Swissogeny Day 5, EPFL, 26th of November 2025

On the active security of the PEARL-SCALLOP group action

Joint with Tako Boris Fouotsa, Marc Houben, Gioella Lorenzon and Parsa Tasbihgou

Ryan Rueger
IBM Research Zurich & Technical University of Munich

This work

We describe an active attack against isogeny class-group actions by orders with non-smooth conductor (Active = No interactive choices made)

With just a handful (*e.g.* 3) of queries to a static CDH-oracle (Somewhat natural in threshold settings) we significantly reduce both the classical and quantum security of the PEARL-SCALLOP group action

Key idea is to query the oracle on a pre-determined set of curves that are not prmitively oriented, reducing the problem to much smaller vectorisation problems

We describe countermeasures to our attack in two different flavours: one using only the group action, and one using a HD division algorithm

Oriented Elliptic Curves

Some definitions

Let $K = \mathbb{Q}(\sqrt{d_K})$ be an imaginary quadratic number field

A K-orientation on $E/\mathbb{F}_{p^n}$ is a morphism of rings $\iota : K \to \mathrm{End}^0(E) = \mathrm{End}(E) \otimes \mathbb{Q}$

The preimage $\mathcal{O}^{\mathrm{pr}}(\iota) = \iota^{-1}(\mathrm{End}(E))$ is an order inside $\mathcal{O}_K$

We say that ι is an primitive $\mathcal{O}^{\mathrm{pr}}$-orientation
...and just an $\mathcal{O}$-orientation for every order $\mathcal{O} \subseteq \mathcal{O}^{\mathrm{pr}}(\iota)$

When p does not split in K, then there exist $\mathcal{O}_K$-oriented elliptic curves $E/\mathbb{F}_q$

Every non-scalar endomorphism ω of E induces an orientation ι_ω on E by $K = \mathbb{Q}(\sqrt{\mathrm{disc}(\omega)})$ by sending $\omega \mapsto \omega$

This is how we usually encode orientations in practice

Oriented Isogenies

Some definitions

Let E be K-oriented by ι

An isogeny $\varphi : E \to E'$ induces a K-orientation on E'

$$\iota^*(\alpha) = \varphi\iota(\alpha)\hat{\varphi} \otimes \frac{1}{\deg(\varphi)}$$

(When p does not split in K) Invertible ideals $\mathfrak{a} \subseteq \mathcal{O}$ give rise to oriented isogenies $\varphi_\mathfrak{a}$ between the $\mathcal{O}_K$-oriented curves with kernels

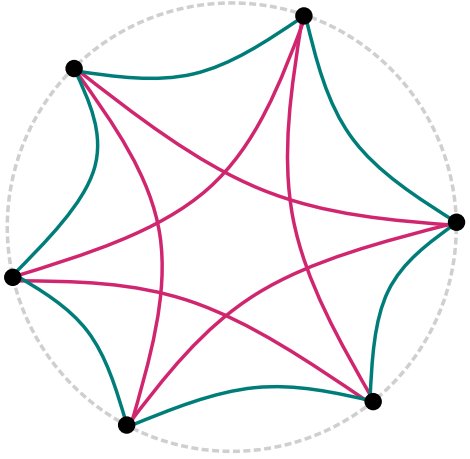
$$\ker(\varphi_\mathfrak{a}) = \bigcap_{a \in \mathfrak{a}} \ker(a) = E[\mathfrak{a}]$$

These isogenies satisfy $\ker(\varphi_\mathfrak{a}\varphi_\mathfrak{b}) = E[\mathfrak{a}\mathfrak{b}]$ and give rise to the isogeny class group action by $\mathcal{O}_K$

This action is free and has at most two orbits

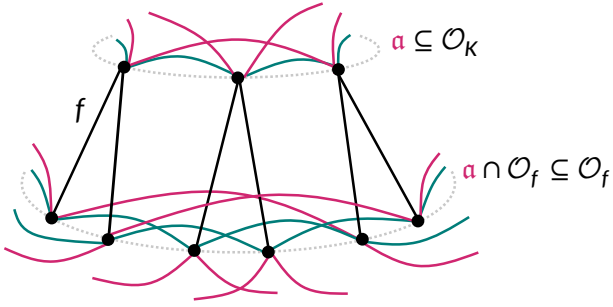
Oriented Isogenies: The surface

(Invertible) Ideals $\mathfrak{a}$, $\mathfrak{b} \subseteq \mathcal{O}_K$ give rise to isogenies



Oriented Isogenies: The volcano

When f splits in $\mathcal{O}_K$, there are $f - 1$ descending isogenies from each curve

