Isogeny-based group actions in cryptography

Sabrina Kunzweiler
Inria Bordeaux, Institut de Mathématiques Bordeaux

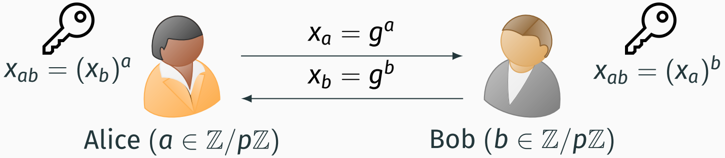
December 05, 2024

Classical Diffie-Hellman setting

Diffie-Hellman key exchange

Idea: Alice and Bob establish a shared session key, communicating over a public channel.

Setting $\mathbb{G} = \langle g \rangle$ of prime order p.



Cryptographic assumptions

We require that the following two problems are hard:

- **DLOG** Given $x, y \in \mathbb{G}$, determine $a \in \mathbb{Z}/p\mathbb{Z}$ with $y = x^a$.
- **CDH** Given $x, y = x^a, z = x^b \in \mathbb{G}$, determine $w \in \mathbb{G}$ so that $w = x^{ab}$.

Solving DLOG in a group $\mathbb{G}$

Generic classical algorithms

- Lower bound: $O(\sqrt{p})$ on a classical computer (Shoup, Eurocrypt '97)
  $\Rightarrow$ achieved by Pollard-Rho and Baby-step-giant-step algorithms

Specialized algorithms

- $\mathbb{G} \subset \mathbb{F}_q$: index calculus attacks $\rightarrow$ subexponential complexity
- $\mathbb{G} \subset E(\mathbb{F}_q)$ for some elliptic curve $E/\mathbb{F}_q$:
  - pairing attack (MOV) when d is small: reduction to DLOG in $\mathbb{F}_q^d$ with $E[p] \subset \mathbb{F}_{q^d}$
  - lifting attack when $E(\mathbb{F}_p) = p$: reduction to DLOG in the formal group of some lift $\tilde{E}$ over $\mathbb{Q}_p$

Shor's algorithm $\rightarrow$ polynomial in $\log p$ on a quantum computer

Cryptographic Group Actions

Group Actions

Group Action Let $(\mathcal{G}, \circ)$ be a group with identity element $id \in \mathcal{G}$, and $\mathcal{X}$ a set. A map $\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ is a group action if it satisfies the following properties:

1. Identity: $id \star x = x$ for all $x \in \mathcal{X}$.
2. Compatibility: $(g \circ h) \star x = g \star (h \star x)$ for all $g, h \in \mathcal{G}$ and $x \in \mathcal{X}$.

Technical Assumptions

- $\mathcal{G}$, $\mathcal{X}$ are finite, $\mathcal{G}$ is abelian, the action is regular.

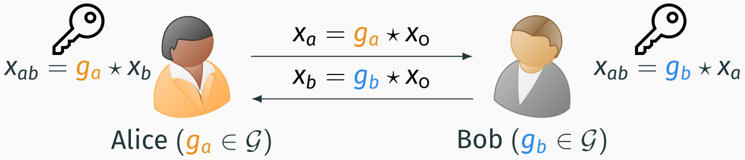
Example

$\mathcal{G} = (\mathbb{Z}/p\mathbb{Z})^*$, $\mathcal{X} = \langle P \rangle \setminus \{0\} \subset E[p]$
$\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}, \quad (a, Q) \mapsto [a] \cdot Q$

⚠ Extra structure:
For $Q_1, Q_2 \in \mathcal{X}$, we can compute $Q_1 + Q_2$.

Group action Diffie–Hellman

Setting $\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}, x_0 \in \mathcal{X}.$



Cryptographic assumptions [1]

We require that the following two problems are hard:

- GA-DLOG: Given $g \star x_0 \in \mathcal{X}$, find $g \in \mathcal{G}$.
- GA-CDH: Given $(g \star x_0, h \star x_0) \in \mathcal{X}^2$, find $z = (g \circ h) \star x_0 \in \mathcal{X}$.

[1] We use the notation of the cryptographic group action framework by (AFMP, AsiaCrypt'20). This is similar to the framework of Hard Homogeneous spaces by (Couveignes, Eprint '06).

Solving GA-DLOG

Consider a group action $\mathcal{G} \times \mathcal{X} \to \mathcal{X}$ with $\#\mathcal{G} = \#\mathcal{X} = N$.

