Practical Lattice-Based Cryptography

Joseph Silverman, Brown University

In this talk I will discuss lattice-based cryptosystems based on the shortest vector and closest vector problems. I will describe a ring-based cryptosystem called NTRUEncrypt, explain the lattice problems underlying NTRU, briefly discuss lattice-based signature schemes and their susceptability to transcript attacks, and conclude by describing a new NTRU-style signature scheme that uses rejection sampling to completely eliminate transcript attacks.