On the security of OSIDH

Pierrick Dartois and Luca De Feo

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

March 15 2022

Introduction: cryptographic group actions

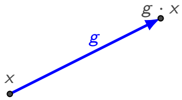
Cryptographic group action[1]

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

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

Cryptographic group action[1]

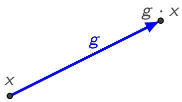
- G: an abelian group.
- X: a set ($|X| = |G|$).
- $\cdot : G \times X \longrightarrow X$ a group action that is:
  - Transitive : $\forall x, \in X, \quad G \cdot x = X$.
  - Faithful : $g \cdot x = x \Longrightarrow g = e$.



[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 $g \cdot x$.



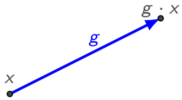
[1] Brassard and Yung (1991), Couveignes (2006).

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: $h \in G$.

$$\begin{tikzcd}
x_0 \arrow[r, "g"] \arrow[d, "h"] & g \cdot x_0 \arrow[d, "h"] \\
h \cdot x_0 \arrow[r, "g"] & (gh) \cdot x_0
\end{tikzcd}$$

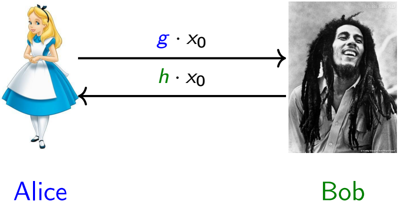
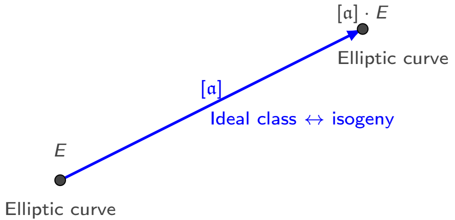


Photo credits: Gallery Yopriceville and Michael Ochs.

Mathematical framework of OSIDH

The ideal class group action on oriented supersingular elliptic curves

- Group: ideal class group $\mathrm{Cl}(\mathcal{O})$.
- Space: primitively $\mathcal{O}$-oriented supersingular elliptic curves[2].
- Group action: isogenies representing ideal classes[2].



[2] up to oriented isomorphism.

Oriented elliptic curves

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

Definition (Colò and Kohel)

A K-orientation of E is an embedding:

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

(E, ι) is an $\mathcal{O}$-orientation if $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$.
It is primitive if $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$.

Oriented elliptic curves

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

Definition (Colò and Kohel)

A K-orientation of E is an embedding:

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

(E, ι) is an $\mathcal{O}$-orientation if $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$.
It is primitive if $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$.

- If E is ordinary, then $\iota(K) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Not very interesting.

Oriented elliptic curves

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

Definition (Colò and Kohel)

A K-orientation of E is an embedding:

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

(E, ι) is an $\mathcal{O}$-orientation if $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$.
It is primitive if $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$.

- If E is ordinary, then $\iota(K) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Not very interesting.
- If E is supersingular, $\mathrm{End}(E)$ is a maximal order in a quaternion algebra: infinitely many possible orientations.

K-oriented isogenies

- (E, ι) is a K-oriented elliptic curve.
- $\varphi : E \longrightarrow F$ is an isogeny.
- We define a K-orientation $\varphi_*(\iota)$ on F by:

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

Definition (Colò and Kohel)

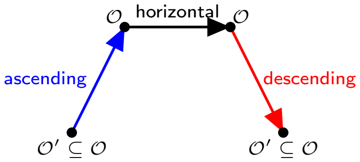
Let (E, ι_E) and (F, ι_F) be two K-oriented elliptic curves.
An isogeny $\varphi : E \longrightarrow F$ is K-oriented if $\varphi_*(\iota_E) = \iota_F$.
We denote this by $\varphi : (E, \iota_E) \longrightarrow (F, \iota_F)$.

Ascending, horizontal, descending K-oriented isogenies

- $\varphi : (E, \iota_E) \longrightarrow (F, \iota_F)$, a K-oriented isogeny.
- $\mathcal{O} := \iota_E^{-1}(\mathrm{End}(E))$.
- $\mathcal{O}' := \iota_F^{-1}(\mathrm{End}(F))$.

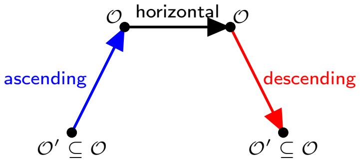
Ascending, horizontal, descending K-oriented isogenies

- $\varphi : (E, \iota_E) \longrightarrow (F, \iota_F)$, a K-oriented isogeny.
- $\mathcal{O} := \iota_E^{-1}(\mathrm{End}(E))$.
- $\mathcal{O}' := \iota_F^{-1}(\mathrm{End}(F))$.
- 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.



