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
$\text{End}(E_0)$

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

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

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

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

WARNING!

with this approach
the response will
be **large**, degree 2^{1000}

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

To learn more about verification in detail:
see tutorial at https://vodice.post-quantum-crypto.com
by Lorenz Panny & me

PART 1

SQIsign

computing the signature

$$\begin{tikzcd}
E_0 \arrow[r, dashed, "\varphi_1"] \arrow[d, "\varphi_a"'] & E_1 \arrow[d, "\varphi_2"] \\
E_a \arrow[r, "\varphi_3"] & E_2
\end{tikzcd}$$

Fact: Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$