Advances in Isogeny-based Cryptography

Benjamin Smith, Inria + École polytechnique

The mad dash for postquantum public-key cryptosystems has led to a renewed interest in isogeny-based cryptosystems, which are predicated on the difficulty of computing unknown isogenies between elliptic curves. Notable examples include Jao and De Feo's SIDH key exchange, which is based on walks in the 2- and 3-isogeny graphs of supersingular elliptic curves; the Charles--Goren--Lauter hash function, based on the supersingular 2-isogeny graph; and the new CSIDH key exchange, which uses higher-degree isogenies between supersingular curves with commutative endomorphism rings. In this talk we will describe these
systems, with a view to their generalizations to isogeny graphs of low-dimensional abelian varieties. We will also consider some idiosyncracies of the hard problems that underwrite CSIDH security.