CO 789: Topics in Cryptography – Post-quantum cryptography
Outline
Winter 2024

This course will cover the mathematical background for leading types of post-quantum cryptography: learning-with-errors, hash-based signatures, and code-based cryptography. This will include constructions, the mathematical problems underlying security, and outlines of attacks and reductions. The course will be self-contained but a background in basic cryptographic definitions (public key encryption, digital signature, etc.) will be helpful.

Short Syllabus

1. Learning-With-Errors/Lattice-based Cryptography
   - (a) Definitions
   - (b) Relation to lattice problems
   - (c) Lattice algorithms
   - (d) Protocols and constructions from LWE (Kyber, Dilithium)
2. Hash-based signatures
   - (a) Background (one-way functions, hash functions)
   - (b) Constructions (Merkle trees, one-time signatures, SPHINCS)
3. Code-based cryptography
   - (a) Definitions
   - (b) Hard coding problems (syndrome decoding)
   - (c) The McEliece protocol

Samuel Jaques, Department of Combinatorics and Optimization, University of Waterloo.