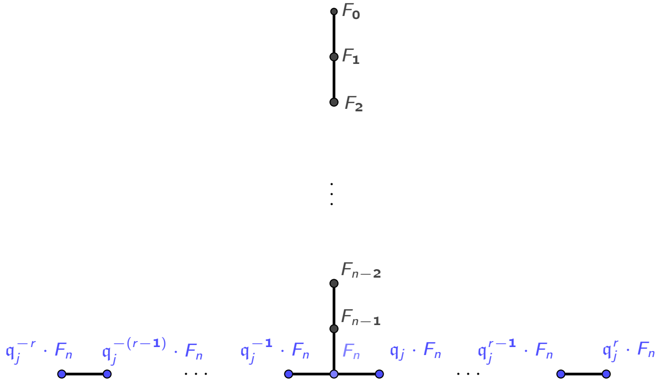
Trick of the real OSIDH protocol:

- Keep the chain $(F_i)_{0 \leq i \leq n} := \mathfrak{a} \cdot (E_i)_{0 \leq i \leq n}$ secret, only F_n matters.
- Some additional data may be useful: $(\mathfrak{q}_j^k \cdot F_n)_{\substack{1 \leq j \leq t \\ -r \leq k \leq r}}$.



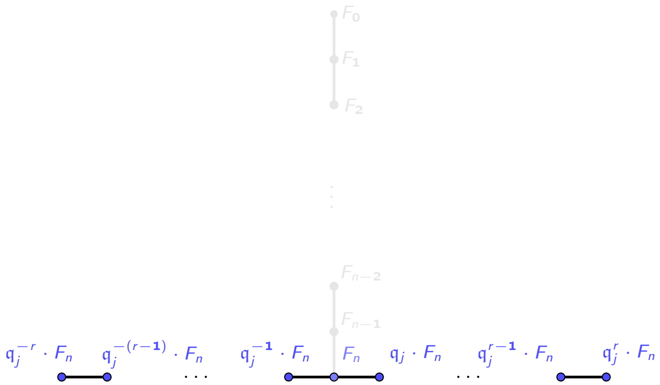
Trick of the real OSIDH protocol:

- Keep the chain $(F_i)_{0 \leq i \leq n} := \mathfrak{a} \cdot (E_i)_{0 \leq i \leq n}$ secret, only F_n matters.
- Some additional data may be useful: $(\mathfrak{q}_j^k \cdot F_n)_{\substack{1 \leq j \leq t \\ -r \leq k \leq r}}$.



Trick of the real OSIDH protocol:

- Keep the chain $(F_i)_{0\leq i\leq n} := \mathfrak{a}\cdot(E_i)_{0\leq i\leq n}$ secret, only F_n matters.
- Some additional data may be useful: $(\mathfrak{q}_j^k \cdot F_n)_{\substack{1\leq j\leq t \\ -r\leq k\leq r}}$.



Cryptanalysis of OSIDH

Idea (Onuki, 2020): Use the chains:

$$\mathfrak{q}_j^{-r} \cdot F_n \longrightarrow \cdots \longrightarrow \mathfrak{q}_j^{r} \cdot F_n \quad (1 \leq j \leq t)$$

to find a cycle.

Idea (Onuki, 2020): Use the chains:

$$\mathfrak{q}_j^{-r} \cdot F_n \longrightarrow \cdots \longrightarrow \mathfrak{q}_j^{r} \cdot F_n \quad (1 \leq j \leq t)$$

to find a cycle.

- Compute $\mathfrak{b} \cdot F_n$ with:

$$\mathfrak{b} := \prod_{j=1}^{t} \mathfrak{q}_j^{e_j} \quad (|e_j| \leq 2r)$$

  a principal ideal.

Idea (Onuki, 2020): Use the chains:

$$\mathfrak{q}_j^{-r} \cdot F_n \longrightarrow \cdots \longrightarrow \mathfrak{q}_j^{r} \cdot F_n \quad (1 \leq j \leq t)$$

to find a cycle.