Ascending, horizontal, descending K-oriented isogenies

- $\varphi : (E, \iota_E) \longrightarrow (F, \iota_F)$, a K-oriented isogeny.
- $\mathcal{O} := \iota_E^{-1}(\mathrm{End}(E))$.
- $\mathcal{O}' := \iota_F^{-1}(\mathrm{End}(F))$.
- 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.



Proposition (Kohel)

If $\ell := \deg(\varphi)$ is prime, then:

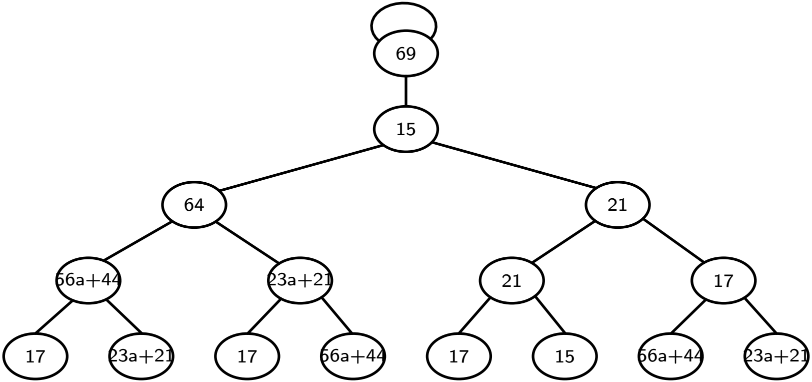
(i) φ is always ascending, horizontal or descending.

(ii) If φ is ascending, then $[\mathcal{O}' : \mathcal{O}] = \ell$.

(iii) If φ is descending, then $[\mathcal{O} : \mathcal{O}'] = \ell$.

K-oriented supersingular ℓ-isogeny graphs

Example: $K = \mathbb{Q}(i)$, $\ell = 2$, $p = 79$, $\mathbb{F}_{79^2} = \mathbb{F}_{79}[a]$ with $a^2 - a + 3 = 0$.



Example: $K = \mathbb{Q}(i)$, $\ell = 2$, $p = 79$, $\mathbb{F}_{79^2} = \mathbb{F}_{79}[a]$ with $a^2 - a + 3 = 0$.

The graph refolds!

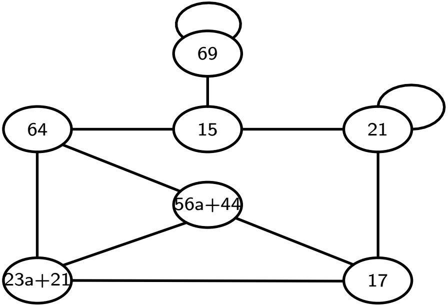


Figure: Supersingular 2-isogeny graph over $\mathbb{F}_{79^2}$.

Representing K-oriented elliptic curves by j-invariants

- $\mathrm{SS}_K(p)$: set of K-oriented supersingular elliptic curves over $\mathbb{F}_{p^2}$ up to K-oriented isomomorphism.
- $\mathrm{SS}(p)$: set of supersingular elliptic curves over $\mathbb{F}_{p^2}$ up to isomomorphism (supersingular j-invariants).
- Unfortunately, the forgetful map:

$$(E,\iota) \in \mathrm{SS}_K(p) \longmapsto E \in \mathrm{SS}(p)$$

is not injective.

Representing K-oriented elliptic curves by j-invariants

- But we can restrict to $\mathcal{O}$-orientations with $\mathrm{disc}(\mathcal{O})$ bounded.
- $\mathrm{SS}_{\mathcal{O}}(p)$: set of $\mathcal{O}$-oriented supersingular elliptic curves over $\mathbb{F}_{p^2}$ up to K-oriented isomomorphism.

Theorem (Colò and Kohel)

If $p > |\mathrm{disc}(\mathcal{O})|$, then the forgetful map:

$$(E, \iota) \in \mathrm{SS}_{\mathcal{O}}(p) \longmapsto E \in \mathrm{SS}(p)$$

is injective.

The ideal class group action

- $\mathrm{SS}_{\mathcal{O}}^{pr}(p)$: set of **primitively** $\mathcal{O}$-oriented supersingular elliptic curves over $\mathbb{F}_{p^2}$ up to K-oriented isomorphism.

