

PART 1
SQIsign

Question

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

easy

easy to verify that
some isogeny exists,
e.g. that E and E'
are **isogenous**

hard

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

PART 1

SQLsign

Question

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

easy

easy to verify that
some isogeny exists,
e.g. that E and E'
are **isogenous**

intermediate

what if we additionally
know some points $P, Q \in E$
and their images $\varphi(P), \varphi(Q) \in E'$

hard

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