- Compute $\mathfrak{b} \cdot F_n$ with:

$$\mathfrak{b} := \prod_{j=1}^{t} \mathfrak{q}_j^{e_j} \quad (|e_j| \leq 2r)$$

  a principal ideal.

- It gives an endomorphism:

$$F_n \longrightarrow \mathfrak{b} \cdot F_n = F_n.$$

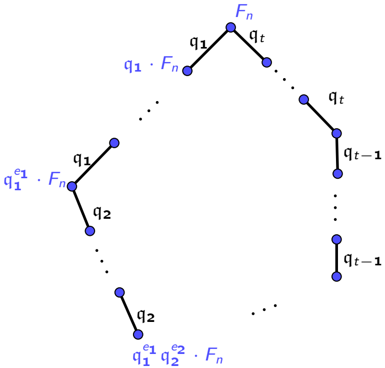


Figure: Cycle in the orbit of $\mathrm{Cl}(\mathcal{O}_n)$.

What can we do with an endomorphism?

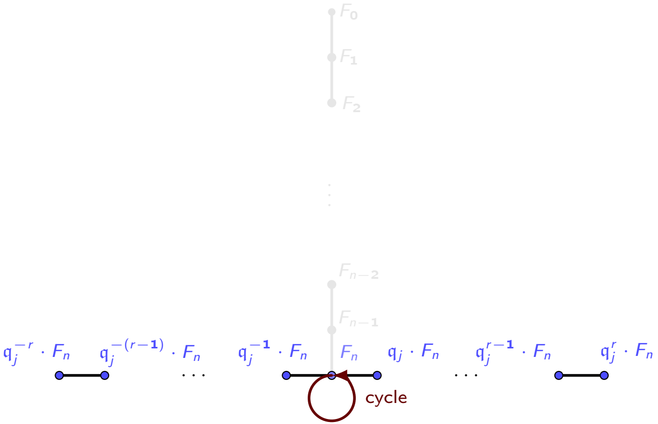
Notations:

- ι'_n: the orientation of F_n.
- $\iota'_n(\beta)$: the endomorphism we found.
- $\mathcal{O}_n := \mathbb{Z}[\alpha]$.
- $\beta := a + b\alpha$ $(b \wedge \ell = 1)$.

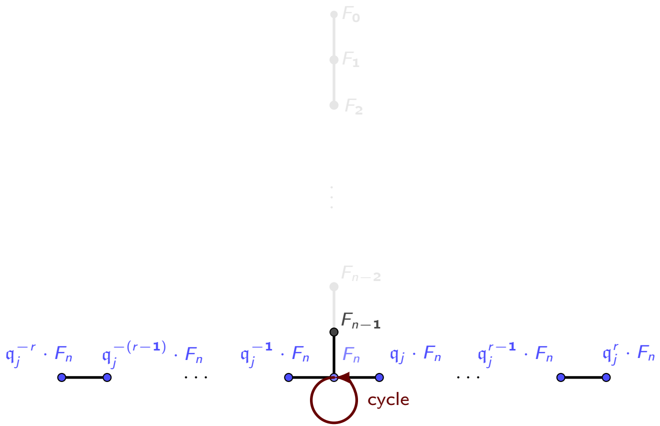
Lemma

$$\ker(\iota'_n(b\alpha)) \cap F_n[\ell] = \ker(\hat{\varphi}_n : F_n \longrightarrow F_{n-1})$$

