PART 1

SQIsign

Key Generation

- **System parameters:** prime p, starting curve E_0
- **Secret Key:** isogeny $\varphi_A : E_0 \to E_A$, and then also $\mathrm{End}(E_A)$
- **Public Key:** the curve $E_A : y^2 = X^3 + Ax^2 + x$, with $A \in \mathbb{F}_q$

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

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

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 $\text{End}(E_0)$

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