Solving the Hidden Number Problem for CSIDH and CSURF via Automated Coppersmith



Jonas Meers



Julian Nowakowski

Ruhr University Bochum

October 11, 2023

CSIDH and CSURF

CSIDH [CLM+18] and CSURF [CD20] are **cryptographic group actions**

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

where

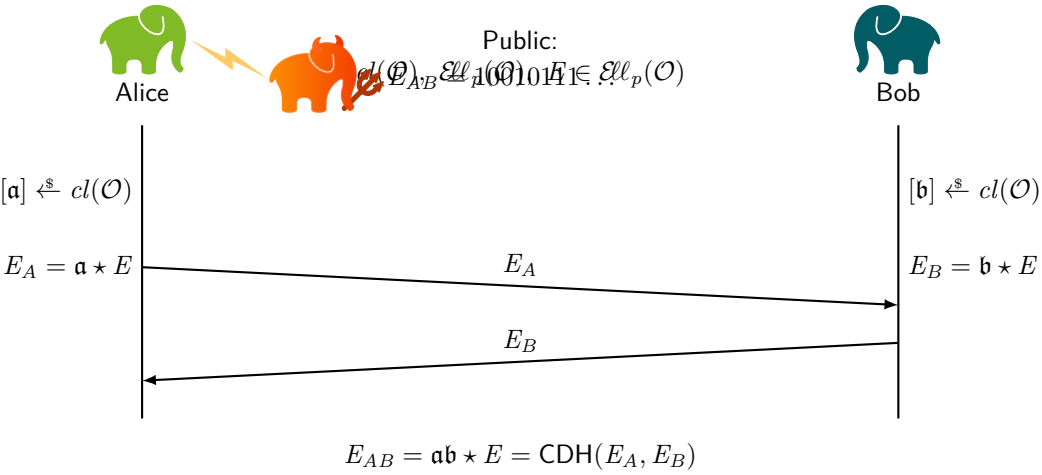
- $cl(\mathcal{O}) =$ ideal-class group of $\mathcal{O}$
- $\mathcal{E}\ell\ell_p(\mathcal{O}) = \{E/\mathbb{F}_p : \mathrm{End}_p(E) \cong \mathcal{O}\}$

They only differ slightly in the **prime** p and the choice of the **order** $\mathcal{O}$.

$\Rightarrow$ 2-isogenies available in CSURF

	$p \bmod 8$	$\mathcal{O}$
CSIDH	3	$\mathbb{Z}[\sqrt{-p}]$
CSURF	7	$\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$

Non-Interactive Key Exchange



The Hidden Number Problem

Given: E_A, E_B and access to an oracle

$$\mathcal{O}_k(E') \coloneqq \mathsf{MSB}_k(\mathfrak{a} \star E')$$

Task: Recover $E_{AB} = \mathsf{CDH}(E_A, E_B)$

- Representation of a curve in CSIDH and CSURF via Montgomery form

$$E : y^2 = x^3 + Mx^2 + x, \qquad M \in \mathbb{F}_p$$

- No fault injection

Question

What is the smallest k that still allows for an efficient recovery?

HNP in Other Contexts

Let $n = |\text{shared key}|$

- [BV96]: Plain Diffie-Hellman over $\mathbb{Z}_p^*$ $k = \sqrt{n}$



- Elliptic Curve Diffie-Hellman over $\mathbb{F}_p$
  - [BHH01]: First attempts $k = 0.98n$



  - [XSWH22]: State of the art (**very** expensive) $k = n/d$



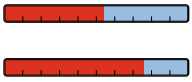
- [GPST16]: SIDH with curves $E/\mathbb{F}_q$ $k = n/2$



- CSIDH and CSURF with curves $E/\mathbb{F}_p$?

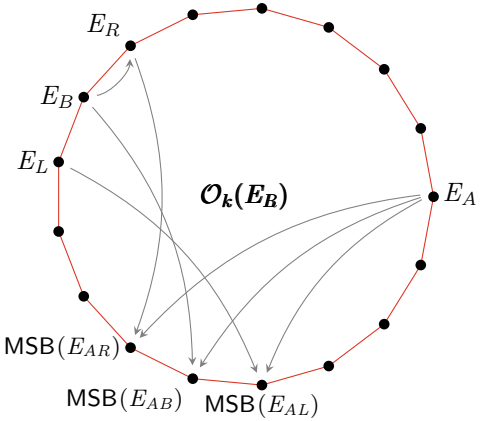
Contributions

1. Efficient heuristic PPT algorithm solving HNP for
   - CSIDH: $k = \frac{13}{24}n \approx 0.54n$
   - CSURF: $k = \frac{31}{41}n \approx 0.76n$
   - Recovery works on any continuous block of missing bits
   - Based on Coppersmith's method