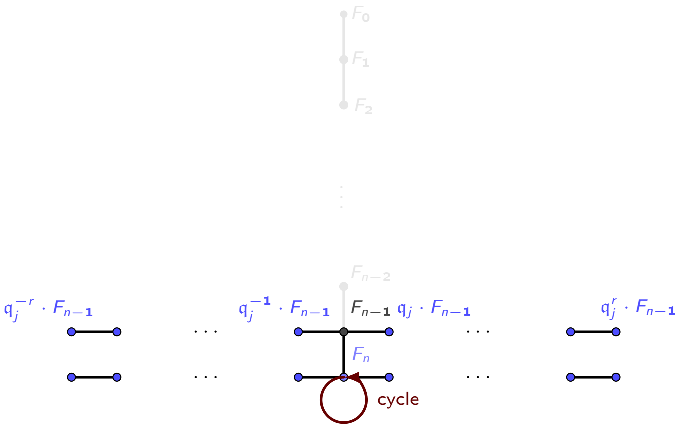
Chain recovery



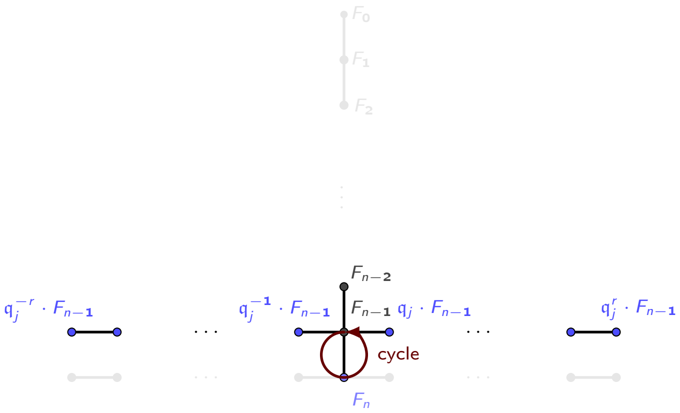
Chain recovery



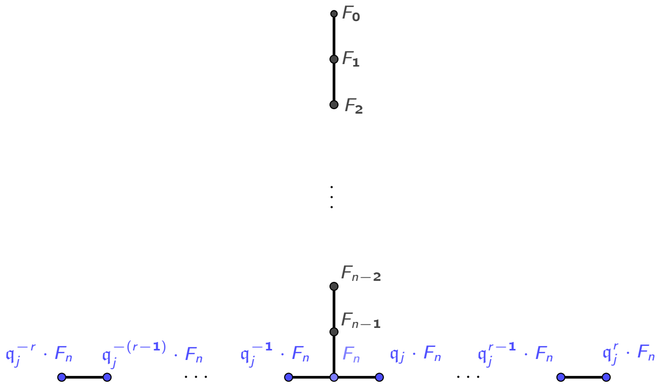
Chain recovery



Chain recovery



Chain recovery



Our main contribution: how to find cycles?

- **Onuki's approach:** Find $\mathfrak{b}$ principal by exhaustive search (costly) and compute $\mathfrak{b} \cdot F_n$ (costly).[2]
- **Our approach:** Look for a shot vector in:

$$L := \left\{ (e_1, \cdots, e_t) \in \mathbb{Z}^t \;\middle|\; \prod_{j=1}^{t} [\mathfrak{q}_j \cap \mathcal{O}_n]^{e_j} = [1] \quad \text{in} \ \mathrm{Cl}(\mathcal{O}_n) \right\}$$

to get $\mathfrak{b} := \prod_{j=1}^{t} (\mathfrak{q}_j \cap \mathcal{O}_n)^{e_j}$ principal.

[2] Here $\mathfrak{b}$ is not necessarily a product of the $\mathfrak{q}_j$.

Complexity of the attack:

- The expensive step: find a short vector in the lattice

$$L := \left\{ (e_1, \cdots, e_t) \in \mathbb{Z}^t \;\middle|\; \prod_{j=1}^{t} [\mathfrak{q}_j \cap \mathcal{O}_n]^{e_j} = [1] \quad \text{in } \mathrm{Cl}(\mathcal{O}_n) \right\}.$$

- **Example:** For $t = 74$ (Colò and Kohel), lattice reduction takes 0.5 s with BKZ.

