# An attack on SIDH with arbitrary starting curve

Luciano Maino and Chloe Martindale

University of Bristol

10th August, 2022

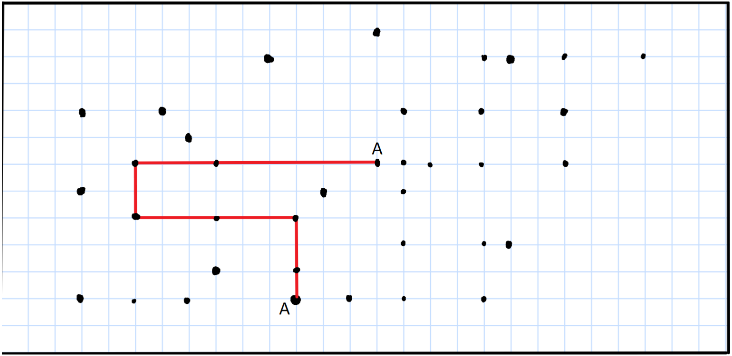
# Outline

# Motivation

- 2016, National Institute of Standards and Technology (NIST) launched **Post-Quantum Cryptography Standardization** competition.
- Isogeny-based protocols
  - ✓ Intensively studied by mathematicians for years
  - ✓ Short keys
  - $\chi$ Slow

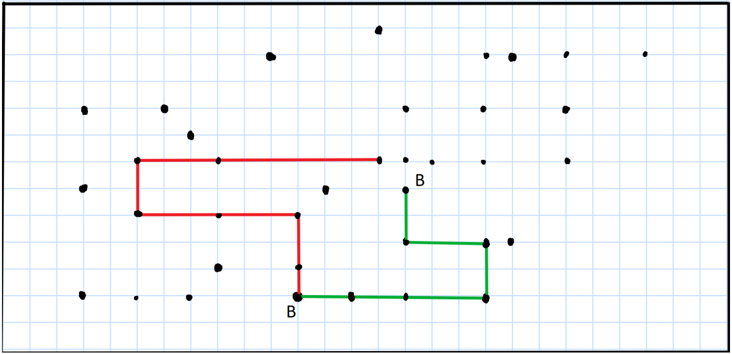
# SIDH

- Supersingular Isogeny Key Encapsulation (**SIKE**) is the only isogeny-based protocol in the competition so far
  - based on Supersingular Isogeny Diffie–Hellman (**SIDH**)



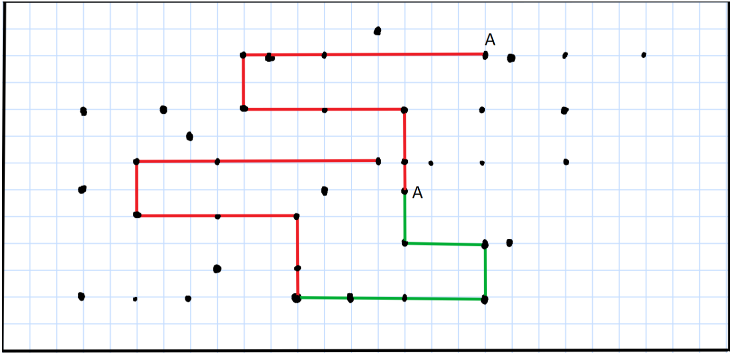
# SIDH

- Supersingular Isogeny Key Encapsulation (**SIKE**) is the only isogeny-based protocol in the competition so far
  - based on Supersingular Isogeny Diffie–Hellman (**SIDH**)

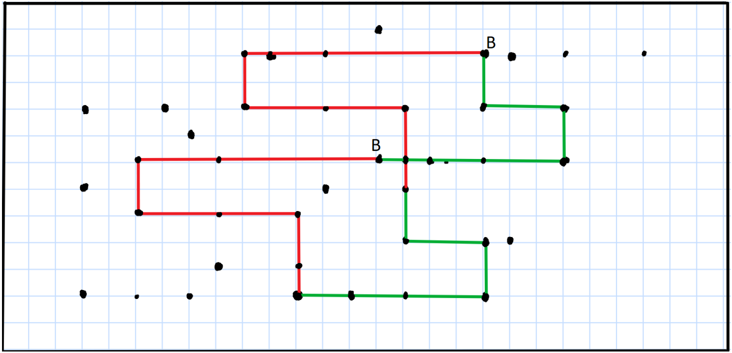


# SIDH

- Supersingular Isogeny Key Encapsulation (**SIKE**) is the only isogeny-based protocol in the competition so far
  - based on Supersingular Isogeny Diffie–Hellman (**SIDH**)



- Supersingular Isogeny Key Encapsulation (**SIKE**) is the only isogeny-based protocol in the competition so far
  - based on Supersingular Isogeny Diffie–Hellman (**SIDH**)



# Supersingular Isogeny with Torsion (SSI-T)

**SSI-T**

Let $p$ be a large prime $p$, and let $A$ and $B$ be two large integers such that $A$, $B$ and $p$ are pairwise coprime. Given two supersingular elliptic curves $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$ connected by an unknown degree-$A$ isogeny $\varphi_A : E_0 \to E_A$, and given the restriction of $\varphi_A$ to the $B$-torsion of $E_0$, recover the isogeny $\varphi_A$.

