A Direct Key Recovery Attack on SIDH

L. Maino, C. Martindale, L. Panny, G. Pope, and B. Wesolowski

25th April, 2023

Contribution

- Merge of two papers:
  - M.–Martindale (2022), independent from Castryck–Decru (2022)
  - Wesolowski (2022)
- Proof-of-Concept Implementation — mainly by Panny and Pope — available at

  https://github.com/Breaking-SIDH/direct-attack

Supersingular Isogeny with Torsion (SSI-T)

SSI-T

Let p be a large prime. There are public elliptic curves E_{start} and E_{Bob}, and a secret isogeny $\varphi_{\text{Bob}} : E_{\text{start}} \to E_{\text{Bob}}$ of degree 3^b.

$$\text{Given } \varphi_{\text{Bob}}(E_{\text{start}}[2^a]),$$

compute φ_{Bob}.

History of the SIDH problem

2011 De Feo, Jao, and Plût introduce SIDH

2016 Galbraith, Petit, Shani, Ti give an active attack

2017 Petit describes passive attacks on some parameter sets - SIDH not affected

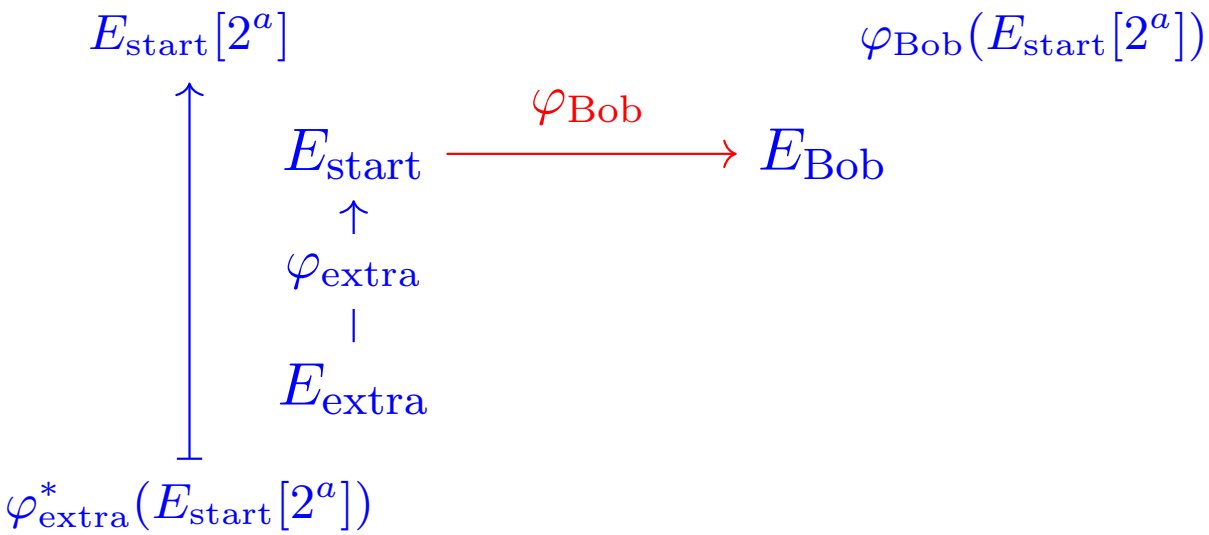
2020 de Quehen, Kutas, Leonardi, Martindale, Panny, Petit, Stange give passive attacks on more parameter sets

The attack

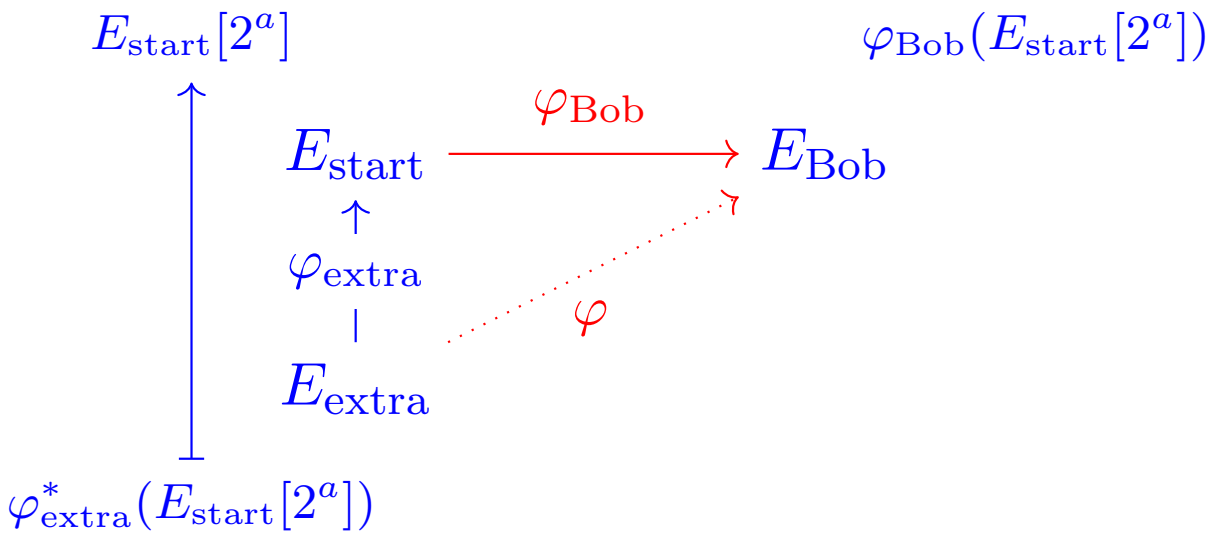
$E_{\text{start}}[2^a]$ $\qquad\qquad$ $\varphi_{\text{Bob}}(E_{\text{start}}[2^a])$

$$E_{\text{start}} \xrightarrow{\varphi_{\text{Bob}}} E_{\text{Bob}}$$

The attack

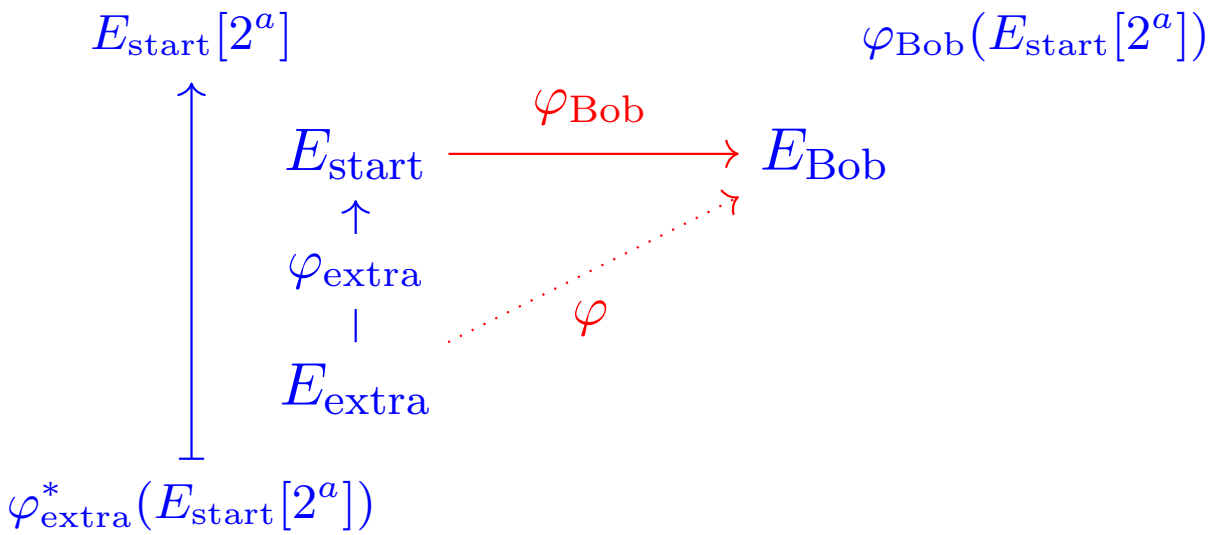

$E_{\text{start}}[2^a]$
$\varphi_{\text{Bob}}(E_{\text{start}}[2^a])$
φ_{Bob}
E_{start}
E_{Bob}
φ_{extra}
E_{extra}
$\varphi^*_{\text{extra}}(E_{\text{start}}[2^a])$

The attack



$$\Phi = \begin{pmatrix} \varphi_{\text{extra}} & -\widehat{\varphi}_{\text{Bob}} \\ * & * \end{pmatrix} : E_{\text{extra}} \times E_{\text{Bob}} \to E_{\text{start}} \times E_{\text{known}}$$

The attack

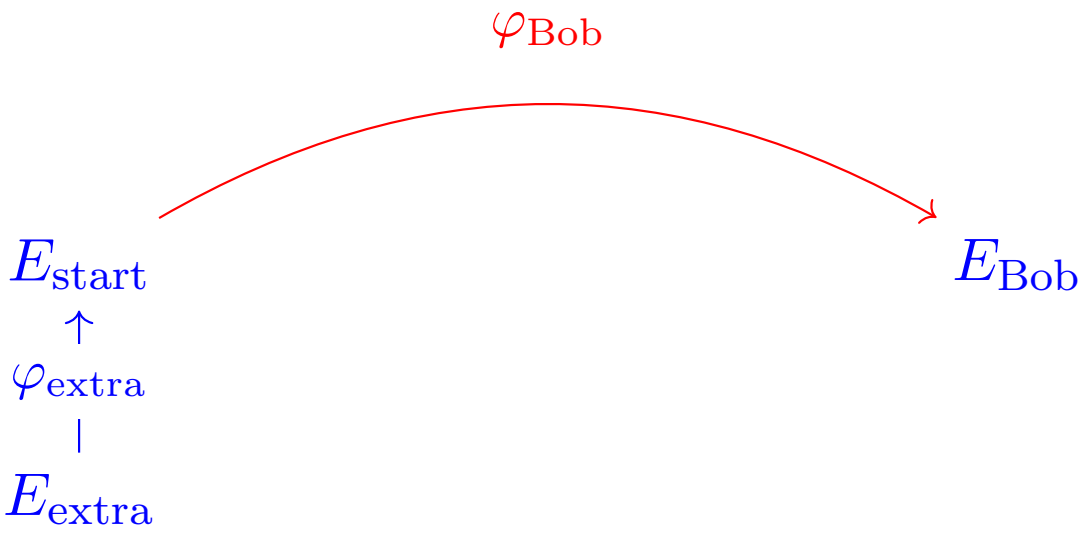


$$\Phi = \begin{pmatrix} \varphi_{\text{extra}} & -\widehat{\varphi}_{\text{Bob}} \\ * & * \end{pmatrix} : E_{\text{extra}} \times E_{\text{Bob}} \to E_{\text{start}} \times E_{\text{known}}$$

$$\text{Ker}(\Phi) = \left(3^b E_{\text{extra}}[2^a], \varphi(E_{\text{extra}}[2^a])\right)$$

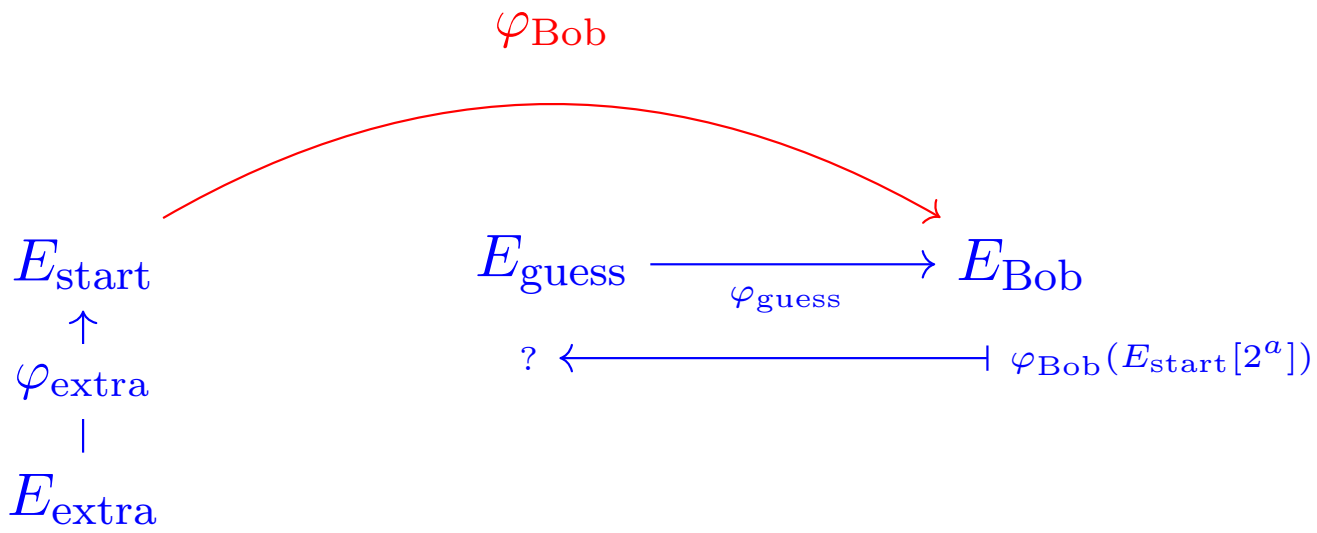
Unknown Endomorphism Ring

- $\deg(\varphi_{\text{extra}}) = 2^a - 3^b$ may not be smooth
- $\deg(\varphi_{\text{extra}}) = e2^{a-j} - 3^{b-i}$ for some small e, i, and j
- This determines the complexity of the attack ($L_{2^a}(1/2)$).



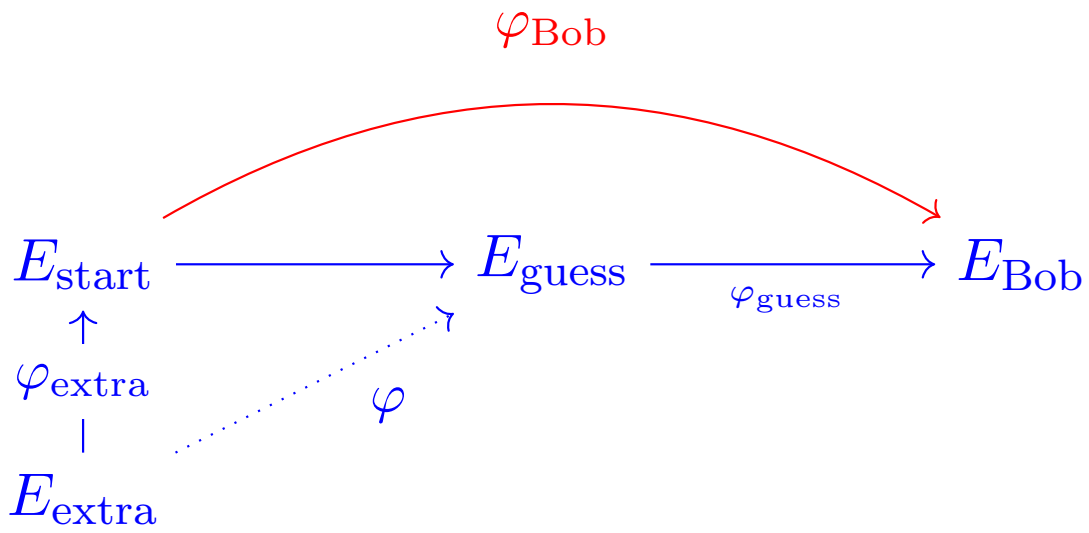
Unknown Endomorphism Ring

- $\deg(\varphi_{\text{extra}}) = 2^a - 3^b$ may not be smooth
- $\deg(\varphi_{\text{extra}}) = e2^{a-j} - 3^{b-i}$ for some small e, i, and j
- This determines the complexity of the attack ($L_{2^a}(1/2)$).



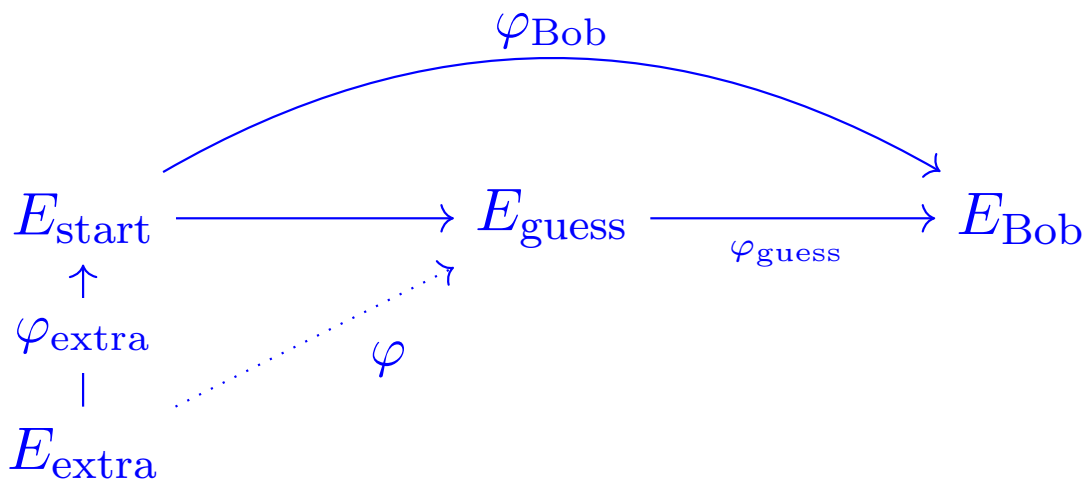
Unknown Endomorphism Ring

- $\deg(\varphi_{\text{extra}}) = 2^a - 3^b$ may not be smooth
- $\deg(\varphi_{\text{extra}}) = e2^{a-j} - 3^{b-i}$ for some small e, i, and j
- This determines the complexity of the attack ($L_{2^a}(1/2)$).



Unknown Endomorphism Ring

- $\deg(\varphi_{\text{extra}}) = 2^a - 3^b$ may not be smooth
- $\deg(\varphi_{\text{extra}}) = e2^{a-j} - 3^{b-i}$ for some small e, i, and j
- This determines the complexity of the attack ($L_{2^a}(1/2)$).



Known Endomorphism Ring

It's ok if $\deg(\varphi_{\text{extra}}) = 2^a - 3^b$ is not smooth.

Known Endomorphism Ring

It's ok if $\deg(\varphi_{\text{extra}}) = 2^a - 3^b$ is not smooth.

Theorem

Assume the generalised Riemann hypothesis. Let E_{start} be a supersingular curve, together with a basis $(\alpha_i)_{i=1}^4$ of $\text{End}(E_{\text{start}})$. There exists a polynomial-time algorithm that finds an isogeny $\varphi_{\text{extra}} : E_{\text{extra}} \to E_{\text{start}}$ of degree $2^a - 3^b$.

Known Endomorphism Ring

It's ok if $\deg(\varphi_{\text{extra}}) = 2^a - 3^b$ is not smooth.

Theorem

Assume the generalised Riemann hypothesis. Let E_{start} be a supersingular curve, together with a basis $(\alpha_i)_{i=1}^4$ of $\text{End}(E_{\text{start}})$. There exists a polynomial-time algorithm that finds an isogeny $\varphi_{\text{extra}} : E_{\text{extra}} \to E_{\text{start}}$ of degree $2^a - 3^b$.

$$\Phi = \begin{pmatrix} \varphi_{\text{extra}} & -\widehat{\varphi}_{\text{Bob}} \\ * & * \end{pmatrix} : E_{\text{extra}} \times E_{\text{Bob}} \to E_{\text{start}} \times E_{\text{known}}$$

The End

Thanks for your attention!

Questions?