- We define a group action:

$$\mathrm{Cl}(\mathcal{O}) \times \mathrm{SS}_{\mathcal{O}}^{pr}(p) \longrightarrow \mathrm{SS}_{\mathcal{O}}^{pr}(p).$$

- If $(E, \iota) \in \mathrm{SS}_{\mathcal{O}}^{pr}(p)$ and $\mathfrak{a} \subseteq \mathcal{O}$ has norm prime to p, we consider:

$$\varphi_{\mathfrak{a}} : E \longrightarrow E/E[\mathfrak{a}]$$

with:

$$\ker(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha)).$$

- We set:

$$[\mathfrak{a}] \cdot (E, \iota) := (E/E[\mathfrak{a}], (\varphi_{\mathfrak{a}})_*(\iota)).$$

The ideal class group action

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

The ideal class group action

Theorem (Onuki)

The ideal class group action $\mathrm{Cl}(\mathcal{O}) \times \mathrm{SS}^{pr}_{\mathcal{O}}(p) \longrightarrow \mathrm{SS}^{pr}_{\mathcal{O}}(p)$ *is well-defined,* ***faithful*** *but* ***not transitive****. Actually, there are two orbits.*

The ideal class group action

Theorem (Onuki)

The ideal class group action $\mathrm{Cl}(\mathcal{O}) \times \mathrm{SS}^{pr}_{\mathcal{O}}(p) \longrightarrow \mathrm{SS}^{pr}_{\mathcal{O}}(p)$ *is well-defined,* ***faithful*** *but* ***not transitive****. Actually, there are two orbits.*

To make it transitive: restrict to the orbit of elliptic curves obtained by reduction mod p of elliptic curves defined over a number field with complex multiplication by $\mathcal{O}$.

ℓ-isogeny chains and ladders

Definition

A K-oriented ℓ-isogeny chain of length n is a sequence of K-oriented ℓ-isogenies:

$$E_0 \xrightarrow{\varphi_0} E_1 \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{n-2}} E_{n-1} \xrightarrow{\varphi_{n-1}} E_n \ .$$

It is descending, horizontal or ascending if all the φ_i are.

ℓ-isogeny chains and ladders

Definition

A K-oriented ℓ-isogeny chain of length n is a sequence of K-oriented ℓ-isogenies:

$$E_0 \xrightarrow{\varphi_0} E_1 \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{n-2}} E_{n-1} \xrightarrow{\varphi_{n-1}} E_n\ .$$

It is descending, horizontal or ascending if all the φ_i are.
A K-oriented ℓ-ladder of length n and degree q is a commutative diagram of K-oriented ℓ-isogeny chains:

$$\begin{tikzcd}
E_0 \arrow[r, "\varphi_0"] \arrow[d, "\psi_0"] & E_1 \arrow[r, "\varphi_1"] \arrow[d, "\psi_1"] & \cdots \arrow[r, "\varphi_{n-2}"] & E_{n-1} \arrow[r, "\varphi_{n-1}"] \arrow[d, "\psi_{n-1}"] & E_n \arrow[d, "\psi_n"] \\
F_0 \arrow[r, "\varphi'_0"] & F_1 \arrow[r, "\varphi'_1"] & \cdots \arrow[r, "\varphi'_{n-2}"] & F_{n-1} \arrow[r, "\varphi'_{n-1}"] & F_n
\end{tikzcd}$$

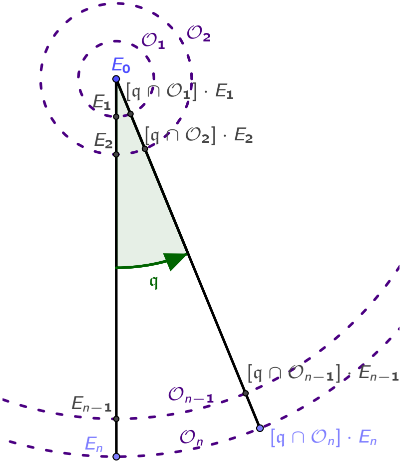
such that $\psi_i : E_i \longrightarrow F_i$ is a K-oriented q-isogeny for all $i \in [\![0\ ;\ n]\!]$.

Computing the ideal class group action in OSIDH

- $\mathcal{O}_i := \mathbb{Z} + \ell^i \mathcal{O}_K$ for all $i \in \mathbb{N}$.
- Represent an $\mathcal{O}_n$-oriented elliptic curve (E_n, ι_n) by a descending ℓ-isogeny chain $(E_i, \iota_i)_{0 \leq i \leq n}$.
- Let $\mathfrak{q} \subseteq \mathcal{O}_K$ be a prime ideal.
- We compute the chain $(F_i, \iota_i')_i := [\mathfrak{q}] \cdot (E_i, \iota_i)_i$:

  $$\forall 0 \leq i \leq n,\ \ F_i := [\mathfrak{q} \cap \mathcal{O}_i] \cdot E_i$$

  to get $F_n := [\mathfrak{q} \cap \mathcal{O}_n] \cdot E_n$.
- Assumption: $\mathrm{Cl}(\mathcal{O}_K) = \{1\}$, so that $E_0 = F_0$.



