FOUNDATIONS OF ISOGENY-BASED CRYPTOGRAPHY

BENJAMIN WESOLOWSKI

Abstract. We present recent developments on the foundations of isogeny-based cryptography. Isogeny-based cryptography relies on the presumed hardness of computational problems of the following kind: given two (supersingular) elliptic curves, find a non-zero morphism between them (an *isogeny*). Many flavors of such isogeny problems have been introduced and used in cryptographic applications. We will review the main variants, and present the latest computational equivalences between them. In particular, it was recently proved that the problem of finding one endomorphism (an isogeny from a curve to itself) is as hard as the problem of finding *all* endomorphisms. This result has consequences on the security of the SQIsign digital signature scheme and on the fastest known algorithms to solve isogeny problems.

ENS de Lyon, CNRS, UMPA, UMR 5669, Lyon, France