CO 789 - Topics in Cryptography: Lattice-based cryptography (Winter 2019)

Instructor

Douglas Stebila

Class time & location

Mondays/Wednesdays/Fridays, 10:30-11:30, MC 6486. **Note as of Wed Nov 21: Time and location probably changing due to a conflict, will update as soon as more information available.**

Due to conflict with the Real World Cryptography conference, there will be no CO 789 lectures during the first week of classes (January 7, 9, 11).

Topics

The first 1/2 to 2/3 of the course will consist of lecture material on the following topics:

- Lattices and lattice problems
- Cryptographic constructions directly from lattices
- Learning with errors (LWE) and variants
- Cryptographic constructions from LWE and variants (public key encryption, signatures, advanced constructions)
- Reductions from lattice problems to learning with errors
- Algorithms for solving lattice problems

The remainder of the course will be seminar-style, with student presentations on recent research papers.

Suggested reading

- Chris Peikert. A Decade of Lattice Cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4):283–424, March 2016. https://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf

Assumed background

I will assume students know the core cryptographic primitives (symmetric encryption, message authentication codes, hash functions, public key encryption, digital signatures, key exchange) taught in any undergraduate crypto or security course. I will also assume typical undergraduate knowledge of probability and linear algebra. I will assume basic understanding of algebra (rings and fields), but will reintroduce more complex notions as needed. Some parts will employ the probable security methodology, which assumes an undergraduate understanding of computational complexity theory, including reductions between problems.