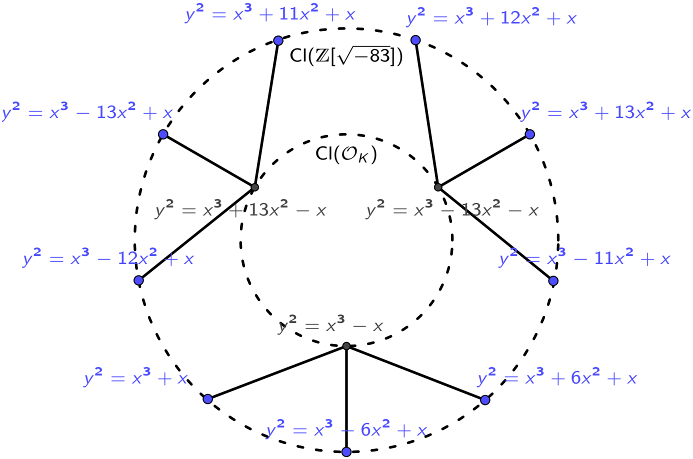
Restricted cryptographic group action

- $q_1, \cdots, q_t \neq \ell$ splitting primes in K.
- $\mathfrak{q}_1, \cdots, \mathfrak{q}_t$ primes of $\mathcal{O}_K$ lying above $q_1, \cdots, q_t$.
- 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 key exchange:

Public parameters:

- Prime ideals $\mathfrak{q}_1, \cdots, \mathfrak{q}_t$.
- $(E_i)_{0 \leq i \leq n}$ a public descending ℓ-isogeny chain.

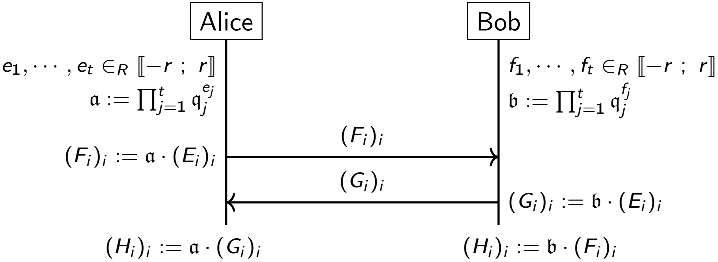


Figure: Naive protocol.

Attack on the ℓ-ladder[3]

- Given $(E_i)_i$ and $(F_i)_i := [\mathfrak{a}] \cdot (E_i)_i$, we recover $[\mathfrak{a} \cap \mathcal{O}_n] \in \mathrm{Cl}(\mathcal{O}_n)$

- Knowing $\mathfrak{a}_i \subseteq \mathcal{O}_K$, such that $[\mathfrak{a}_i \cap \mathcal{O}_i] = [\mathfrak{a} \cap \mathcal{O}_i]$, we look for:

$$\mathfrak{a}_{i+1} := \mathfrak{a}_i \cdot \mathfrak{b}$$

  with $[\mathfrak{b} \cap \mathcal{O}_{i+1}] \in \ker(\mathrm{Cl}(\mathcal{O}_{i+1}) \twoheadrightarrow \mathrm{Cl}(\mathcal{O}_i))$ such that:

$$[(\mathfrak{a}_i \cdot \mathfrak{b}) \cap \mathcal{O}_{i+1}] \cdot E_{i+1} = F_{i+1}$$

- $|\ker(\mathrm{Cl}(\mathcal{O}_{i+1}) \twoheadrightarrow \mathrm{Cl}(\mathcal{O}_i))| \leq \ell + 1$, so we have a few values of $\mathfrak{b}$ to test.

$$\begin{tikzcd}
E_0 \arrow[r, equal] \arrow[d] & F_0 \arrow[d] \\
\vdots \arrow[d] & \vdots \arrow[d] \\
E_i \arrow[r, "\mathfrak{a}_i"] \arrow[d] & F_i \arrow[d] \\
E_{i+1} \arrow[r, dashed, "\mathfrak{a}_{i+1} := \mathfrak{a}_i \cdot \mathfrak{b}"] \arrow[d] & F_{i+1} \arrow[d] \\
\vdots & \vdots
\end{tikzcd}$$

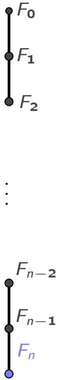
[3] Colò and Kohel.

Trick of the real OSIDH protocol (Colò and Kohel):

- 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.