Classical attacks

- Lower bound in the *generic group action model*: $O(\sqrt{N})$ (DHK**K**LR, PKC'23)
  $\Rightarrow$ achieved by (a variant of) the baby-step-giant-step algorithm

Note: N is not assumed to be prime. Pohlig-Hellman-style attacks do not apply!

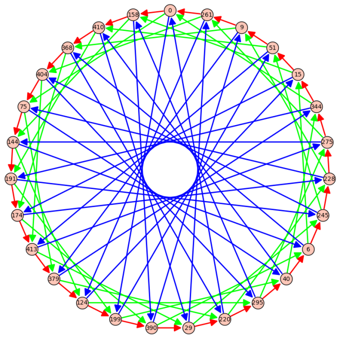
Quantum attacks

- Best known attack: Kuperberg's algorithm with subexponential complexity
- No meaningful lower bounds from a *quantum generic group action model*.

The CSIDH group action

CSIDH [CLMPR, AsiaCrypt'18] Isogeny Graph

Setting: prime $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ with $\ell_1, \ldots, \ell_n$ are small odd primes, and $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$.



Isogeny Graph over $\mathbb{F}_{419}$ with 3-, 5-, and 7- isogenies.

Vertices: Elements in $\mathcal{E}\ell\ell_p(\mathcal{O})$,
i.e. elliptic curves with endomorphism ring $\mathcal{O}$.

- cardinality: $O(\sqrt{p})$
- labelled by Montgomery coefficient A
  $\Rightarrow E_A : y^2 = x^3 + Ax^2 + x$

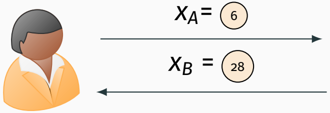
Edges: ℓ_i-isogenies for $\ell_1, \ldots, \ell_n$

- 2-regular for each ℓ_i
- directed graph
- *dual isogenies* allow to go back

Commutative Supersingular Isogeny Diffie-Hellman (CSIDH)

Key Idea: Alice and Bob take secret walks on the isogeny graphs.
They only exchange the end vertices.

An example with $p = 59$. The starting vertex is fixed to (0).



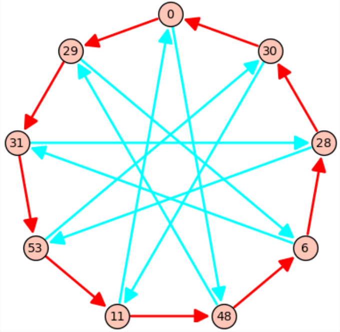
Alice: $a = (2, -1)$

$\Rightarrow x_A =$ (6)

Bob: $b = (-1, -2)$

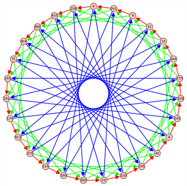
$\Rightarrow x_B =$ (28)

$K_{ab} =$ (11)



Graph with 3- and 5- isogenies.

Formal description of CSIDH



- $\mathcal{G} = cl(\mathcal{O})$ with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$, $p = 4\,\ell_1 \cdots \ell_n - 1$.
- $\mathcal{X} = \mathcal{E}\ell\ell_p(\mathbb{Z}[\pi])$ with π the Frobenius endomorphism.

  $\star : cl(\mathcal{O}) \times \mathcal{E}\ell\ell_p(\mathcal{O}) \mapsto \mathcal{E}\ell\ell_p(\mathcal{O}), \quad ([\mathfrak{a}], E) \mapsto E/\mathfrak{a}$.

Evaluating the group action

- The primes $\ell_1, \ldots, \ell_n$ are Elkies primes in $\mathcal{O}$, we have

$$(\ell_i) = l_i \bar{l}_i, \text{ with } l_i = (\ell, \pi_p - 1),\ \bar{l}_i = (\ell, \pi_p + 1).$$

- $[l_i]$ defines the isogeny $E \to E'$ with kernel $G = \ker([\ell]) \cap E(\mathbb{F}_p)$. Notation: $E' = [l_i] \star E$.
- Efficient evaluation of elements $[\mathfrak{a}] \star E$ where $\mathfrak{a} = \prod l_i^{e_i}$ and e_i small.

