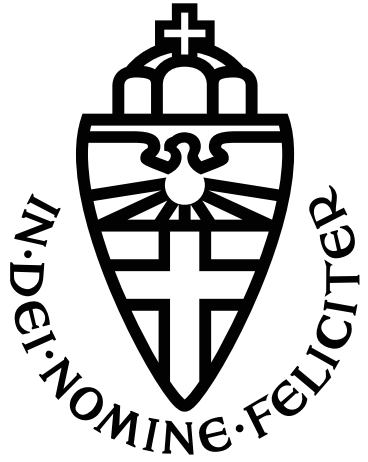
PART 1
SQIsign

Radboud University



Question

, can we find

given supersingular

weird, funky endomorphisms

$$\omega \in \mathrm{End}(E)\,?$$

easy to verify that
such endoms exists,
e.g. that E
is **supersingular**

easy

actually giving an endom. $\omega \in \mathrm{End}(E)$ or some way to compute this

hard

we know $\mathrm{End}(E_0)$ for the
specific curve $E_0 : y^2 = x^3 + x$
and for any $E_0 \to E_A$,
we can then compute $\mathrm{End}(E_A)$

surprisingly easy

(knowledge of endom. ring is contagious)

, can we find

an isogeny

given

and

$$\varphi : E \to E'?$$

actually giving an isogeny $\varphi : E \to E'$ or some way to compute this

actually giving an endom. $\omega \in \mathrm{End}(E)$ or some way to compute this

hard

actually giving an isogeny $\varphi : E \to E'$ or some way to compute this

hard