DEPARTMENT OF MATHEMATICS
Illinois State University

Undergraduate Colloquium

Title: Post-Quantum Cryptography

Speaker: Emily Stamm
Security Researcher
Allstate

Location: CVA 149
Time: 1:00 - 2:00 pm on Thursday (10/17/2019)

Abstract: Once a sufficiently powerful quantum computer is developed, all of our current public key cryptography (e.g. RSA, DSA, ECC) will be obsolete. For this reason, the department of defense has announced their transition to post-quantum cryptography, which is quantum-resistant cryptography that runs on our classical computers. NIST is holding a competition to standardize new public key cryptography algorithms, and recently the competition was narrowed down to 26 algorithms, most of which are based on lattices. In this talk we introduce the new forms of cryptography (lattice-based, code-based, and multivariate) that will become the new public key standard.