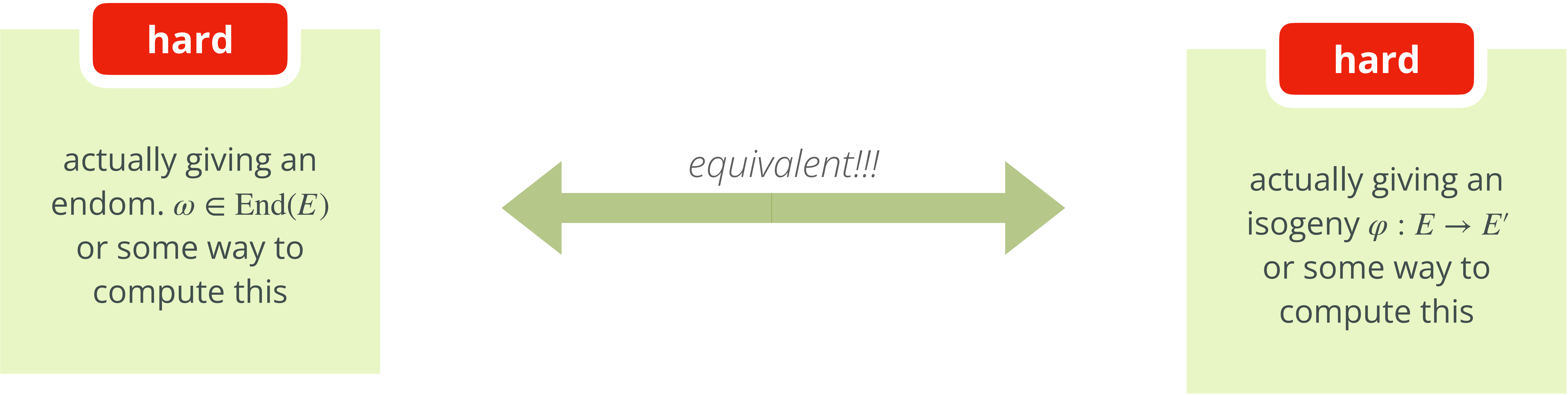
## Question

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

## Question

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



hard

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

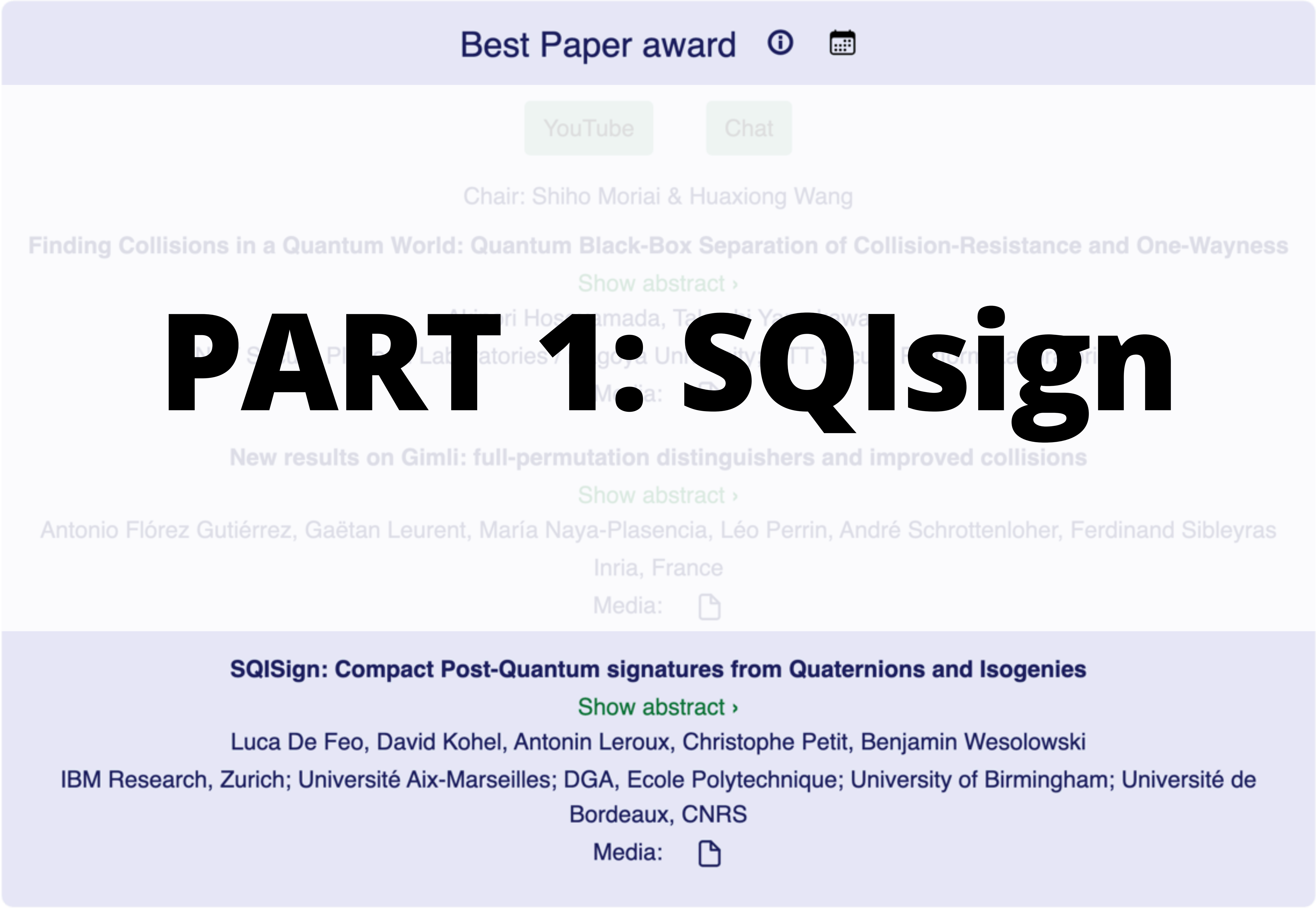
*equivalent!!!*

hard

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

# Best Paper ASIACRYPT 2020

# PART 1: SQIsign



Best Paper award

Chair: Shiho Moriai & Huaxiong Wang

**Finding Collisions in a Quantum World: Quantum Black-Box Separation of Collision-Resistance and One-Wayness**

Show abstract ›

Akinori Hosoyamada, Takashi Yamakawa

NTT Secure Platform Laboratories / Nagoya University; NTT Secure Platform Laboratories

Media:

**New results on Gimli: full-permutation distinguishers and improved collisions**

Show abstract ›

Antonio Flórez Gutiérrez, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, André Schrottenloher, Ferdinand Sibleyras

Inria, France

Media:

**SQISign: Compact Post-Quantum signatures from Quaternions and Isogenies**

Show abstract ›

Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, Benjamin Wesolowski

IBM Research, Zurich; Université Aix-Marseilles; DGA, Ecole Polytechnique; University of Birmingham; Université de Bordeaux, CNRS

Media: