

PART 1

SQLsign

SQLsign

A new isogeny-based
signature scheme,
with **high soundness**

2020

2021

2022

2023

2024

PART 1

SQLsign

Key Generation

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

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

E_0