SCALLOP: scaling the CSI-FiSh

Luca De Feo   Tako Boris Fouotsa   Péter Kutas

Antonin Leroux   **Simon-Philipp Merz**   Lorenz Panny

Benjamin Wesolowski

May 2023

PKC 2023, Atlanta

Cryptographic group actions

Definition

A *group action* of a group G on a set X is a function

$$\star : G \times X \to X$$

- $e \star x = x$
- $(gh) \star x = g \star (h \star x)$

Cryptographic group actions

Definition

A *group action* of a group G on a set X is a function

$$\star : G \times X \to X$$

- $e \star x = x$
- $(gh) \star x = g \star (h \star x)$

- Vectorization prob.: given $x, y \in X$, find $g \in G$ s.t. $y = g \star x$
- Parallelization prob.: given $x, g \star x, h \star x$, find $(gh) \star x$

Cryptographic group actions

Definition

A *group action* of a group G on a set X is a function

$$\star : G \times X \to X$$

- $e \star x = x$
- $(gh) \star x = g \star (h \star x)$

- Vectorization prob.: given $x, y \in X$, find $g \in G$ s.t. $y = g \star x$
- Parallelization prob.: given $x, g \star x, h \star x$, find $(gh) \star x$

- Candidates for post-quantum Diffie-Hellman key exchange, e.g. reasonably efficient isogeny-based scheme CSIDH (NIKE)
- SCALLOP: a new isogeny-based group action

CSIDH: a restricted effective group action

- CSIDH is not an effective group action (EGA)!

CSIDH: a restricted effective group action

- CSIDH is not an effective group action (EGA)!

Caution

Evaluating group action $\mathfrak{g} \star E$ is not efficient for all group elements $\mathfrak{g} \in G$ and $E \in X$!

CSIDH: a restricted effective group action

- CSIDH is not an effective group action (EGA)!

Caution

Evaluating group action $\mathfrak{g} \star E$ is not efficient for all group elements $\mathfrak{g} \in G$ and $E \in X$!

Solution:

- Restrict group action to list of elements $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ spanning G such that $\mathfrak{l}_i \star E$ can be efficiently evaluated for every E
- Can evaluate action $\prod_i \mathfrak{l}_i^{e_i} \star E$ efficiently as long as exponents $(e_1, \ldots, e_n) \in \mathbb{Z}^n$ are sufficiently small

$\Rightarrow$ Restricted effective group action (REGA)

General strategy: REGA to EGA

Precomputation done once:

- Compute cardinality of acting group $|G|$
- Compute *lattice of relations* $\mathcal{L}$ of $\mathfrak{l}_i$, i.e. lattice spanned by vectors $(e_1, \dots, e_n)$ such that $\prod_i \mathfrak{l}_i^{e_i} \in \mathbb{Z}$ acts trivially on set X
- Compute reduced basis of $\mathcal{L}$ suitable to solve CVP instances efficiently

General strategy: REGA to EGA

Precomputation done once:

- Compute cardinality of acting group $|G|$
- Compute *lattice of relations* $\mathcal{L}$ of $\mathfrak{l}_i$, i.e. lattice spanned by vectors $(e_1, \ldots, e_n)$ such that $\prod_i \mathfrak{l}_i^{e_i} \in \mathbb{Z}$ acts trivially on set X
- Compute reduced basis of $\mathcal{L}$ suitable to solve CVP instances efficiently

Online phase to evaluate $\mathfrak{l}_1^e \star E$ (for all $e \in \mathbb{Z}$):

- Solve (approximate) CVP of $(e, 0, \ldots, 0)$ in $\mathcal{L}$ to find decomposition $\mathfrak{l}_1^e = \prod_i \mathfrak{l}_i^{e_i}$ with small exponents e_i
- Evaluate the restricted group action $\prod_i \mathfrak{l}_i^{e_i} \star E$

General strategy: REGA to EGA

Precomputation done once:

- Compute cardinality of acting group $|G|$
- Compute *lattice of relations* $\mathcal{L}$ of $\mathfrak{l}_i$, i.e. lattice spanned by vectors $(e_1, \dots, e_n)$ such that $\prod_i \mathfrak{l}_i^{e_i} \in \mathbb{Z}$ acts trivially on set X
- Compute reduced basis of $\mathcal{L}$ suitable to solve CVP instances efficiently

Online phase to evaluate $\mathfrak{l}_1^e \star E$ (for all $e \in \mathbb{Z}$):

- Solve (approximate) CVP of $(e, 0, \dots, 0)$ in $\mathcal{L}$ to find decomposition $\mathfrak{l}_1^e = \prod_i \mathfrak{l}_i^{e_i}$ with small exponents e_i
- Evaluate the restricted group action $\prod_i \mathfrak{l}_i^{e_i} \star E$

Caution

Depending on the group G, the precomputation might be computationally infeasible!

CSI-FiSh signature scheme [BKV19]

- Based on group action of CSIDH-512
- Precompute *lattice of relations* $\mathcal{L}$ for the generators used in CSIDH-512 using an index-calculus approach
- CSI-FiSh required a world-record class group computation to obtain the lattice for the smallest CSIDH parameters

CSI-FiSh signature scheme [BKV19]

- Based on group action of CSIDH-512
- Precompute *lattice of relations* $\mathcal{L}$ for the generators used in CSIDH-512 using an index-calculus approach
- CSI-FiSh required a world-record class group computation to obtain the lattice for the smallest CSIDH parameters

Caution

Computing the structure of the acting group for larger CSIDH parameters is infeasible with currently known algorithms.

CSI-FiSh signature scheme [BKV19]

- Based on group action of CSIDH-512
- Precompute *lattice of relations* $\mathcal{L}$ for the generators used in CSIDH-512 using an index-calculus approach
- CSI-FiSh required a world-record class group computation to obtain the lattice for the smallest CSIDH parameters

Caution

Computing the structure of the acting group for larger CSIDH parameters is infeasible with currently known algorithms.

Motivation

Introduce group action that solves the scaling issue of CSI-FiSh

(to some extent..)

Group actions on oriented curves

- Let $\mathfrak{O}$ be an imaginary quadratic order, e.g. $\mathbb{Z}[\sqrt{-p}]$
- Let X be the set of supersingular elliptic curves up to isomorphism such that $\mathfrak{O}$ embeds into their endomorphism ring
- Invertible ideals of $\mathfrak{O}$ act on X, principal ideals act trivially, i.e. group action by class group $\mathrm{Cl}(\mathfrak{O})$

$$\mathrm{Cl}(\mathfrak{O}) \times X \to X$$

- CSIDH: special case where $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$

Group actions on oriented curves

- Let $\mathfrak{O}$ be an imaginary quadratic order, e.g. $\mathbb{Z}[\sqrt{-p}]$
- Let X be the set of supersingular elliptic curves up to isomorphism such that $\mathfrak{O}$ embeds into their endomorphism ring
- Invertible ideals of $\mathfrak{O}$ act on X, principal ideals act trivially, i.e. group action by class group $\mathrm{Cl}(\mathfrak{O})$

$$\mathrm{Cl}(\mathfrak{O}) \times X \to X$$

- CSIDH: special case where $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$

Can we use different $\mathfrak{O}$?

How to represent and compute with different orientation?