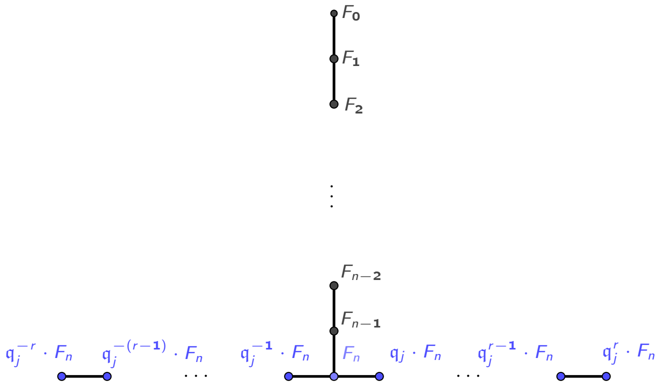
Trick of the real OSIDH protocol (Colò and Kohel):

- 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: $\left(\mathfrak{q}_j^k \cdot F_n\right)_{\substack{1\leq j\leq t \\ -r\leq k\leq r}}$.



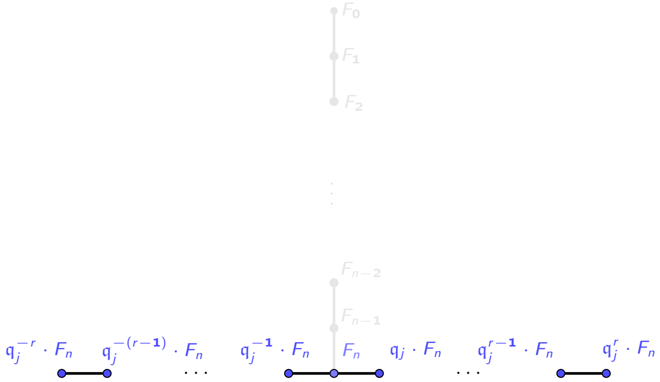
Trick of the real OSIDH protocol (Colò and Kohel):

- 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 (Colò and Kohel):

- 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: $(\mathfrak{q}_j^k \cdot F_n)_{\substack{1\leq j\leq t \\ -r\leq k\leq r}}$.



 The OSIDH protocol

Why does it work?

Example: Bob computes $H_n = [\mathfrak{b}] \cdot F_n$ with $[\mathfrak{b}] = [\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2]^{f_2}$.

$$
\begin{tikzcd}
{[\mathfrak{q}_2]^{f_2} \cdot E_{A,n}} \arrow[r] & {[\mathfrak{q}_1][\mathfrak{q}_2]^{f_2} \cdot F_n} \arrow[r] & \cdots \arrow[r] & {[\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2]^{f_2} \cdot F_n} \\
{[\mathfrak{q}_2]^{f_2-1} \cdot F_n} \arrow[r] \arrow[u] & {[\mathfrak{q}_1][\mathfrak{q}_2]^{f_2-1} \cdot F_n} \arrow[r] \arrow[u] & \cdots \arrow[r] & {[\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2]^{f_2-1} \cdot F_n} \arrow[u] \\
\vdots \arrow[u] & \vdots \arrow[u] & \ddots & \vdots \arrow[u] \\
{[\mathfrak{q}_2] \cdot F_n} \arrow[r] \arrow[u] & {[\mathfrak{q}_1][\mathfrak{q}_2] \cdot F_n} \arrow[r] \arrow[u] & \cdots \arrow[r] & {[\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2] \cdot F_n} \arrow[u] \\
F_n \arrow[r, "\mathfrak{q}_1"] \arrow[u, "\mathfrak{q}_2"] & {[\mathfrak{q}_1] \cdot F_n} \arrow[r] \arrow[u] & \cdots \arrow[r] & {[\mathfrak{q}_1]^{f_1} \cdot F_n.} \arrow[u]
\end{tikzcd}
$$

 The OSIDH protocol

The protocol[4]

Public parameters:

$(E_i)_i,\ \mathfrak{q}_1, \cdots, \mathfrak{q}_t$

Alice | **Bob**

Alice:

$e_1, \cdots, e_t \in_R [\![-r\ ;\ r]\!]$

$\mathfrak{a} := \prod_{j=1}^{t} \mathfrak{q}_j^{e_j}$

$(F_i)_i := [\mathfrak{a}] \cdot (E_i)_i$

Bob:

$f_1, \cdots, f_t \in_R [\![-r\ ;\ r]\!]$

$\mathfrak{b} := \prod_{j=1}^{t} \mathfrak{q}_j^{f_j}$

Alice → Bob: $[\mathfrak{q}_j]^{-r} \cdot F_n \longrightarrow \cdots \longrightarrow [\mathfrak{q}_j]^{r} \cdot F_n$

Bob → Alice: $[\mathfrak{q}_j]^{-r} \cdot G_n \longrightarrow \cdots \longrightarrow [\mathfrak{q}_j]^{r} \cdot G_n$

Bob: $(G_i)_i := [\mathfrak{b}] \cdot (E_i)_i$

Alice: $H_n := [\mathfrak{a}] \cdot G_n$

Bob: $H_n := [\mathfrak{b}] \cdot F_n$

Figure: The OSIDH protocol.

