Supersingular Isogeny Key Encapsulation

David Jao

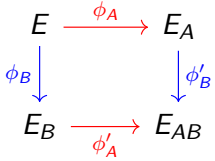
University of Waterloo

November 30, 2022

Supersingular Isogeny Key Encapsulation

Public parameters:

- $p = A \cdot B - 1$
- $E : y^2 = x^3 + 6x^2 + x$ defined over $\mathbb{F}_p$
- P_A, Q_A, P_B, Q_B with $E[A] = \langle P_A, Q_A \rangle$ and $E[B] = \langle P_B, Q_B \rangle$



Private key:

- $\ker \phi_A \subset E[A]$
- $\deg \phi_A = A$

Public key:

- $E_A, \phi_A(P_B), \phi_A(Q_B)$

Ephemeral key:

- $\ker \phi_B \subset E[B]$
- $\deg \phi_B = B$

Shared secret (SIDH):

- $\ker \phi'_B = \phi_A(\ker \phi_B)$
- $\ker \phi'_A = \phi_B(\ker \phi_A)$

SIKE = SIDH + Fujisaki-Okamoto

Attacks on SIKE

- Galbraith, Petit, Shani, Ti (2016/859; Asiacrypt 2016)
- Petit (2017/571; Asiacrypt 2017)
- de Quehen, Kutas, Leonardi, Martindale, Panny, Petit, Stange (2020/633; Crypto 2021)
- Fouotsa and Petit (2021/1322; CT-RSA 2022)
- Castryck and Decru (2022/975)

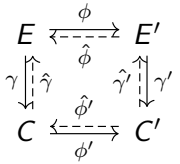
The Castryck-Decru attack

(with contributions by Oudompheng, Wesolowski, Maino and Martindale)

An *isogeny diamond* [Kani 1997] is a diagram where

- $\deg \phi = A$
- $\deg \gamma = B - A$
- $\ker \gamma' = \phi(\ker \gamma)$
- $\ker \phi' = \gamma(\ker \phi)$

For SIDH/SIKE, we take $\phi = \phi_A$.



Theorem

The isogeny $f : C \times E' \to E \times C'$ *given by* $f(P, Q) = (\hat{\gamma}(P) + \hat{\phi}(Q), \gamma'(Q) - \phi'(P))$ *has degree equal to* (B, B) *and kernel equal to* $\ker f = \{([A]P, -\phi\hat{\gamma}(P)) : P \in C[B]\}$.

Exploiting the isogeny diamond

Theorem

$\hat{\phi}$ is equal to the composition: $E' \xrightarrow{i_2} C \times E' \xrightarrow{f} E \times C' \xrightarrow{\pi_1} E$
where i_2 is inclusion and π_1 is projection.

Proof.

$$\pi_1 \circ f \circ i_2(Q) = \pi_1 \circ f(\mathcal{O}, Q) = \pi_1(\hat{\gamma}(\mathcal{O}) + \hat{\phi}(Q),\ \gamma'(Q) - \phi'(\mathcal{O})) = \hat{\phi}(Q). \qquad \square$$

- Recall $\ker f = \{([A]P, -\phi\hat{\gamma}(P)) : P \in C[B]\}$.
- $[A]P$ is trivial to compute.
- We can compute $\hat{\gamma}(P)$ since we constructed γ.
- $\hat{\gamma}(P) \in E[B]$, so we can use the known torsion points to compute $-\phi\hat{\gamma}(P)$.

Hence we can evaluate f, so we can evaluate $\hat{\phi}$, and hence we can compute $\ker \phi = \hat{\phi}(E'[A])$.

Implementing the attack

- γ is simply any isogeny with $\deg \gamma = B - A$.
- A necessary condition is $B > A$.
  (If not, swap A and B, or guess part of ϕ_A, which reduces the effective value of A.)
- If E has known endomorphism ring, then one can easily construct $\gamma \in \mathrm{End}(E)$.
  - The SIKE curve $E : y^2 = x^3 + 6x^2 + x$ has known endomorphism ring.
  - Under reasonable heuristics, the attack is polynomial time in this case.
  - Castryck and Decru implemented a break of `SIKEp434` in 1 hour and `SIKEp751` in 20 hours.
  - Several subsequent improvements have lowered these times.
- Maino and Martindale (2022/1026): Use γ with $\deg \gamma = xB - yA$ where x, y, and $\deg \gamma$ are all smooth. Yields a subexponential attack against unknown endomorphism rings.
- Robert (2022/1038): Polynomial-time attack using 8-dimensional abelian varieties.

Countermeasures?

Some attempts have been made to salvage SIDH, but large parameter sizes are required.

- Moriya (2022/1019): Masked-degree SIDH
- Fouotsa (2022/1054): SIDH with masked torsion point images

Queen's Gazette

Wednesday, November 30, 2022

Dr. Ernst Kani

"Our problem had nothing to do with cryptography, which is why I was surprised when I heard of the algorithm attack. It was quite ingenious, what they did there!" says Dr. Kani. "One of the co-authors of the SIKE algorithm expressed surprise in the fact that genus two curves could be used to gain information about elliptic curves. But this was precisely our original strategy in the 1980's and 1990's (and afterwards)."

The future of isogeny-based cryptography

Broken:

- SIDH
- SIKE
- B-SIDH
- SIOT

Not (yet) broken:

- SIDH signatures
- CSIDH, SeaSign, CSI-FiSH
- OSIDH
- SQISign

Clearly, more research is needed in order to understand the security of isogeny-based cryptosystems. *We hope that such research will continue.*