DAVID JAO, University of Waterloo, 200 University Ave. W., Waterloo, ON N2L 3G1
Evaluating isogenies on elliptic curves in subexponential time

An isogeny between elliptic curves is an algebraic morphism which is a group homomorphism. Many applications in cryptography require evaluating large degree isogenies between elliptic curves efficiently. For ordinary curves of the same endomorphism ring, the previous best known algorithm has a worst case running time which is cubic exponential in the length of the input. We show that this problem can be solved in subexponential time under reasonable heuristics, and we present examples of evaluated isogenies which well exceed the previous world record for the evaluation of general prime degree isogenies, including examples of cryptographic size. Time permitting, we will also discuss applications to elliptic curve cryptography and the discrete logarithm problem.

Joint work with Vladimir Soukharev.