2. Near complete automation of Coppersmith's method

Strategy: Query the oracle on related inputs



ℓ-isogeny graph $\mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$ for odd ℓ

Strategy



- **Modular polynomials** encode neighborhood relation

$$\Phi_\ell(j_0, j_1) \equiv 0 \bmod p \quad \Longleftrightarrow \quad E_0, E_1 \text{ are } \ell\text{-isogenous}$$

- Write j-invariant as

$$j_i = \underbrace{J_i \cdot 2^{n-k}}_{\text{MSBs, shifted}} + \underbrace{x_i}_{\text{Unknown LSBs}}$$

- System of polynomial equations with a "small" root (x_0, x_1, x_2)

$$\tilde{\Phi}_\ell(x_0, x_1) \equiv 0 \bmod p$$
$$\tilde{\Phi}_\ell(x_0, x_2) \equiv 0 \bmod p$$

Coppersmith algorithm

- Finds a "small" root $(x_0, \ldots, x_s)$ of a system of polynomial equations over $\mathbb{F}_p$
- We call a root **small** if

$$\prod_{i=0}^{s} x_i < p^{\varepsilon}$$

- **Goal:** make ε as large as possible to increase recovery rate
- ε increases if
  - the polynomials have low degree
  - the number of equations is high
  - the polynomials are of the same *shape*

Finding good polynomials

How well do modular polynomials perform for CSIDH/CSURF?

- **Problem:** CSIDH/CSURF use Montgomery coefficients
- Formula for j-invariant is of degree 6

$$j(E_A) = 2^8 \frac{(A^2-3)^3}{(A^2-4)}$$

- Modular polynomial is at least of total degree 4

$$\Phi_2(j_0, j_1) = j_0^3 - j_0^2 j_1^2 + 1488 j_0^2 j_1 \ldots$$

$\Rightarrow$ More efficient formulas needed

Efficient formulas for CSURF

Strategy: Take the formulas that are used to compute the group action

Intuition: Small degree isogenies result in low-degree polynomials.

Theorem (Renes [Ren18])

Let $E_A : y^2 = x^3 + Ax^2 + x$ be defined over $\mathbb{F}_p$ and $G \subset E_A(\bar{\mathbb{F}}_p)$ a finite subgroup s.t. $(0,0) \notin G$. Then there exists a Montgomery curve $E_B : y^2 = x^3 + Bx^2 + x$ isomorphic to E_A/G with

$$B = \tau(A - 3\sigma), \quad \tau = \prod_{P \in G \setminus \{\infty\}} x_P, \quad \sigma = \sum_{P \in G \setminus \{\infty\}} \left(x_P - \frac{1}{x_P} \right).$$

$\Rightarrow$ In CSURF we have **2-isogenies** available.

Theorem (Castryck-Decru [CD20])

Let $E_A : y^2 = x^3 + Ax^2 + x$, then $E_B \cong E_A/\langle (0,0) \rangle$ satisfies

$$E_B : y^2 = x^3 + Bx^2 + x, \qquad B = \frac{A+6}{2\sqrt{A+2}}$$

Efficient formulas for CSURF



The resulting system of polynomial equations for **2-isogenies** is:

$$M_2^2 + 12M_2 - 4M_0^2 M_2 - 8M_0^2 + 36 \equiv 0 \bmod p$$
$$M_0^2 + 12M_0 - 4M_1^2 M_0 - 8M_1^2 + 36 \equiv 0 \bmod p$$

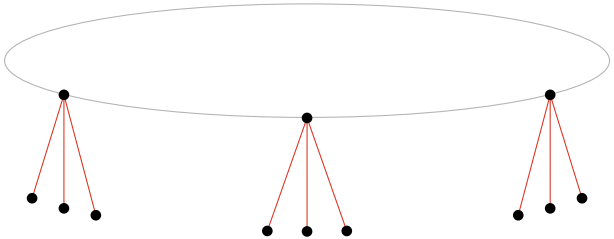
Write Montgomery coefficient as $M_i = m_i \cdot 2^{n-k} + x_i$

Theorem

The root (x_0, x_1, x_2) can be recovered in polynomial time if $k = 0.76 \log p$.