SCALLOP: Precomputation

SCALable isogeny action based on Oriented supersingular curves with Prime conductor

Idea: can compute class number $|\mathrm{Cl}(\mathfrak{O})|$ for $\mathfrak{O}$ of the form $\mathbb{Z} + f\mathfrak{O}_0$ from class number $|\mathrm{Cl}(\mathfrak{O}_0)|$ and factorization of f

SCALLOP: Precomputation

SCALable isogeny action based on Oriented supersingular curves with Prime conductor

Idea: can compute class number $|\mathrm{Cl}(\mathfrak{O})|$ for $\mathfrak{O}$ of the form $\mathbb{Z} + f\mathfrak{O}_0$ from class number $|\mathrm{Cl}(\mathfrak{O}_0)|$ and factorization of f

- Take $\mathfrak{O}_0$ with $|\mathrm{Cl}(\mathfrak{O}_0)| = 1$
- Generate candidates for $\mathfrak{O}$ with smooth generator until
  - conductor f is prime (avoids factoring f)
  - class number $|\mathrm{Cl}(\mathfrak{O})|$ is reasonably smooth (asymptotically, $L_f(1/2)$ search for $L_f(1/2)$-smooth $|\mathrm{Cl}(\mathfrak{O})|$)

SCALLOP: Precomputation

SCALable isogeny action based on Oriented supersingular curves with Prime conductor

Idea: can compute class number $|\mathrm{Cl}(\mathfrak{O})|$ for $\mathfrak{O}$ of the form $\mathbb{Z} + f\mathfrak{O}_0$ from class number $|\mathrm{Cl}(\mathfrak{O}_0)|$ and factorization of f

- Take $\mathfrak{O}_0$ with $|\mathrm{Cl}(\mathfrak{O}_0)| = 1$
- Generate candidates for $\mathfrak{O}$ with smooth generator until
  - conductor f is prime (avoids factoring f)
  - class number $|\mathrm{Cl}(\mathfrak{O})|$ is reasonably smooth (asymptotically, $L_f(1/2)$ search for $L_f(1/2)$-smooth $|\mathrm{Cl}(\mathfrak{O})|$)
- Compute lattice of relations $\mathcal{L}$ by solving instances of discrete logarithm problem in $\mathrm{Cl}(\mathfrak{O})$

SCALLOP: Precomputation

SCALable isogeny action based on Oriented supersingular curves with Prime conductor

Idea: can compute class number $|\mathrm{Cl}(\mathfrak{O})|$ for $\mathfrak{O}$ of the form $\mathbb{Z} + f\mathfrak{O}_0$ from class number $|\mathrm{Cl}(\mathfrak{O}_0)|$ and factorization of f

- Take $\mathfrak{O}_0$ with $|\mathrm{Cl}(\mathfrak{O}_0)| = 1$
- Generate candidates for $\mathfrak{O}$ with smooth generator until
  - conductor f is prime (avoids factoring f)
  - class number $|\mathrm{Cl}(\mathfrak{O})|$ is reasonably smooth (asymptotically, $L_f(1/2)$ search for $L_f(1/2)$-smooth $|\mathrm{Cl}(\mathfrak{O})|$)
- Compute lattice of relations $\mathcal{L}$ by solving instances of discrete logarithm problem in $\mathrm{Cl}(\mathfrak{O})$
- Compute reduced basis of $\mathcal{L}$ using BKZ as in CSI-FiSh
- Generate a starting curve with $\mathfrak{O}$-orientation

SCALLOP: Online phase

- Generator of smooth norm of $\mathfrak{O}$ corresponds to endomorphism ω_E of smooth degree which we represented by kernels of two isogenies
- ω_E stabilizes kernels of isogenies used to compute group action

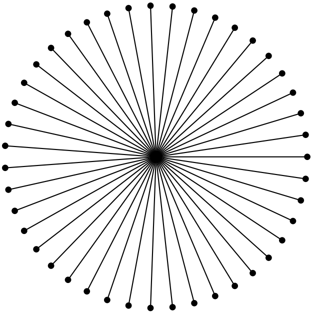

Figure: Isogeny volcano for $\mathfrak{O}$-oriented curves in SCALLOP.

