PART 1 SQIsign

Identification protocol

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

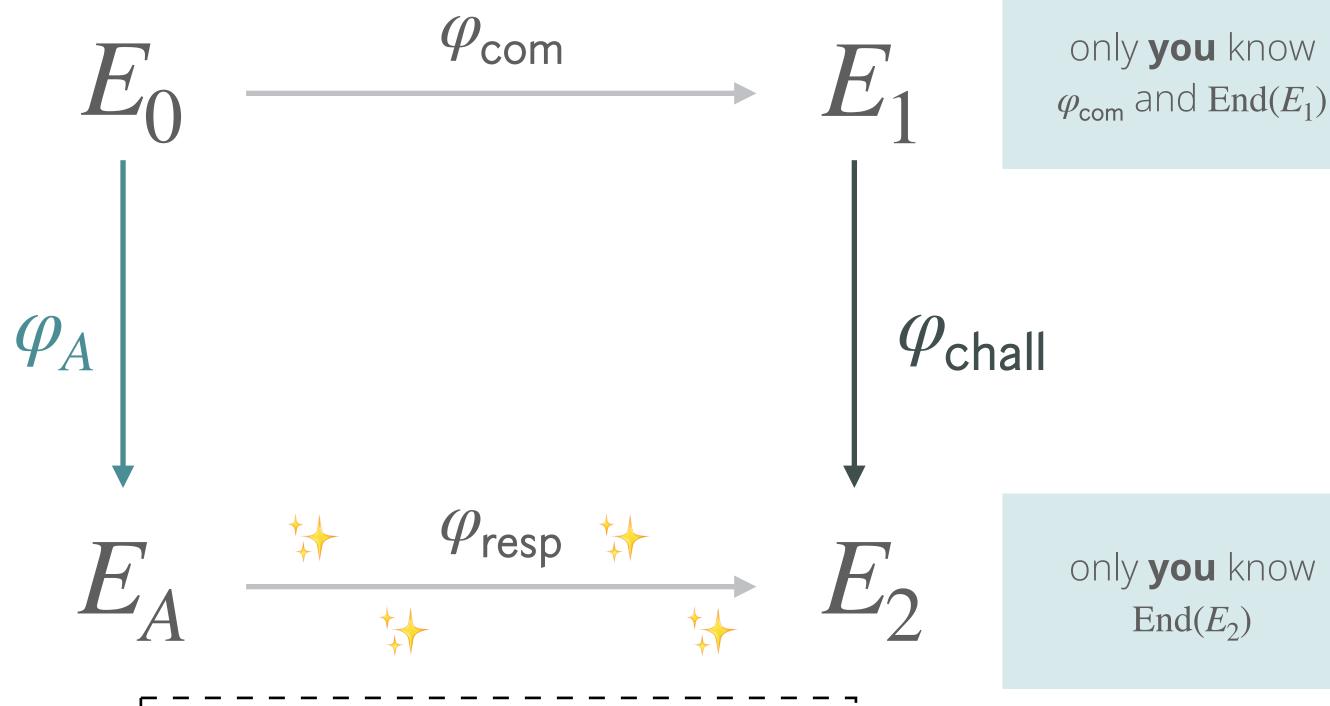
signature scheme

replace semi-random $\varphi_{\rm chall}$ by a challenge isogeny generated from SHAKE256(msg $||E_1|$)

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

only **you** know

 φ_A and $\operatorname{End}(E_A)$



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



PART 1 SQIsign

Identification protocol

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

signature scheme

replace semi-random $\varphi_{\rm chall}$ by a challenge isogeny generated from SHAKE256(msg $||E_1|$)

only **you** know

 φ_{com} and $\mathsf{End}(E_1)$

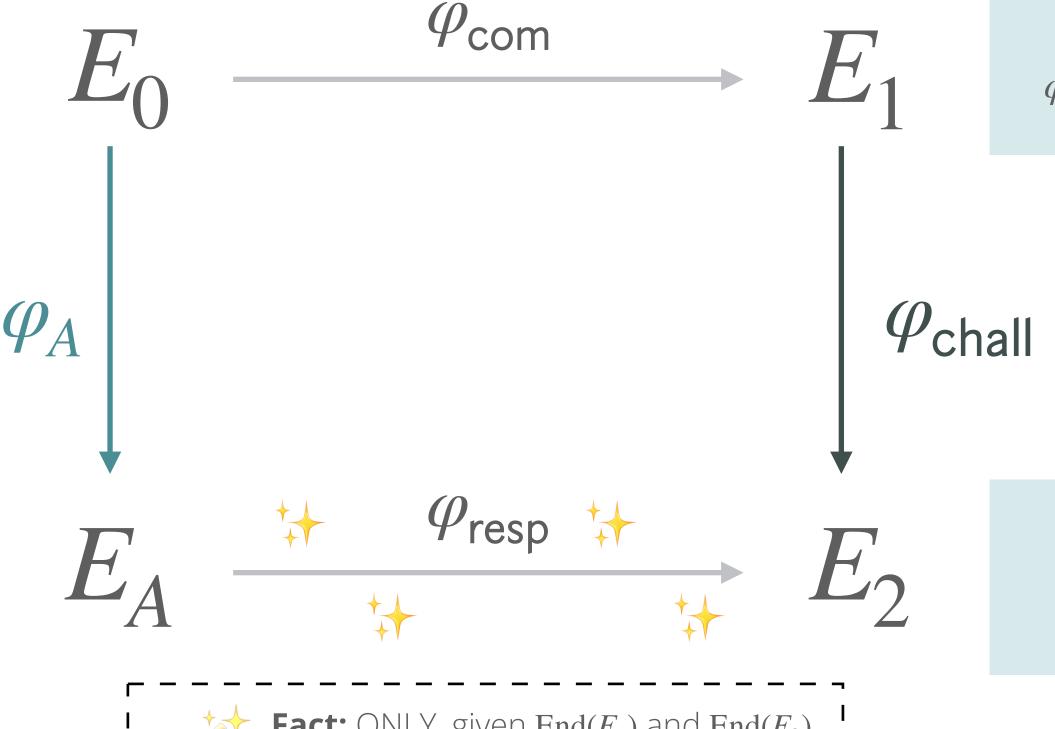
only you know

 $\operatorname{End}(E_2)$

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

only you know

 φ_A and $\operatorname{End}(E_A)$



WARNING!

with this approach the response will be **large**, degree 2¹⁰⁰⁰

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

Radboud University

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