Class groups in isogeny-based cryptography

Marc Houben

COSIC, KU Leuven, Belgium

Classically, cryptography based on elliptic curves relies on the difficulty of the discrete logarithm problem. Since this can be solved in quantum polynomial time, there has been continued interest in finding different ways to employ elliptic curves in cryptography that are safe against quantum attacks. One such method uses commutative group actions on elliptic curves by ideal class groups of imaginary quadratic orders, giving rise to key exchange mechanisms such as CRS, CSIDH, and OSIDH. We discuss how to both construct and attack such schemes, using bilinear maps on elliptic curves known as pairings.

KU Leuven, ESAT/COSIC, Kasteelpark Arenberg 10, bus 2452, B-3001 Leuven-Heverlee, Belgium
houben.mr@gmail.com