[4] Colò and Kohel.

Cryptanalysis of OSIDH

Recovering the chain with oriented endomorphisms[5]

- Given $(E_i)_i$ and $(F_i)_i := [\mathfrak{a}] \cdot (E_i)_i$, we can recover the secret $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_n)$.

[5] Onuki (2020).

Recovering the chain with oriented endomorphisms[5]

- Given $(E_i)_i$ and $(F_i)_i := [\mathfrak{a}] \cdot (E_i)_i$, we can recover the secret $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_n)$.
- **Problem:** recover $(F_i)_i$ with the knowledge of:

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

[5] Onuki (2020).

Recovering the chain with oriented endomorphisms[5]

- Given $(E_i)_i$ and $(F_i)_i := [\mathfrak{a}] \cdot (E_i)_i$, we can recover the secret $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_n)$.
- **Problem:** recover $(F_i)_i$ with the knowledge of:

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

- Assume that we know a K-oriented endomorphism $\iota_n'(\beta) \in \mathrm{End}(F_n)$ for some known value $\beta \in \mathcal{O}_n \setminus \mathcal{O}_{n+1}$.

[5] Onuki (2020).

Recovering the chain with oriented endomorphisms[5]

- Given $(E_i)_i$ and $(F_i)_i := [\mathfrak{a}] \cdot (E_i)_i$, we can recover the secret $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_n)$.
- **Problem:** recover $(F_i)_i$ with the knowledge of:

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

- Assume that we know a K-oriented endomorphism $\iota_n'(\beta) \in \mathrm{End}(F_n)$ for some known value $\beta \in \mathcal{O}_n \setminus \mathcal{O}_{n+1}$.
- Set $\mathcal{O}_K := \mathbb{Z}[\theta]$ and $\beta := a + b\ell^n\theta$ with $b \wedge \ell = 1$.
- We know $\iota_n'(a) = [a]$ so we know $\iota_n'(b\ell^n\theta)$.

[5] Onuki (2020).

Recovering the chain with oriented endomorphisms[5]

- Given $(E_i)_i$ and $(F_i)_i := [\mathfrak{a}] \cdot (E_i)_i$, we can recover the secret $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_n)$.
- **Problem:** recover $(F_i)_i$ with the knowledge of:

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

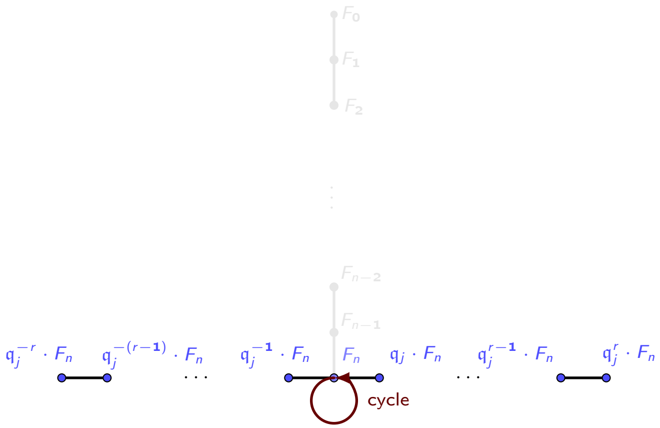
- Assume that we know a K-oriented endomorphism $\iota_n'(\beta) \in \mathrm{End}(F_n)$ for some known value $\beta \in \mathcal{O}_n \setminus \mathcal{O}_{n+1}$.
- Set $\mathcal{O}_K := \mathbb{Z}[\theta]$ and $\beta := a + b\ell^n\theta$ with $b \wedge \ell = 1$.
- We know $\iota_n'(a) = [a]$ so we know $\iota_n'(b\ell^n\theta)$.

Lemma

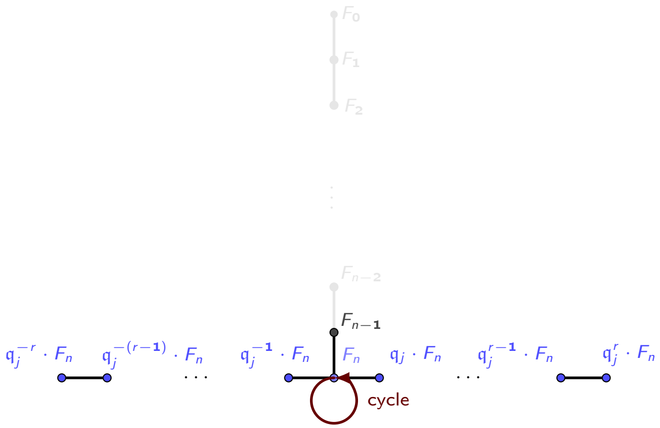
$\ker(\iota_n'(b\ell^n\theta)) \cap F_n[\ell] = \ker(\widehat{\varphi}_{n-1}')$, *with* $\varphi_{n-1}' : F_{n-1} \longrightarrow F_n$.