Exponent vector $(e_1, \ldots, e_n)$ $\leftrightarrow$ element $[\mathfrak{a}] = [l_1^{e_1} \cdots l_n^{e_n}]$ $\leftrightarrow$ path in the isogeny graph

Security assumptions and special properties of the CSIDH group action

(A) Restricted effective group action (REGA)

Ideally, we want a group action $\mathcal{G} \times \mathcal{X} \to \mathcal{X}$ to be effective. Essentially:

- Efficient computation in $\mathcal{G}$.
- Membership testing for elements in $\mathcal{X}$.
- Distinguished element $x_0 \in \mathcal{X}$.
- Efficient evaluation of $\star$.

CSIDH is only a restricted effective group action (AFMP, Asiacrypt'20).

- We can evaluate $[\mathfrak{a}] \star E$ efficiently, when $[\mathfrak{a}] = \prod \mathfrak{l}_i^{e_i}$ for a small exponent vector e.

REGA-DLOG

- Given $x, y \in \mathcal{X}$, find a (small) exponent vector $(e_1, \ldots, e_n)$ with $y = \prod g_i^{e_i} \star x$, say $e \in \{-m, \ldots, m\}^n$ for some n.

(A) Attacks on REGA-DLOG

Given $x, y \in \mathcal{X}$, find small $e \in \mathbb{Z}^n$, so that $y = \prod g_i^{e_i} \star x$.

Notation: $N = \#\mathcal{G}$ and $N_m = \#\{-m, \ldots, m\}^n = (2m+1)^n$.

Classic	Quantum
Pollard-style random walk $\mathcal{O}(\sqrt{N})$	Kuperberg $2^{\mathcal{O}(\sqrt{\log N})}$
Meet-in-the-middle [2] $\mathcal{O}(\sqrt{N_m})$	Grover / Claw finding $\mathcal{O}(\sqrt[3]{N_m})$

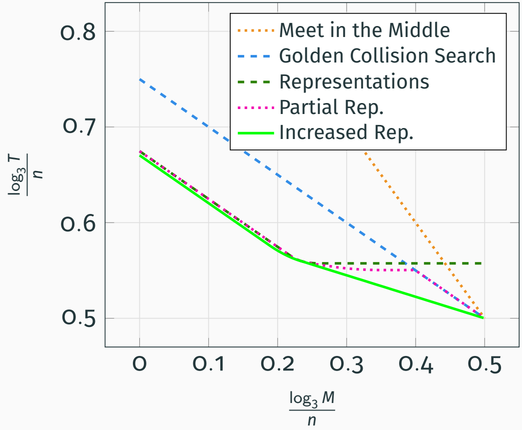
In practice $N_m \ll N$

- Smaller secret keys
- Faster computations

$\Rightarrow$ **Ternary key spaces** $\{-1, 0, 1\}^n$ (The SQALE of CSIDH '2022).

[2] In practice, $\mathcal{O}\left(\frac{N_m^{3/4}}{\sqrt{W}}\right)$ with Parallel Collision Search (PCS) is more realistic.

(A) Classical security analysis of CSIDH with ternary keys



Standard techniques:

- Meet-in-the-middle: high memory cost
- Golden collision: low memory requirements

Time-memory trade-offs with partial representations (CE**K**M, ACNS'23)

- technique known from the cryptanalysis of codes

(B) Twists in CSIDH

For $E_A : y^2 = x^3 + Ax^2 + x$, the quadratic twist is given by

$$(E_A)^t : -y^2 = x^3 + Ax^2 + x$$

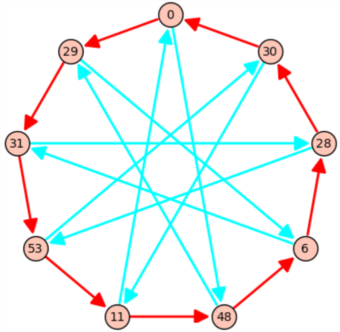
which is $\mathbb{F}_p$-isomorphic to $E_{-A} : y^2 = x^3 - Ax^2 + x$.

- Twisting corresponds to inverting the group action:

$$([\mathfrak{a}] \star E_0)^t = [\mathfrak{a}]^{-1} \star E_0.$$

⚠ Different from the classical DH setting! E.g. given g^a, it is hard to compute $g^{a^{-1}}$.