Complexity of the attack:

- The expensive step: find a short vector in the lattice

$$L := \left\{ (e_1, \cdots, e_t) \in \mathbb{Z}^t \;\middle|\; \prod_{j=1}^{t} [\mathfrak{q}_j \cap \mathcal{O}_n]^{e_j} = [1] \quad \text{in } \mathrm{Cl}(\mathcal{O}_n) \right\}.$$

- **Example:** For $t = 74$ (Colò and Kohel), lattice reduction takes 0.5 s with BKZ.
- All other steps are polynomial (including the computation of L).

Complexity of the attack:

- The expensive step: find a short vector in the lattice

$$L := \left\{ (e_1, \cdots, e_t) \in \mathbb{Z}^t \;\middle|\; \prod_{j=1}^{t} [\mathfrak{q}_j \cap \mathcal{O}_n]^{e_j} = [1] \quad \text{in } \mathrm{Cl}(\mathcal{O}_n) \right\}.$$

- **Example:** For $t = 74$ (Colò and Kohel), lattice reduction takes 0.5 s with BKZ.
- All other steps are polynomial (including the computation of L).
- Polynomial time operations (group action) are very slow.
- No practical implementation of the protocol.

Implementation with toy parameters: $\ell = 2$, $n = 28, t = 10$, $r = 3$ and $K = \mathbb{Q}(i)$.

```
sage: load("Documents/Codes/OSIDH/OSIDH_attack_tests.py")

Protocol execution:

Alice:
Alice's secret key:
[2, 1, -3, 3, 3, 3, 3, -1, -3, 1]
Alice's action on public chain complete.

Bob:
Bob's secret key:
[2, 0, -1, 1, 3, -3, 1, 2, 0, 2]
Bob's action on public chain complete.

Alice's action on Bob's data complete.

Bob's action on Alice's data complete.

Shared chains coincide: True
Protocol execution time: 86.6418662071228 s
```

```
Attack: part 1 - recovering the chains of Alice and Bob

Alice
Alice's chain recovered: True

Bob
Bob's chain recovered: True

Timing part 1: 243.38196992874146 s

Attack: part 2 - recovering Alice's secret exponents

Timing part 2: 109.8835232257843 s

Attack: part 3 - recovering the shared secret chain
Attack is correct: True
Timing part 3: 8.221031904220581 s

Total attack timing : 361.48652505874634 s
```

Find our implementation on github.com/Pierrick-Dartois/OSIDH.

Implementation with toy parameters: $\ell = 2$, $n = 28, t = 10$, $r = 3$ and $K = \mathbb{Q}(i)$.

	Protocol	Complete attack
Average (in s)	84.83	376.05
Standard deviation (in s)	5.61	18.29
Margin of error (95 %) on the average (in s)	1.46	4.76

Countermeasures - preliminary remark:

Theorem

$$\lambda_1^{(\infty)}(L) \simeq \frac{\# \operatorname{Cl}(\mathcal{O}_n)^{1/t}}{2}$$

The attack runs under the hypothesis that the key space

$$\left\{ \prod_{j=1}^{t} [\mathfrak{q}_j \cap \mathcal{O}_n]^{e_j} \;\middle|\; e_1, \cdots, e_t \in [\![-r\ ;\ r]\!] \right\}$$

tightly covers $\operatorname{Cl}(\mathcal{O}_n)$:

$$(2r+1)^t \simeq \# \operatorname{Cl}(\mathcal{O}_n) \simeq \ell^n.$$

so that $\lambda_1^{(\infty)}(L) \leq 2r$.

Countermeasures:

	Method 1	**Method 2**
Description	Increase n and t, keep $(2r+1)^t \simeq \#\mathrm{Cl}(\mathcal{O}_n) \simeq \ell^n$	Increase n, so that $(2r+1)^t \ll \ell^n$
Consequence	SVP is hard	No short enough vectors
Drawbacks	(1). Slows the protocol (2). Lattice based security assumption	No longer a cryptographic group action

Conclusion

To sum up: Our attack severely undermines the relevance of OSIDH.

Thanks for watching!