University of Windsor

SAC2022

Invited Talk: Hard problems for isogeny-based cryptography

Benjamin Wesolowski

Abstract: Isogeny-based cryptography is one of the few branches of public-key cryptography that promises to resist quantum attacks. The security of these cryptosystems relates to the (presumed) hardness of a variety of computational problems: finding paths in large "isogeny graphs", computing endomorphisms of elliptic curves, or inverting group actions. We present these problems, and analyse how they relate to each other: which are equivalent, easier, or harder, and how they relate to cryptosystems.