- Constructive use (BKV, Asiacrypt'19; LGS, Eurocrypt'21)
- Destructive use (AEK**K**R, Crypto'22)



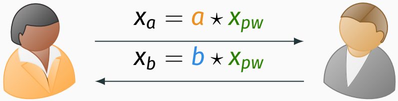
Isogeny graph over $\mathbb{F}_{59}$ with 3- and 5- isogenies.

(B) Twists as a security risk (1/2)

Example: Password-Authenticated Key Exchange (PAKE)

Literal translation of **SPEKE** (Jablon '96) to the group action setting.

- H: hash function $\{0,1\}^* \to \mathcal{X}$



Alice ($a \in \mathcal{G}$) — Bob ($b \in \mathcal{G}$)

$x_{pw} = H(pw)$ — $x_{pw} = H(pw)$

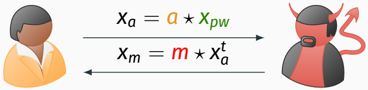
$K_{ab} = (a \star x_b)$ — $K_{ab} = (b \star x_a)$

- General idea: Alice and Bob share a (potentially weak) password $pw \in \{0,1\}^*$ that is used for authentication.

⚠ The twisiting property makes the protocol insecure.

(B) Twists as a security risk (1/2)

Offline dictionary attack against *group action SPEKE* (with twists).



Alice ($a \in \mathcal{G}$) — Mallory ($m \in \mathcal{G}$)

$x_{pw} = H(pw)$ — $x_a^t = \texttt{twist}(x_a)$

$K_{ab} = a \star x_m = (a \cdot m \cdot a^{-1}) \star x_{pw}^t$ — $K_{ab} = ?$

$$K_{ab} = m \star {x_{pw}}^t$$

After this execution of the protocol, Mallory can test all passwords pw $\in \mathcal{PW}$ until finding the correct session key K_{ab}.

(C) Hashing into the set $\mathcal{X} = \mathcal{E}\ell\ell_p(\mathcal{O})$

Second problem with the *group action SPEKE* (and many other protocols).

We need a **secure** hash function $H : \{0,1\}^* \to \mathcal{X}$.

It is easy to define a hash function into the group $H' : \{0,1\}^* \to \mathcal{G}, \quad \mathrm{pw} \mapsto g_{\mathrm{pw}}$.

Then define $H : \{0,1\}^* \to \mathcal{X}, \quad \mathrm{pw} \mapsto g_{\mathrm{pw}} \star x_0$.

⚠ This hash function is not considered secure.
Here, secure means no information about the DLOG of an element.

This remains is an open problem (Failing to hash into supersingular isogeny graphs, BBDFG**K**MPSSTVVWZ, Computer Journal '24)

(D) The decisional Diffie-Hellman problem: Genus theory

DDH Given $x, y = g_a \star x, z = g_b \star x, w \in \mathcal{X}$, decide if $w = (g_a \circ g_b) \star x$.

Genus theory attacks (CSV, Crypto'20)

- Let $\mathcal{O}$ order in an imaginary quadratic field with discriminant Δ.
- For all odd primes $m \mid \Delta$, there is a quadratic character $\chi_m : cl(\mathcal{O}) \to \{\pm 1\}$, $[\mathfrak{a}] \mapsto \left(\frac{N(\mathfrak{a})}{m}\right)$.

⚠ Given E and $[\mathfrak{a}] \star E$, can evaluate $\chi_m(\mathfrak{a}) = \chi_m(E, [\mathfrak{a}] \star E)$.
$\Rightarrow$ **Implication for DDH**: Testing $\chi_m(x, y) \stackrel{?}{=} \chi_m(z, w)$ breaks the assumption **if χ_m is non-trivial** (and m small).

- In CSIDH: $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$, $\Delta = -4p$
  The attack does not apply to CSIDH.

Summary

The CSIDH group action: Summary and questions

1. Which properties distinguish CSIDH from a generic group action?
    - REGA-property: no uniform sampling, smaller key spaces
    - twists: given $x = g \star x_0$, can compute $x^t = g^{-1} \star x_0$ without knowing g.
    - More ideas ?
2. Can we sample supersingular elliptic curves at random without revealing information on the endomorphism ring?
3. Can we solve the Decisional Diffie Hellman Problem?

$$\mathrm{DDH}(x, y = g_a \star x, z = g_b \star x, w) = \begin{cases} 1 & \text{if } w = (g_a \circ g_b) \star x \\ 0 & \text{otherwise.} \end{cases}$$

Thanks!