SCALLOP: Online phase

- Generator of smooth norm of $\mathfrak{O}$ corresponds to endomorphism ω_E of smooth degree which we represented by kernels of two isogenies
- ω_E stabilizes kernels of isogenies used to compute group action
- Evaluate group action by transporting explicit orientation along the group action
- Computing explicit orientation leads to slowdown compared to CSI-FiSh with canonical orientation

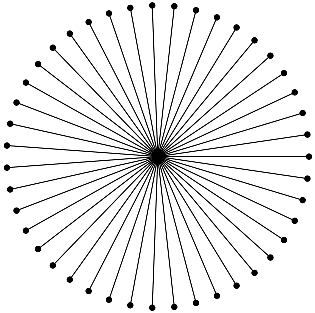

Figure: Isogeny volcano for $\mathfrak{O}$-oriented curves in SCALLOP.

Effective Group Actions: CSI-FiSh vs SCALLOP

CSI-FiSh

- $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$

SCALLOP

- $\mathfrak{O} = \mathbb{Z} + f\mathfrak{O}_0$, f prime

Effective Group Actions: CSI-FiSh vs SCALLOP

CSI-FiSh

- $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$
- Expensive class group computation, only feasible for CSIDH-512 parameters

SCALLOP

- $\mathfrak{O} = \mathbb{Z} + f\mathfrak{O}_0$, f prime
- $|\mathrm{Cl}(\mathfrak{O})|$ free, sieve until smooth enough to compute lattice of relations

Effective Group Actions: CSI-FiSh vs SCALLOP

CSI-FiSh

- $\mathfrak{O} = \mathbb{Z}[\sqrt{-p}]$
- Expensive class group computation, only feasible for CSIDH-512 parameters
- Evaluation of group action with implicit orientation
- Online phase fast

SCALLOP

- $\mathfrak{O} = \mathbb{Z} + f\mathfrak{O}_0$, f prime
- $|\mathrm{Cl}(\mathfrak{O})|$ free, sieve until smooth enough to compute lattice of relations
- Need to compute explicit orientation along group action
- Online phase slower, but feasible for larger security levels

Implementation

Proof of concept implementation in C++ available at:
https://github.com/isogeny-scallop/scallop

- Concrete instantiation for SCALLOP matching the security levels of CSIDH-512 and CSIDH-1024
- Public keys of size roughly 1600bits for SCALLOP-512 and 2300bits for SCALLOP-1024

Implementation

Proof of concept implementation in C++ available at:
https://github.com/isogeny-scallop/scallop

- Concrete instantiation for SCALLOP matching the security levels of CSIDH-512 and CSIDH-1024
- Public keys of size roughly 1600bits for SCALLOP-512 and 2300bits for SCALLOP-1024
- Evaluation of the group action takes about 35 seconds for the smaller and 12.5 minutes for the larger parameter set
- Implementation shows feasibility, but further work needed to make the group action practical

Summary

- Provide framework to evaluate a new family of group actions on oriented elliptic curves via isogenies

Summary

- Provide framework to evaluate a new family of group actions on oriented elliptic curves via isogenies
- Concrete instantiations of class group action using action of class group of imaginary quadratic order with large prime conductor f inside an imaginary quadratic field of small discriminant (SCALLOP)
- This instantiates effective group actions for security levels previously out of reach

Summary

- Provide framework to evaluate a new family of group actions on oriented elliptic curves via isogenies
- Concrete instantiations of class group action using action of class group of imaginary quadratic order with large prime conductor f inside an imaginary quadratic field of small discriminant (SCALLOP)
- This instantiates effective group actions for security levels previously out of reach
- Can build schemes that require to uniquely represent and efficiently act by *arbitrary* group elements for larger security levels than with CSIDH group action

Questions

Open

- How to make group action evaluation more practical?
- How to resolve the scaling issues of SCALLOP?

Questions

Open

- How to make group action evaluation more practical?
- How to resolve the scaling issues of SCALLOP?

Thank you!

More details:
ia.cr/2023/058

Questions

Open

- How to make group action evaluation more practical?
- How to resolve the scaling issues of SCALLOP?

Thank you!

More details:
ia.cr/2023/058