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 $\mathrm{End}(E_0)$

E_0

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 $\mathrm{End}(E_A)$