SCALLOP-HD: group action from 2-dimensional isogenies

Mingjie Chen, Antonin Leroux, Lorenz Panny

Université Libre de Bruxelles

March 13, 2024

Game Goal

Construct a **scalable** quantum safe effective group action (**EGA**).

- **EGA**: a group action $G \curvearrowright S$ that is **effective**
  - $g^n \star s$ can be computed efficiently where $g \in G$ is a generator, $n \in \mathbb{Z}_{\geq 0}$ and $s \in S$.
- **scalable**: we can scale the EGA to bigger parameters

What has been achieved so far ($\mathrm{Cl}(\mathfrak{O}) \curvearrowright \mathcal{S}_{\mathfrak{O}}(p)$)

CSIDH [Castryck-Lange-Martindale-Panny-Renes 2018]

- $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$, set elements are j-invariants of $E/\mathbb{F}_p$
- REGA: $\prod \mathfrak{l}_i^{e_i}$

CSI-FiSh [Beullens-Kleinjung-Vercauteren 2019]

- $\mathfrak{O}$ and set elements are same as in CSIDH
- EGA: $\mathfrak{g}^e$
- REGA $\rightarrow$ EGA

  Offline:

  - $\mathrm{Cl}(\mathfrak{O})$;
  - $\mathcal{L}$ lattice of relations (r_i's such that $[\mathfrak{l}_i] = [\mathfrak{g}^{r_i}]$)
  - lattice reduction

  Online:

  - approximate-CVP $\Rightarrow \mathfrak{g}^e = \prod_{i=1}^{i=n} \mathfrak{l}_i^{e_i}$
  - class group action evaluation

SCALLOP [De Feo-Fouotsa-Kutas-Leroux-Merz-Panny-Wesolowski 2023]

- $\mathfrak{O} = \mathbb{Z}[f\sqrt{-d}]$, set elements are $(E, \iota) \in \mathcal{S}_{\mathfrak{O}}(p)$
- EGA (same strategy as CSI-FiSh)

Scalability

Problem

*(**Vectorization**) Given $x, y \in S$, find $g \in G$ such that $y = g \star x$.*

- Since 2019, a series of papers studied the quantum security of CSIDH, leaving whether CSIDH-512 and CSIDH-1024 achieve **NIST level 1 security** under debate.
- It is desirable to have an efficient isogeny-based EGA at higher security level.
- In terms of scalability, CSI-FiSh was able to scale to CSIDH-512, and SCALLOP managed to scale to achieve the security level of CSIDH-512 and CSIDH-1024. [1]

[1] Here we model the quantum security of SCALLOP as that of CSIDH when the underlying class groups have the same size.

SCALLOP revisit

- **The quadratic order:** $\mathbb{Z}[f\sqrt{-d}]$

  $$\#\mathrm{Cl}(\mathfrak{O}) = \left(f - \left(\frac{-d}{f}\right)\right)\frac{1}{|\mathbb{Z}[-d]^*|/2} \text{ when } \#\mathrm{Cl}(\mathbb{Z}[\sqrt{-d}]) = 1.$$

  It's easy to find a generator of such class groups!

- **The set element:** (E, P, Q)
  P, Q give rise to the kernel of a generator[2] α of $\mathfrak{O}$ of norm $L_1^2 L_2$ where L_1 and L_2 are two smooth coprime integers.

- **The group action computation:** **involved**

- **Scaling bottleneck:** **Solving discrete logarithm in $\mathrm{Cl}(\mathfrak{O})$.**

[2] meaning $\mathfrak{O} = \mathbb{Z}[\alpha]$

The "HD" Rush

Let φ, φ' be a-isogenies and ψ, ψ' be b-isogenies for integers a, b that satisfy the commutative diagram:

$$\begin{tikzcd} E_1' \arrow[r, "\varphi'"] & E_2' \\ E_1 \arrow[u, "\psi"] \arrow[r, "\varphi"] & E_2 \arrow[u, "\psi'"'] \end{tikzcd}.$$

Define $F : E_2 \times E_1' \longrightarrow E_1 \times E_2'$ by the matrix form $\begin{pmatrix} \hat{\varphi} & -\hat{\psi} \\ \psi' & \varphi' \end{pmatrix}$.
F is a d-isogeny between abelian surfaces with $d = a + b$.

If $\ker \varphi \cap \ker \psi = \{0\}$,

$$\ker(F) = \{(\varphi(x), \psi(x)) \mid x \in E_1[d]\}.$$ [Kani97']

SCALLOP-HD???

Can we come up with a "better" representation of orientations than that in SCALLOP using the idea of high dimension representation?

Yes, and this leads to several improvements over SCALLOP.

Tiny remarks

Representing an $\mathfrak{O}$-orientation ι on E
$\Leftrightarrow$ representing an endomorphism $\theta \in \iota(\mathfrak{O})$ such that $\mathbb{Z}[\theta] \cong \mathfrak{O}$

Representing an endomorphism $\theta \in \mathrm{End}(E)$
$\Leftrightarrow$ representing the $\mathbb{Z}[\theta]$-orientation on E induced by θ

2dim-representation of orientations and endomorphisms

Definition

Let $\mathfrak{O}$ be an imaginary quadratic order with discriminant $D_{\mathfrak{O}}$. Given an $\mathfrak{O}$-oriented supersingular elliptic curve (E, ι), take any $\omega \in \mathfrak{O}$ such that $\mathfrak{O} = \mathbb{Z}[\omega]$ and define $\omega_E := \iota(\omega)$. Let $\beta \in \mathfrak{O}$ such that $n(\omega) + n(\beta) = 2^e$ and $\gcd(n(\beta), n(\omega)) = 1$. Let P, Q be a basis of $E[2^e]$. Then the tuple $(E, \omega, \beta, P, Q, \omega_E(P), \omega_E(Q))$ is called a *2*dim-**representation of** (E, ι).

An automatic isogeny diamond

Given a 2dim-representation $(E, \omega, \beta, P, Q, \omega_E(P), \omega_E(Q))$ of (E, ι), we immediately have the following isogeny diamond.

$$\begin{tikzcd} E \arrow[r, "\omega_E"] & E \\ E \arrow[u, "\beta_E"] \arrow[r, "\omega_E"] & E \arrow[u, "\beta_E"'] \end{tikzcd}$$

This defines an isogeny $F : E^2 \to E^2$ given by the matrix form

$$F := \begin{pmatrix} \hat{\omega}_E & -\hat{\beta}_E \\ \beta_E & \omega_E \end{pmatrix}$$

If $\ker \omega_E \cap \ker \beta_E = \{0\}$, then

$$\ker(F) = \{(\omega_E(x), \beta_E(x)) \mid x \in E[2^e]\}.$$

Finding 2dim-representations

Proposition

Let $\mathfrak{O}$ be an imaginary quadratic order of discriminant $D_{\mathfrak{O}} \equiv 5 \bmod 8$, then any $(E, \iota) \in \mathcal{S}_{\mathfrak{O}}(p)$ admits a 2dim-representation.

- It suffices to show that when e is big enough, we can always find $\omega, \beta \in \mathfrak{O}$ such that

$$\mathfrak{O} = \mathbb{Z}[\omega],\ \gcd(n(\omega), n(\beta)) = 1,\ n(\omega) + n(\beta) = 2^e.$$

- $\omega = x + \frac{D_{\mathfrak{O}} + \sqrt{D_{\mathfrak{O}}}}{2}$ and $\beta = y + z\frac{D_{\mathfrak{O}} + \sqrt{D_{\mathfrak{O}}}}{2}$ for some integers x, y, z. Therefore, it suffices to finding an integer solution of the following equation:

$$(2x + D_{\mathfrak{O}})^2 + (2y + D_{\mathfrak{O}} z)^2 = 2^{e+2} + D_{\mathfrak{O}}(z^2 + 1).$$

- We ensure that $\gcd(n(\omega), n(\beta)) = 1$ since $n(\omega) = x^2 + D_{\mathfrak{O}} x + \frac{D_{\mathfrak{O}}(D_{\mathfrak{O}} - 1)}{4}$ is **odd** when $D_{\mathfrak{O}} \equiv 5 \bmod 8$.

Proof continued

$$(2x + D_{\mathfrak{O}})^2 + (2y + D_{\mathfrak{O}} z)^2 = 2^{e+2} + D_{\mathfrak{O}}(z^2 + 1).$$

Heuristic

Let $e, D_{\mathfrak{O}}$ be as above. If z is sampled as random integers, then the integers $2^{e+2} + D_{\mathfrak{O}}(1 + z^2)$ behave like random integers of the same size that are either congruent to $1 \bmod 4$ or equal to 2 times an integer that is equal to 1 modulo 4.

Finding 2dim-representations

Proposition

Let $\mathfrak{O}$ be an imaginary quadratic order of discriminant $D_{\mathfrak{O}} \equiv 5 \bmod 8$, then any $(E, \iota) \in \mathcal{S}_{\mathfrak{O}}(p)$ admits a 2dim-representation.

- It suffices to show that when e is big enough, we can always find $\omega, \beta \in \mathfrak{O}$ such that

$$\mathfrak{O} = \mathbb{Z}[\omega],\ \gcd(n(\omega), n(\beta)) = 1,\ n(\omega) + n(\beta) = \cancel{2^e}\mathbf{N}.$$

- $\omega = x + \frac{D_{\mathfrak{O}} + \sqrt{D_{\mathfrak{O}}}}{2}$ and $\beta = y + z\frac{D_{\mathfrak{O}} + \sqrt{D_{\mathfrak{O}}}}{2}$ for some integers x, y, z. Therefore, it suffices to finding an integer solution of the following equation:

$$(2x + D_{\mathfrak{O}})^2 + (2y + D_{\mathfrak{O}} z)^2 = \cancel{2^{e+2}}\mathbf{4N} + D_{\mathfrak{O}}(z^2 + 1).$$

- We ensure that $\gcd(n(\omega), n(\beta)) = 1$ since $n(\omega) = x^2 + D_{\mathfrak{O}} x + \frac{D_{\mathfrak{O}}(D_{\mathfrak{O}} - 1)}{4}$ is **odd** when $D_{\mathfrak{O}} \equiv 5 \bmod 8$.

Applications

- It's recently used in *[Leroux 2023]* to provide a new algorithm to perform the Deuring correspondence using isogenies in dimension 2.
- It can be used in the endomorphism division algorithm (*[Robert 2022]*,*[Merdy-Wesolowski 2023]*) to replace isogeny computations in dimension $4/8$ to computations in dimension 2.

Group action computation

Let

- $(E, \omega, \beta, P, Q, \omega_E(P), \omega_E(Q))$ be a 2dim-representation of (E, ι)
- $\mathfrak{a}$ an invertible $\mathfrak{O}$-ideal such that $2 \nmid \mathrm{Norm}(\mathfrak{a})$

Let $\phi_{\mathfrak{a}}$ be the isogeny with kernel $E[\mathfrak{a}]$. To calculate a 2dim-representation for $\mathfrak{a} \star (E, \iota) = (E_{\mathfrak{a}}, \iota_{\mathfrak{a}})$, we can keep the same ω and β. Since $\gcd(n(\mathfrak{a}), 2) = 1$, $\{\phi_{\mathfrak{a}}(P), \phi_{\mathfrak{a}}(Q)\}$ form a basis of $E_{\mathfrak{a}}[2^e]$. By definition,

$$\iota_{\mathfrak{a}}(\omega)(\phi_{\mathfrak{a}}(P, Q)) = \frac{1}{n(\mathfrak{a})}\phi_{\mathfrak{a}} \circ \omega_E \circ \hat{\phi}_{\mathfrak{a}}(\phi_{\mathfrak{a}}(P, Q)) = \phi_{\mathfrak{a}}(\omega_E(P, Q)).$$

Let $\{R, S\}$ be an arbitrary basis of $E_{\mathfrak{a}}[2^e]$, then $\iota_{\mathfrak{a}}(\omega)(R, S)$ can be recovered from $\iota_{\mathfrak{a}}(\omega)(\phi_{\mathfrak{a}}(P, Q))$ efficiently.

SCALLOP-HD!!!

- Quadratic orders $\mathfrak{O} = \mathbb{Z}[f\sqrt{-d}]$ such that $D_{\mathfrak{O}} \equiv 5 \bmod 8$

- $(E, \iota) \in \mathcal{S}_{\mathfrak{O}}(p)$ is represented by 2dim-representation $(E, \omega, \beta, P, Q, \omega_E(P), \omega_E(Q))$

  – We fix ω, β in $(E, \omega, \beta, P, Q, \omega_E(P), \omega_E(Q))$. Moreover, if we use a deterministic algorithm to compute a basis of $E[2^e]$, then the representation can be given by $(E, \omega_E(P), \omega_E(Q))$.

Important parameters

- Choice of f: ensure that $\#\mathrm{Cl}(\mathfrak{O}) = \left(f - \left(\frac{-d}{f}\right)\right) \frac{1}{|\mathfrak{O}_0^*|/2}$ is as smooth as possible.
- Choice of field characteristic p:
  - To efficiently represent the orientation, we require that 2^e-torsion is defined over $\mathbb{F}_{p^2}$.
  - For efficient computation of the group action, we also require to have the $\prod_{1 \le i \le n} \ell_i$-torsion defined over $\mathbb{F}_{p^2}$.

$$\implies p = c 2^e \prod_{i=1}^{n} \ell_i \pm 1,$$

where c is a small cofactor.

Generating a starting curve

We find $(E, \iota) \in \mathcal{S}_{\mathbb{Z}[f\sqrt{-d}]}(p)$ by computing a descending isogeny φ_f of degree f from $(E_0, \iota_0) \in \mathcal{S}_{\mathbb{Z}[\sqrt{-d}]}(p)$. To obtain 2dim-representation of (E, ι):

$$\begin{tikzcd} E_0 \arrow[loop above, "\gamma"] \arrow[d, bend right, "\varphi_f"'] \arrow[d, bend left, "\psi"] \\ E \end{tikzcd}$$

- $\deg \gamma \text{``}=\text{''} f \cdot 2^{e/2} \prod \ell_i \approx p$, so $\gamma \in \mathcal{O}_0$ can be found efficiently with FullRepresentInteger *[De Feo-Leroux-Longa-Wesolowski 2023]*.
  (note that the first equality is not exactly true, an exhuastive search step is involved)
- Being able to evaluate γ and ψ allows evaluation of φ_f on a basis of $E_0[2^{e/2}]$.
- This implies evaluation of ω_E on a basis of $E[2^{e/2}]$, which allows one to evaluate ω_E on a basis of $E[2^e]$ *[Dartois-Leroux-Robert-Wesolowski 2023]*.

Remaining steps

- **Offline**:
  - Class group computation is efficient.
  - Lattice of relation can be computed in polynomial time since $\mathrm{Cl}(\mathfrak{O})$ has powersmooth order.
  - Lattice reduction algorithm remains the same.
- **Online**:
  - The CVP step remains the same.
  - A new formula to compute the class group action.

A remark on security

$$\begin{tikzcd} E_0 \arrow[d, "\varphi_f"] \\ E \end{tikzcd}$$

A polynomial time quantum algorithm exists to compute $\mathrm{End}(E)$ given the evaluation of φ_f on points of powersmooth order *[Chen-Imran-Ivanyos-Kutas-Leroux-Petit 2023]*.

Therefore, the security of SCALLOP(-HD) boils down to:

Can we use the effective orientation ω_E revealed in SCALLOP(-HD) to evaluate φ_f?

Another remark on security

Let

- N to be a product of split primes in $\mathfrak{O}_0 = \mathbb{Z}[\sqrt{-d}]$
- P, Q be two generators of the eigenspaces of ω_0 in $E_0[N]$
- T, S be two generators of the eigenspaces of ω_E in $E[N]$

key observation: we know $\varphi_f(P, Q)$ up to scalars as eigenspaces of ω_0 are mapped to eigenspaces of ω_E by φ_f

What about applying FESTA attack in [Castryck-Vercauteren 2023]?

our conclusion: it's hard as we need to find $\sigma \in \mathrm{End}(E_0)$ whose matrix of action on $\{P, Q\}$ is also diagonal

- see our paper for more discussions

Implementation and performance

Scalability We managed to compute the reduced lattice of relation for $D \approx 4096$ bits.
An issue We haven't finished generating a starting curve for 2048 and 4096, due to the lack of sufficiently general genus-2 isogeny libraries.

Performance

D	512	1024	2048	4096
f	254	508	1021	2043
n	74	100	200	300
p	1137	1909	tbf	tbf

Table: Bit-size for D, f, n and p.

	512	1024	2048 & 4096
SCALLOP	42 sec	15 min	—
SCALLOP-HD	88 sec	19 min	tbf

Table: Runtime for a single group action evaluation. Experiments run on an Intel Alder Lake CPU core clocked at 2.1 GHz. C++ implementation of SCALLOP compared with SageMath implementation of SCALLOP-HD.

Conclusion and future work

Conclusion:

- We introduce the notation of 2dim-**representation** for representing orientations and endomorphisms. This is interesting in its own right.
- We present the **SCALLOP-HD group action**. Compared with SCALLOP:
  - it has **better scalability**,
  - the group action formula is **simpler**,
  - the efficiency of SCALLOP-HD can **at least compete**.

Future work:
Improve current implementation of the SCALLOP-HD group action.

Thank you!