# Supersingular Isogeny with Torsion (SSI-T)

**SSI-T**

Let $p$ be a large prime $p$, and let $A$ and $B$ be two large integers such that $A$, $B$ and $p$ are pairwise coprime. Given two supersingular elliptic curves $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$ connected by an unknown degree-$A$ isogeny $\varphi_A : E_0 \to E_A$, and given the restriction of $\varphi_A$ to the $B$-torsion of $E_0$, recover the isogeny $\varphi_A$.

$E_0$ is not special in any way

# Supersingular Isogeny with Torsion (SSI-T)

**SSI-T**

Let $p$ be a large prime $p$, and let $A$ and $B$ be two large integers such that $A$, $B$ and $p$ are pairwise coprime. Given two supersingular elliptic curves $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$ connected by an unknown degree-$A$ isogeny $\varphi_A : E_0 \to E_A$, and given the restriction of $\varphi_A$ to the $B$-torsion of $E_0$, recover the isogeny $\varphi_A$.

$E_0$ is not special in any way

Related work: [CD22]

# Outline

# The Attack

$$
\begin{tikzcd}
E_0 \arrow[rr, bend left, "\varphi_A"] & & E_A
\end{tikzcd}
$$

# The Attack

$$
\begin{tikzcd}
E_0 \arrow[rr, bend left, "\varphi_A"] & & E_A \\
E \arrow[u, "\varphi_f"] & &
\end{tikzcd}
$$

$$
\begin{tikzcd}
E_0 \arrow[rr, bend left, "\varphi_A"] & & E_A \\
E \arrow[u, "\varphi_f"] \arrow[urr, "\varphi"] & &
\end{tikzcd}
$$

# Main Theorem

## Main Theorem

Let $f$, $A$, and $B$ be pairwise coprime integers such that $B = f + A$ and $-1/fA = c^2 \pmod{B}$. Let $E/\mathbb{F}_{p^2}$ and $E'/\mathbb{F}_{p^2}$ be two supersingular elliptic curves connected by an $fA$-isogeny $\varphi : E \to E'$, let $\lambda$ be the product polarization on $E \times E'$, let $(P_B, Q_B)$ be a basis of $E[B]$, and let

$$K := \langle (P_B, c\varphi(P_B)), (Q_B, c\varphi(Q_B)) \rangle.$$

Then $K$ is the kernel of a $(B, B)$-isogeny of principally polarized abelian surfaces $(E \times E', B\lambda) \to (E \times E', \lambda)$ represented by the endomorphism

$$\Phi := \begin{pmatrix} B - cfA & \widehat{\varphi} \\ c\varphi & -1 \end{pmatrix} \in \mathsf{End}(E \times E').$$

# Outline

# Computing isogenies

- We can compute isogenies via their kernels
- Using Vélu's formulae, computing an isogeny $\varphi\colon E \to E'$ of prime degree $\ell$ costs $\mathcal{O}(\ell)$ operations over the field of definition of a point that generates the kernel
- The state-of-the-art for large $\ell$ is given by $\sqrt{\acute{e}lu}$ formulae [BDLS20]
    - $\mathcal{O}(\sqrt{\ell})$ operations over the field of definition of a point that generates the kernel
    - memory/complexity trade-off

# Complexity

- $A = \ell_A^a$, $B = \ell_B^b$
- $f = B - A$ may not be smooth
- To increase the pool of smooth $f$'s, $eB = A + f$ for some smooth $e$

# Complexity

- $A = \ell_A^a$, $B = \ell_B^b$
- To increase the pool of smooth $f$'s, $eB\ell_B^{-j} = A\ell_A^{-i} + f$ for some smooth $e$ and small $i$ and $j$

1. Precomputation step of $(e, i, j, f)$
2. Cofactor isogeny computation
3. Guess and computation of the endomorphism on $E \times E'$

$$
\begin{tikzcd}
E_0 \arrow[r, "\varphi'"'] \arrow[rr, bend left, "\varphi_A"] & E' \arrow[r, "\varphi_{\ell_A^i}"'] & E_A \\
E \arrow[u, "\varphi_f"] \arrow[ur, "\varphi"'] & &
\end{tikzcd}
$$

