# 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

 $\varphi_{\mathsf{com}}$  and  $\mathsf{End}(E_1)$ 

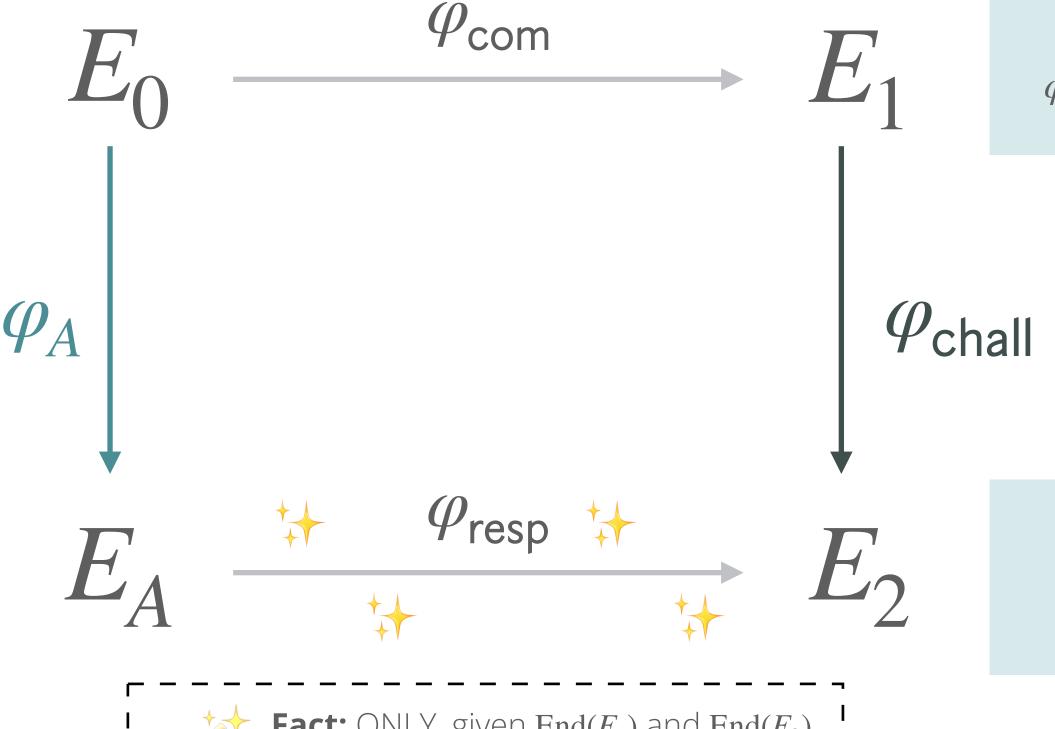
only you know

 $\operatorname{End}(E_2)$ 

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

only you know

 $\varphi_A$  and  $\operatorname{End}(E_A)$ 



#### **WARNING!**

with this approach the response will be **large**, degree 2<sup>1000</sup>

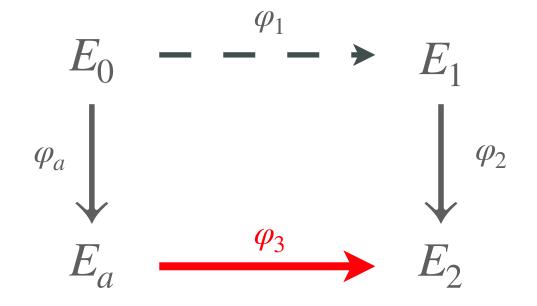
Fact: ONLY, given  $\operatorname{End}(E_a)$  and  $\operatorname{End}(E_2)$  you can compute a proper response

Radboud University

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

# PART 1 SQIsign

## computing the signature



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