Torsion-point attacks on isogeny-based cryptography

Chloe Martindale
University of Bristol

Abstract

Cryptography is the science of secure communication over an insecure channel. Post-quantum cryptography is the science of secure communication using everyday devices over an insecure channel, where additionally the person trying to access your messages has access to a quantum computer. This means, for example, that we can't rely on cryptographic algorithms whose security reduces to breaking the discrete logarithm problem in an abelian group (such as the Diffie-Hellman key exchange). Some of the proposals for a post-quantum secure "hard problem" for use in secure messaging and encryption in general are built on the isogeny problem: Given two uniformly random elliptic curves defined over a large finite field, find an isogeny between them (if it exists). A weaker version of this problem, where the image of some torsion points under such an isogeny are known, was the underlying security assumption in SIKE (Supersingular Isogeny Key Encapsulation), that was being considered by the National Institute for Standards in Technology (NIST) in the USA for international standardization. In this talk we will explain the key concepts behind this idea before showing how to solve this instantiation of this isogeny problem, or in other words, how to break SIKE.

This is joint work with Luciano Maino, and also concerns joint work with Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski.