SCALLOP-HD: group action from 2-dimensional isogenies

Leuven Isogeny Days 4

Mingjie Chen, Antonin Leroux

University of Birmingham

October 11, 2023

"History" of group action ($\mathrm{Cl}(\mathfrak{O}) \curvearrowright \mathcal{S}_{\mathfrak{O}}(p)$) in isogeny-based cryptography

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]

- 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

OSIDH [Colò-Kohel 2020]

- Introduced the notion of orientation
- $\mathfrak{O} = \mathbb{Z}[2^n\sqrt{-1}]$
- Insecure for the parameter suggested [Dartois-De Feo 2022]

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

Scalability

Problem

*(***Vectorization***) Given $x, y \in X$, 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 overview

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

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

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

- **The set element:** (E, P, Q)
  P, Q give 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:

$$\begin{array}{ccc} E_1' & \xrightarrow{\varphi'} & E_2' \\ {\scriptstyle\psi}\uparrow & & \uparrow{\scriptstyle\psi'} \\ E_1 & \xrightarrow{\varphi} & E_2. \end{array}$$

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

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

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 orientation $\mathfrak{O}$-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 2dim-**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.

$$\begin{array}{ccc} E & \xrightarrow{\omega_E} & E \\ {\scriptstyle \beta_E}\uparrow & & \uparrow{\scriptstyle \beta_E} \\ E & \xrightarrow{\omega_E} & E \end{array}$$

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 $D_{\mathfrak{O}} \equiv 5 \bmod 8$.

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 (from [Merdy-Wesolowski 2023]) to replace isogeny computations in dimension 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 $\mathbb{F}_{p^2}$.

$$\implies p = c2^e \prod_{i=1}^{n} \ell_i \pm 1,$$

where c is a small cofactor.

Remaining steps

- An algorithm for **generating a starting curve** in $\mathcal{S}_{\mathfrak{O}}(p)$.

- **Offline**:
  - Class group computation is efficient.
  - Lattice of relation can be computed in polynomial time since $\mathrm{Cl}(\mathfrak{O})$ has smooth order.
  - Lattice reduction algorithm remains the same.

- **Online**:
  - The CVP step remains the same.
  - A new formula to compute the class group action.

Conclusion and future work

Conclusion:

- We introduce the notion of *2*dim-**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**.

Future work:

Implement SCALLOP-HD group action to see its efficiency. We **expect it to be more efficient than SCALLOP due to its simplicity**.

Thank you!