Speaker: Jason LeGrow

Title: Some Problems in Isogeny-Based Cryptography

Abstract: Isogeny-based cryptography is a relatively new subfield of post-quantum cryptography. The security of isogeny-based protocols is based on the difficulty of finding certain “structured" isogenies between a given pair of elliptic curves. These protocols typically have very small key and message sizes relative to other post-quantum schemes, which makes isogeny-based protocols well-suited to applications where low memory or small bandwidth are key.

In this talk I will introduce the high-level ideas of isogeny-based key establishment and discuss some problems I have worked on in this area, such as optimizing algorithms for complex multiplication, quantum cryptanalysis of CSIDH, and analysis of fault attacks. Finally, I will present some interesting research questions and directions for isogeny-based cryptography.