Cryptology ePrint Archive: Report 2011/506

Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies

David Jao and Luca De Feo

Abstract: We present new candidates for quantum-resistant public-key cryptosystems based on the conjectured difficulty of finding isogenies between supersingular elliptic curves. The main technical idea in our scheme is that we transmit the images of torsion bases under the isogeny in order to allow the two parties to arrive at a common shared key despite the noncommutativity of the endomorphism ring. Our work is motivated by the recent development of a subexponential-time quantum algorithm for constructing isogenies between ordinary elliptic curves. In the supersingular case, by contrast, the fastest known quantum attack remains exponential, since the noncommutativity of the endomorphism ring means that the approach used in the ordinary case does not apply. We give a precise formulation of the necessary computational assumption along with a discussion of its validity, and prove the security of our protocols under this assumption. In addition, we present implementation results showing that our protocols are multiple orders of magnitude faster than previous isogeny-based cryptosystems over ordinary curves.

Category / Keywords: public-key cryptography / elliptic curves, isogenies, quantum-resistant cryptosystems

Publication Info: PQCrypto 2011

Date: received 15 Sep 2011

Contact author: djao at math uwaterloo ca