

PART 1

SQLsign

Identification protocol

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

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



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

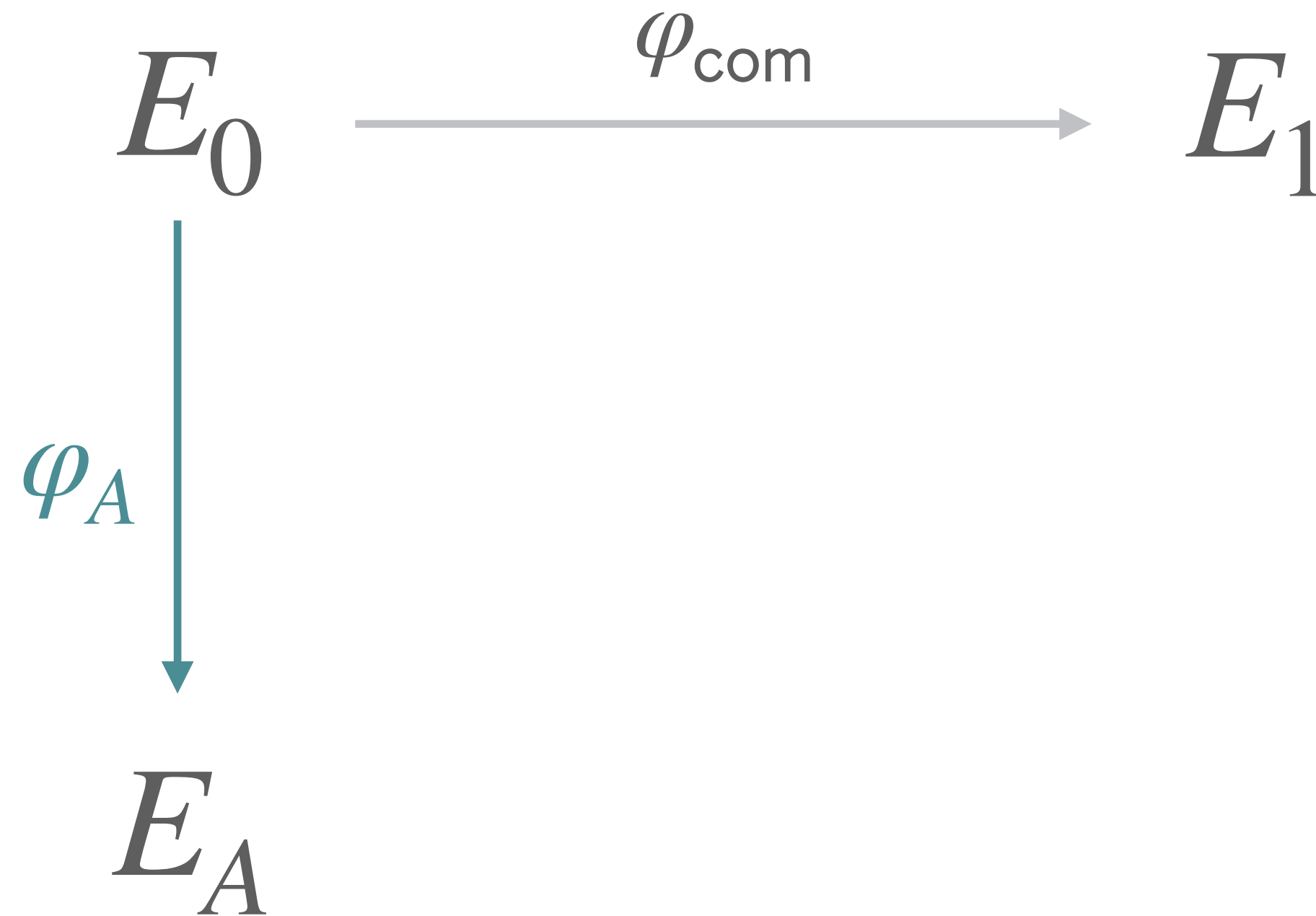
PART 1

SQLsign

Identification protocol

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

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



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

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