

PART 1
SQLsign

Question

given supersingular E , can we find
weird, funky endomorphisms $\omega \in \text{End}(E)$?

hard

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

Question

given E and E' , can we find
an isogeny $\varphi : E \rightarrow E'$?

hard

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

PART 1
SQIsign

Question

given supersingular E , can we find
weird, funky endomorphisms $\omega \in \text{End}(E)$?

hard

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

equivalent!!!

hard

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

Question

given E and E' , can we find
an isogeny $\varphi : E \rightarrow E'$?