[5] Onuki (2020).

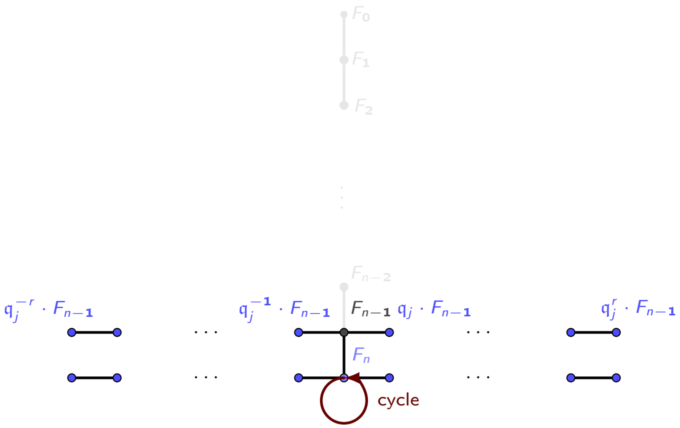
Chain recovery



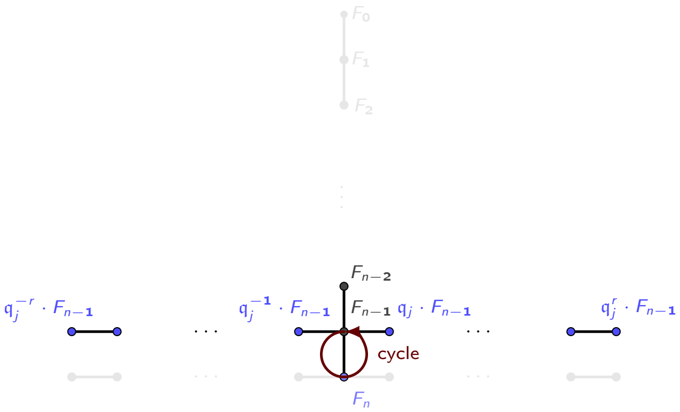
Chain recovery



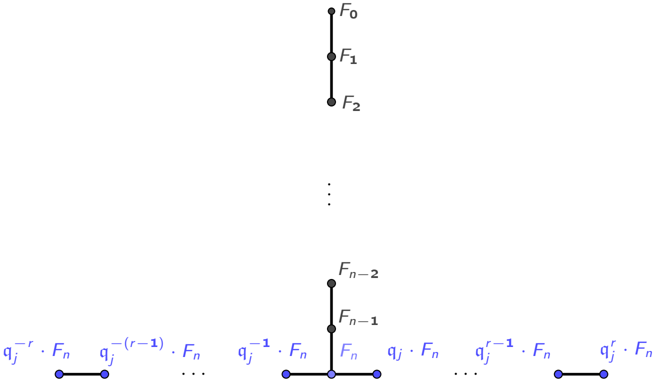
Chain recovery



Chain recovery



Chain recovery



Our contribution: a lattice reduction to find oriented endomorphisms

- We look for $\beta \in \mathcal{O}_n \setminus \mathcal{O}_{n+1}$ such that $\iota'_n(\beta)$ is easy to compute.
- We look for:

$$\beta\mathcal{O}_n = \prod_{j=1}^{t} (\mathfrak{q}_j \cap \mathcal{O}_n)^{e_j}$$

with $e_1, \cdots, e_t \in [\![-2r \ ; \ 2r]\!]$, so that $\iota'_n(\beta)$ can be inferred from:

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

- We look for short vectors (of infinity norm $\leq 2r$) in the relations lattice:

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

Our contribution: a lattice reduction to find oriented endomorphisms

- The relations lattice L can be computed in polynomial time (in n and t) because discrete logarithms are easy to compute in $\mathrm{Cl}(\mathcal{O}_n)$.

Our contribution: a lattice reduction to find oriented endomorphisms

- The relations lattice L can be computed in polynomial time (in n and t) because discrete logarithms are easy to compute in $\mathrm{Cl}(\mathcal{O}_n)$.

