FLORIDA ATLANTIC UNIVERSITY

Department of Mathematical Sciences
Florida Atlantic University

PhD Dissertation Defense

Aaron Hutchinson

Algorithms in Elliptic Curve Cryptography

Monday, November 5, 10:30am in SE 215

Advisor: Koray Karabina

Elliptic curves have played a large role in modern cryptography. Most notably, the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm are widely used in practice today for their efficiency and small key sizes. More recently, the Supersingular Isogeny-based Diffie-Hellman (SIDH) algorithm provides a method of exchanging keys which is conjectured to be secure in the post-quantum setting. For ECDSA and ECDH, efficient and secure algorithms for scalar multiplication of points are necessary for modern use of these protocols. Likewise, in SIDH it is necessary to be able to compute an isogeny from a given finite subgroup of an elliptic curve in a fast and secure fashion. We therefore find strong motivation to study and improve the algorithms used in elliptic curve cryptography, and to develop new algorithms to be deployed within these protocols. In this thesis we design and develop d-MUL, a multidimensional scalar multiplication algorithm which is uniform in its operations and generalizes the well known 1-dimensional Montgomery ladder addition chain and the 2-dimensional addition chain due to due to Dan J. Bernstein. We analyze the construction and derive many optimizations, implement the algorithm in software, and prove many theoretical and practical results. In the final chapter of the thesis we analyze the operations carried out in the construction of an isogeny from a given subgroup, as performed in SIDH. We detail how to efficiently make use of parallel processing when constructing this isogeny.

A copy of the dissertation is available in the office of Mathematical Sciences, SE 234

ALL ARE CORDIALLY INVITED