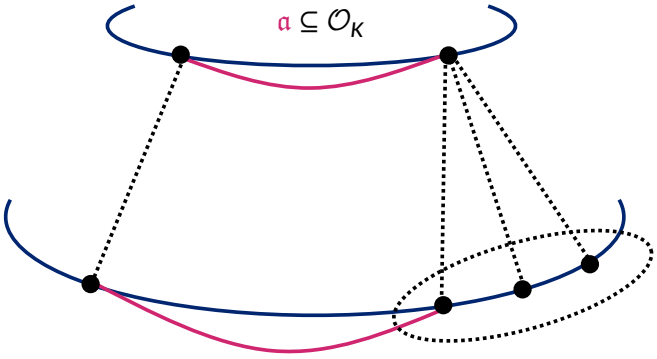


The curves below are primitvely oriented by $\mathcal{O}_f \subseteq \mathcal{O}_K$, the order of conductor f

This gives an action $\mathrm{Cl}(\mathcal{O}_f)$ on the lower curves (this action is also free and has at most two orbits)

The class number of $\mathcal{O}_f$ is $(f - 1)$ times the class number of $\mathcal{O}_K$

Oriented Isogenies: Compatibility of the action



Extension $\mathfrak{b} \mapsto \mathfrak{b}\mathcal{O}_K$ gives a surjective map $\mathrm{Cl}(\mathcal{O}_f) \to \mathrm{Cl}(\mathcal{O}_K)$

The kernel k_i of this map acts trivially on siblings

PEARL-SCALLOP

SCALLOP constructs a group action by using this volcano structure

Here, the discriminant is $d_K = -1$ and f a big prime

However, it is not enough to know just the class number, one also needs to compute the class group structure

This involves lattice reduction, which is feasible, yet still subexponential cost in f

Moreover, there are restrictions on f to allow the orienting endomorphisms to be efficiently represented

This leaves high security parameters ($\log_2(\text{disc})\mathcal{O}_f)) \approx 2000/4000$) out of reach

PEARL-SCALLOP resolves these issues by using a discriminant d_K of 256 bits, and a conductor $f = f_1 \cdots f_r$ that is the product of a few large primes (*e.g.* 128 bits)

The Static-CDH Oracle

Our attack uses the following Static CDH-Oracle

$$\mathcal{A}^{\mathfrak{a}}(E) = [\mathfrak{a}] * E = E^{\mathfrak{a}}$$

This is very strong, but appears naturally in threshold settings (2019/1288)

Algorithm 1: Threshold variant of the group action computation.

Input : $E_0 \in \mathcal{E}$, set of participants S.
Output: $[s]E_0$.

Set $E \leftarrow E_0$.
foreach $i \in S$ **do**
    If $E \notin \mathcal{E}$, participant $\mathcal{P}_i$ outputs $\perp$ and the algorithm stops.
    Participant $\mathcal{P}_i$ outputs $E \leftarrow \left[s_i \cdot L_{0,i}^{S}\right] E$.
return E.

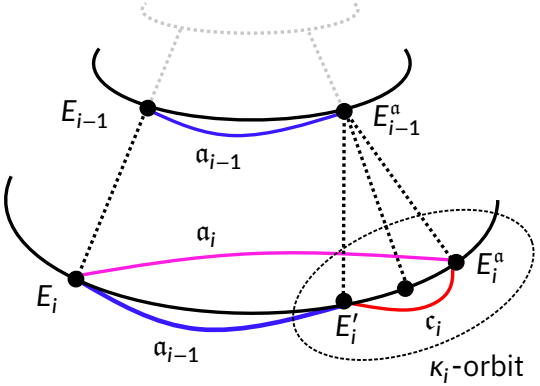
The attack in one slide

Suppose the conductor is $f = f_1 \cdots f_r$

Pre-compute some curves (E_i, ι_i) such that ι_i is a primitive $\mathcal{O}_{f_1 \cdots f_i}$-orientation

Query the oracle on (E_i, ι_i) to obtain $(E^{\mathfrak{a}}, \iota_i^{\mathfrak{a}})$ for $i = 1, \ldots, r$ (Online)

Recover $\mathfrak{a}$ by doing smaller vectorisations (Offline)



Cost of the attack

Vectorisation on the surface

Classical cost $O(\sqrt{|\mathrm{Cl}(\mathcal{O}_K)|})$ group operations using meet-in-the-middle.

Quantum cost subexponential Kuperberg applied to group of size $|\mathrm{Cl}(\mathcal{O}_K)|$

Vectorisation inside the orbits

Classical cost $O(\sqrt{f_i})$ group operations using meet-in-the-middle.

Quantum cost subexponential Kuperberg applied to group of size f_i

PEARL-SCALLOP-1024

$|\mathrm{Cl}(\mathcal{O}_K)| \sim 2^{128}$, $f_i \sim 2^{128}$ and $f = f_1 \cdots f_3$

...so the attack requires 4 $\mathcal{A}^{\mathfrak{a}}$ oracle calls, and classical effort of 2^{64} group actions

PEARL-SCALLOP-{2048,4096}

$|\mathrm{Cl}(\mathcal{O}_K)| \sim 2^{128}$, $f_i \sim \{2^{300}, 2^{640}\}$ and $f = f_1 \cdots f_7$

Since PEARL-SCALLOP target 128 bits of classical security, this does not constitute an attack

Countermeasures: Verifying Primitivity of Orientations

Validation Given a K-oriented curve (E, ι) and an order $\mathcal{O} \subseteq \mathcal{O}_K$, how does one verify that ι is a primitive $\mathcal{O}$-orientation, *i.e.* that $\mathcal{O}^{\mathrm{pr}}(\iota) = \mathcal{O}$?

Recall In practice, orientations are encoded as an endomorphisms ω on E, *i.e.* $\iota = \iota_\omega$

K-Orientation If $d_K \mid \mathrm{disc}(\omega)$, then ι is a K-orientation
$\mathcal{O}$-Orientation If $\mathrm{disc}(\omega) = f^2 d_K = \mathrm{disc}(\mathcal{O})$, then ι is a $\mathcal{O}$-orientation

So the first step is to verify that $\mathrm{disc}(\omega)$ matches the prescribed value $f^2 d_K$

Countermeasures: Verifying the discriminant

Given an endomorphism ω of E and a value d, how do we verify that $\mathrm{disc}(\omega) = d$? We assume ω is given in efficient representation, and so $\deg(\omega)$ is assumed to be known

Hence verifying the value of the discriminant $\mathrm{disc}(\omega) = \mathrm{tr}(\omega)^2 - 4\deg(\omega) \stackrel{!}{=} f^2 d_K$ amounts to verifying the value of the trace $\mathrm{tr}(\omega)$

Lemma Let ω is an endomorphism on E and R a point of order at least $\sqrt{\deg(\omega)} + 1$. If $\omega^2(R) + [t]\omega(R) + \deg(\omega) = 0$, then $t = \pm\mathrm{tr}(\omega)$

Applying this lemma to PEARL-SCALLOP and reusing reusing endomorphism evaluations, we can verify the discriminant of the given endomorphism using only one additional pairing computation

Countermeasures: Using the group action

Is the curve (E, ι) primitively oriented by $\mathcal{O}$?

Let $\mathcal{O}$ have conductor $f = f_1 \cdots f_r$
The orientation is primitive, if it cannot be extended to any order $\mathcal{O}_{f/f_i}$ with conductor $\mathcal{O}_{f/f_i}$

This can be tested, by acting on E by an invertible $\mathcal{O}$-ideal $\mathfrak{T}$ which becomes principal in $\mathcal{O}_{f/f_i}$ by extension $\mathfrak{T}\mathcal{O}_{f/f_i}$ (*i.e.* an element of $\ker(\mathcal{O}_f \to \mathcal{O}_{f/f_i})$)

If the action by $\mathfrak{T}$ is non-trivial for all i, then E is primitively oriented

In the PEARL-SCALLOP CSIDH-1024 parameters, $r = 3$, and so the action becomes slower by a factor of 4
By enforcing that the class group is cyclic at parameter generation time, $\mathfrak{T}$ ideals are easier to pre-compute because $\ker(\mathcal{O}_f \to \mathcal{O}_{f/f_i}) \cong \mathbb{F}_{f_i}^\times$

Can we do better?

Countermeasures: Using a HD division algorithm

Is the curve (E, ι_ω) primitively oriented by $\mathcal{O}$?
We assume that the trace has been verified, and that the norm is known, *i.e.* that $\mathbb{Z}[\omega] = \mathcal{O}$ with $\mathrm{disc}(\omega) = f^2 d_0$

Lemma ι_ω is a primitive $\mathbb{Z}[\omega]$-orientation if and only if $\omega_0 = 2\omega - \mathrm{tr}(\omega)$ is not divisible by 2ρ for any prime divisor ρ of f

This is because $\omega_0/2\rho$ viewed as an algebraic integer generates the index-ρ superorder.

Countermeasures: Using a HD division algorithm

In general testing scalar division of an n-isogeny (in efficient representation) requires computing an 8-dimensional N-isogeny

For PEARL-SCALLOP-1024

The parameters are chosen by picking a random prime a of size 2^{128} and sampling $f_1 = a, f_2 = 2^{e+1} - a, f_3 = (2^{e+1} + a)/3$ until all f_i are prime

The degree $\deg(\omega_0 = 2\omega - \mathrm{tr}(\omega) = f_1^2 f_2^2 f_3^2 D_K \sim 2^{2e}$

We look for a so that $2^\bullet - f_1^2 f_2^2 f_3^2 D_K / f_i^2 = x_i^2 + y_i^2$
This requires splitting the HD isogeny, because $2^\bullet \geq 2^e$

Since $f = f_1 \cdot f_2 \cdot f_3$, this requires computing $2r$ 4-dimensional 2^{384} over a field of characteristic of 1024 bits
Using timings from {qt-,}PEGASIS, this should take around 30 seconds in total (a 50% overhead)

Thank you for your attention

Slides https://rueg.re/swissogeny4