Efficient formulas for CSIDH

- Only **3-isogenies** available ($\approx 16\%$ recovery rate)...
- ... but rational **4-isogeny** exist as well



$\mathscr{E}\ell\ell_p(\mathbb{Z}[(1+\sqrt{-p})/2])$

$\mathscr{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$

Theorem (Onuki-Tagaki [OT20])

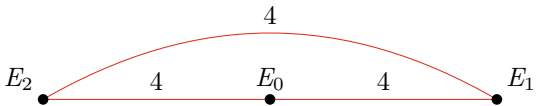
The two 4-isogenous neighbors of $E_A : y^2 = x^3 + Ax^2 + x$ *are*

$$E_B : y^2 = x^3 + Bx^2 + x, \qquad B = 2\frac{A-6}{A+2}$$

and

$$E_C : y^2 = x^3 + Cx^2 + x, \qquad C = 2\frac{A+6}{A-2}$$

Efficient formulas for CSIDH



The resulting system of polynomial equations for **4-isogenies** is:

$$
\begin{aligned}
2M_0 - M_0M_1 - 2M_1 - 12 &\equiv 0 \bmod p \\
2M_2 - M_0M_2 - 2M_0 - 12 &\equiv 0 \bmod p \\
2M_1 - M_1M_2 - 2M_2 - 12 &\equiv 0 \bmod p
\end{aligned}
$$

Write Montgomery coefficient as $M_i = m_i \cdot 2^{n-k} + x_i$

Theorem

The root (x_0, x_1, x_2) *can be recovered in polynomial time if* $k = 0.54 \log p$.

Things to mention

Coppersmith method relies on a mild **heuristic**

- Recovery only successful if the polynomials span a zero-dimensional variety
- Heuristic verified in practice

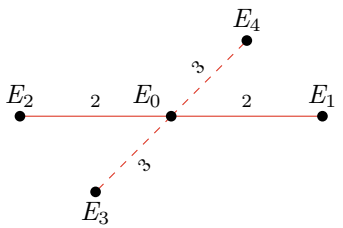
Recovery for **arbitrary** continuous blocks

- Shift the missing part too: $M = m_{\texttt{top}} \cdot 2^{n-k} + x \cdot 2^{n-\ell} + m_{\texttt{bot}}$

Incorporate **higher degree** isogenies

- Only two equations per degree, but higher degree polynomials and different shape
- Recovery rate **decreases**

$$\prod_{i=0}^{2} x_i < p^{\varepsilon} \qquad \text{vs} \qquad \prod_{i=0}^{4} x_i < p^{\varepsilon'}$$



Summary

- We solved the **Hidden Number Problem** for CSIDH and CSURF
  - CSIDH: 46% recovery 
  - CSURF: 24% recovery 
- Recovery strongly benefits from a **small order subgroup** in the CSIDH setting
- Combinatorial reformulation of Coppersmith that allows for **near-complete automation**



https://ia.cr/2023/1409

[BHH01] Dan Boneh, Shai Halevi, and Nick Howgrave-Graham. The modular inversion hidden number problem. In Colin Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 36–51. Springer, Heidelberg, December 2001.

[BV96] Dan Boneh and Ramarathnam Venkatesan. Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes. In Neal Koblitz, editor, *CRYPTO'96*, volume 1109 of *LNCS*, pages 129–142. Springer, Heidelberg, August 1996.

[CD20] Wouter Castryck and Thomas Decru. CSIDH on the surface. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020*, pages 111–129. Springer, Heidelberg, 2020.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 395–427. Springer, Heidelberg, December 2018.

[GPST16] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 63–91. Springer, Heidelberg, December 2016.

[OT20] Hiroshi Onuki and Tsuyoshi Takagi. On collisions related to an ideal class of order 3 in CSIDH. In Kazumaro Aoki and Akira Kanaoka, editors, *IWSEC 20*, volume 12231 of *LNCS*, pages 131–148. Springer, Heidelberg, September 2020.

[Ren18] Joost Renes. Computing isogenies between Montgomery curves using the action of (0, 0). In Tanja Lange and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018*, pages 229–247. Springer, Heidelberg, 2018.

[XSWH22] Jun Xu, Santanu Sarkar, Huaxiong Wang, and Lei Hu. Improving bounds on elliptic curve hidden number problem for ECDH key exchange. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part III*, volume 13793 of *LNCS*, pages 771–799. Springer, Heidelberg, December 2022.