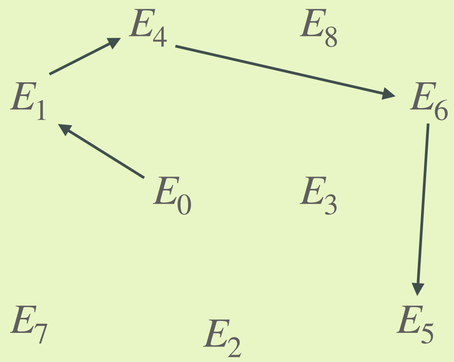
PART 1

SQIsign

Deuring correspondence

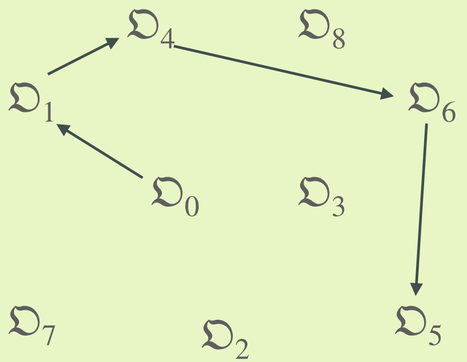
world of supersingular curves



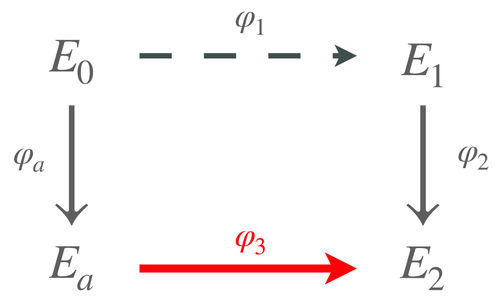
Equivalence of categories

$E \mapsto \mathrm{End}(E) \cong \mathfrak{O}$

world of maximal orders



computing the signature



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

curve-order dictionary

supersingular curves	quaternion orders
curve E (up to Galois conjugacy)	maximal order $\mathfrak{O}$ (up to isomorphism)
isogeny $\varphi : E_1 \to E_2$	integral ideal I_φ that is left $\mathfrak{O}_1$-ideal and right $\mathfrak{O}_2$-ideal
endomorphism $\psi : E \to E$	principal ideal $(\beta) \subset \mathfrak{O}$
and this continues for the *degree*, the *dual*, *equivalence*, *composition*...	and this continues for the *norm*, the *dual*, *equivalence*, *multiplication*...

PART 1

SQIsign

SQIsign

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

SQIsign2

A new algorithm to translate ideals to isogenies.

2020 2021 2022 2023 2024