Lemma

Heuristically, we have:

$$\left(1 - \frac{\log\log(t)}{t}\right) \frac{|\,\mathrm{Cl}(\mathcal{O}_n)|^{1/t}}{2} \leq \lambda_1^{(\infty)}(L) \leq \left(1 + \frac{\log\log(t)}{t}\right) \frac{|\,\mathrm{Cl}(\mathcal{O}_n)|^{1/t}}{2}$$

Our contribution: a lattice reduction to find oriented endomorphisms

- The relations lattice L can be computed in polynomial time (in n and t) because discrete logarithms are easy to compute in $\mathrm{Cl}(\mathcal{O}_n)$.

Lemma

Heuristically, we have:

$$\left(1-\frac{\log\log(t)}{t}\right)\frac{|\,\mathrm{Cl}(\mathcal{O}_n)|^{1/t}}{2} \leq \lambda_1^{(\infty)}(L) \leq \left(1+\frac{\log\log(t)}{t}\right)\frac{|\,\mathrm{Cl}(\mathcal{O}_n)|^{1/t}}{2}$$

- If the key space:

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

covers $\mathrm{Cl}(\mathcal{O}_n)$, then $|\,\mathrm{Cl}(\mathcal{O}_n)| \leq (2r+1)^t$ and:

$$\lambda_1^{(\infty)}(L) < 2r$$

- Finding a short vector is exponential but practical with BKZ.

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
```

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

Can we scale up the attack?

Testing lattice reduction: $\ell = 2$, $n = 256, t = 74$, $r = 5$ and $K = \mathbb{Q}(i)$.

- Relations lattice computation: 1h04.
- Finding a short vector with BKZ: 0.5s.
- Shortest vector:

$$\begin{aligned} u :=(&-4, 1, 4, 4, -3, 1, 3, 5, 5, 2, 9, 5, 3, 5, -1, 5, -7, 2, -3, 5, 3, -3, 2,\\ &0, 2, 2, 0, -6, -2, -2, -9, 0, -6, 4, 1, -2, 1, 0, 7, 6, -2, -5, -3, -4,\\ &6, -1, 0, -3, -2, -3, 2, 6, 0, 6, -8, -3, -2, -3, 4, 4, -3, -5, 1, 0,\\ &0, 1, -1, 0, 5, -1, -1, 1, -2, -4) \end{aligned}$$

$\|u\|_\infty = 9 < 2r$.

Countermeasures:

- **Method 1:** increase t (and n) to make it computationally hard to find short vectors.
- **Method 2:** increase n to make sure that $(2r+1)^t \ll |\mathrm{Cl}(\mathcal{O}_n)|$, so that:

$$\lambda_1^{(\infty)}(L) \geq \left(1 - \frac{\log\log(t)}{t}\right) \frac{|\mathrm{Cl}(\mathcal{O}_n)|^{1/t}}{2} > 2r$$

Countermeasures:

- **Method 1:** increase t (and n) to make it computationally hard to find short vectors.
- **Method 2:** increase n to make sure that $(2r+1)^t \ll |\operatorname{Cl}(\mathcal{O}_n)|$, so that:

$$\lambda_1^{(\infty)}(L) \geq \left(1 - \frac{\log\log(t)}{t}\right) \frac{|\operatorname{Cl}(\mathcal{O}_n)|^{1/t}}{2} > 2r$$

- Drawbacks of method 1:
  - Increases the protocol complexity by a lot.
  - Diversity: the security relies on a lattice problem.

Countermeasures:

- **Method 1:** increase t (and n) to make it computationally hard to find short vectors.
- **Method 2:** increase n to make sure that $(2r+1)^t \ll |\operatorname{Cl}(\mathcal{O}_n)|$, so that:

$$\lambda_1^{(\infty)}(L) \geq \left(1 - \frac{\log\log(t)}{t}\right) \frac{|\operatorname{Cl}(\mathcal{O}_n)|^{1/t}}{2} > 2r$$

- Drawbacks of method 1:
  - Increases the protocol complexity by a lot.
  - Diversity: the security relies on a lattice problem.
- Drawback of method 2: reduces the key space:

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

This impedes other cryptographic constructions.

Conclusion

To sum up: Our attack significantly undermines OSIDH:

- Either OSIDH becomes an inefficient protocol based on a lattice reduction problem.
- Or it no longer satisfies the hypothesis of a cryptographic group action (key space too small).

To sum up: Our attack significantly undermines OSIDH:

- Either OSIDH becomes an inefficient protocol based on a lattice reduction problem.
- Or it no longer satisfies the hypothesis of a cryptographic group action (key space too small).

Future works:

- Improve the protocol implementation to scale up the attack.
- Find a complete cryptanalysis (without countermeasures).
- Or look for other constructions with the OSIDH framework that can work with a small key space.

Questions