# Precomputation

- $f$ determines the cost of computing the cofactor isogeny $\varphi_f$
  - if $q|f$, the minimal field of definition for a $q$-torsion point has extension degree $\approx q$
- $j$ has no restrictions since $B\ell_B^{-j}$-torsion points can be computed from $B$-torsion points via a $\ell_B^j$ multiplication
- $i$ determines the number of guesses for $\varphi_{\ell_A^i}$
- $e$ must be smooth since to compute the endomorphism on $E \times E'$, we must compute $(eB\ell_B^{-j}, eB\ell_B^{-j})$-isogenies

# The Cofactor Isogeny

- Let $\varphi_q \colon E_n \to E_{n+1}$ be a prime factor of $\varphi_f$

# The Cofactor Isogeny

- Let $\varphi_q \colon E_n \to E_{n+1}$ be a prime factor of $\varphi_f$
- We can guarantee that
    - the codomain $E_{n+1}$ must be defined over $\mathbb{F}_{p^2}$
    - for all $P \in E_n[AB]$, $\varphi_q(P) \in E_{n+1}(\mathbb{F}_{p^2})$

# The Cofactor Isogeny

- Let $\varphi_q \colon E_n \to E_{n+1}$ be a prime factor of $\varphi_f$
- We can guarantee that
  - the codomain $E_{n+1}$ must be defined over $\mathbb{F}_{p^2}$
  - for all $P \in E_n[AB]$, $\varphi_q(P) \in E_{n+1}(\mathbb{F}_{p^2})$
- Methods to compute isogenies over $\mathbb{F}_{p^2}$
  - $\sqrt{\acute{e}lu}$ formulas in [BDLS20, §4.14] at the cost of $\widetilde{\mathcal{O}}(q^{3/2})$
  - Kohel's Algorithm from kernel polynomials [K96, §2.4] at the cost of $\widetilde{\mathcal{O}}(q^2)$

# The Cofactor Isogeny

- Let $\varphi_q \colon E_n \to E_{n+1}$ be a prime factor of $\varphi_f$
- We can guarantee that
  - the codomain $E_{n+1}$ must be defined over $\mathbb{F}_{p^2}$
  - for all $P \in E_n[AB]$, $\varphi_q(P) \in E_{n+1}(\mathbb{F}_{p^2})$
- Methods to compute isogenies over $\mathbb{F}_{p^2}$
  - $\sqrt{\acute{e}lu}$ formulas in [BDLS20, §4.14] at the cost of $\widetilde{\mathcal{O}}(q^{3/2})$
  - Kohel's Algorithm from kernel polynomials [K96, §2.4] at the cost of $\widetilde{\mathcal{O}}(q^2)$
- Factoring $q-$division polynomials is polynomial time in $q$ and $\log(p)$

# Outline

# Example

Microsoft SIKE Challenge: $A = 3^{67}$, $B = 2^{110}$,
$i = 7$, $e = 1$, $j = 2$,

$$f = 5 \cdot 7 \cdot 13^3 \cdot 43^2 \cdot 73 \cdot 151 \cdot 241 \cdot 269 \cdot 577 \cdot 613 \cdot 28111 \cdot 321193.$$

The extension field degrees for all the factors of $f$ are given by

$$\begin{aligned}[k,q] = &[8,5],[12,7],[24,13],[28,43],[144,73],[75,151],[480,241],\\ &[67,269],[1152,577],[1224,613],[56220,28111],[642384,321193].\end{aligned}$$

# Outline

# Open Problems

1. How can we compute the optimal choice for $f$, taking into account all speed-ups available? Can we implement an operation counter to find best trade-off?
2. The algorithm we currently use to select parameters is just a brute-force search over the entire parameter space, which becomes infeasible for large instances, although good parameters may still exist. Can we improve this search, or even construct a smooth $f$ deterministically?
3. Given a security parameter $\lambda$, can we prove that there exists no $(e, i, j, f)$ such that our attack takes more than $2^\lambda$ multiplications over $\mathbb{F}_{p^2}$?

Thanks for your attention!

Questions?

# References


Wouter Castryck and Thomas Decru (2022)
An efficient key recovery attack on SIDH (preliminary version)
https://eprint.iacr.org/2022/975

Daniel J. Bernstein and Luca De Feo and Antonin Leroux and Benjamin Smith (2020)
Faster computation of isogenies of large prime degree
https://eprint.iacr.org/2020/341

David Kohel (1996)
Endomorphism rings of elliptic curves over finite fields
http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf