PART 1
SQIsign

Identification protocol

- **Commitment:** random isogeny $\varphi_{\text{com}} : E_0 \to E_1$
- **Challenge:** semi-random isogeny $\varphi_{\text{chall}} : E_1 \to E_2$
- **Response:** "matching" isogeny $\varphi_{\text{resp}} : E_A \to E_2$

everyone knows $\mathrm{End}(E_0)$

only **you** know φ_{com} and $\mathrm{End}(E_1)$

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_{\text{com}}"] \arrow[d, "\varphi_A"'] & E_1 \arrow[d, "\varphi_{\text{chall}}"] \\ E_A \arrow[r, "\varphi_{\text{resp}}"] & E_2 \end{tikzcd}$$

only **you** know φ_A and $\mathrm{End}(E_A)$

only **you** know $\mathrm{End}(E_2)$

Fact: ONLY, given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute a proper response

PART 1
SQIsign

Identification protocol

- **Commitment:** random isogeny $\varphi_{\text{com}} : E_0 \to E_1$
- **Challenge:** semi-random isogeny $\varphi_{\text{chall}} : E_1 \to E_2$
- **Response:** "matching" isogeny $\varphi_{\text{resp}} : E_A \to E_2$

signature scheme

replace semi-random φ_{chall}
by a challenge isogeny generated
from SHAKE256(msg || E_1)

everyone knows
$\mathrm{End}(E_0)$

only **you** know
φ_{com} and $\mathrm{End}(E_1)$

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_{\text{com}}"] \arrow[d, "\varphi_A"'] & E_1 \arrow[d, "\varphi_{\text{chall}}"] \\ E_A \arrow[r, "\varphi_{\text{resp}}"] & E_2 \end{tikzcd}$$

only **you** know
φ_A and $\mathrm{End}(E_A)$

only **you** know
$\mathrm{End}(E_2)$

Fact: ONLY, given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$
you can compute a proper response