Topics in Lattice-Based Cryptography

Fall 2022

Instructor:	Xiong Fan	**Time:**	sometime
Email:	XYZ@rutgers.edu	**Place:**	somewhere.

Course Pages:

1. http://yourWebPage1.com/teaching

Office Hours: After class, or by appointment, or send me an email. Please include [XXX] in all email communication about course-related matters.

Course Overview: This class is a graduate-level introduction to lattie-based cryptography. The lattices have significantly empowered modern cryptography by giving us (a) a basis for cryptosystems which are secure against quantum computers, (b) multiple breakthroughs in cryptographic primitives such as fully homomorphic encryption and signatures, attribute-based encryption, which are widely used in privacy-preserving machine learning. This course explores the various aspects of the lattices and their applications in cryptography.

Main References: There is no required textbook for this class — lectures, notes, and research papers are the main source of content. The following lecture notes from similar courses are very helpful:

- Lattices, Learning with Errors and Post-Quantum Cryptography, taught by Vinod Vaikuntanathan at UC Berkeley: http://people.csail.mit.edu/vinodv/CS294/lecturenotes.pdf.
- Peikert, C., 2016. A decade of lattice cryptography: https://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf.
- Lattices in Computer Science, taught by Oded Regev at NYU: https://cims.nyu.edu/~regev/teaching/lattices_fall_2009/index.html.

Prerequisites: There are no formal prerequisite classes. A previous course in cryptography is helpful but is not required. This course is mathematically rigorous, hence the mathematical maturity and comfort with linear algebraic notions are the most important pre-requisite, followed by courses in the theory of computation.

Tentative Course Outline:

- Introduction to lattices and the hardness assumptions, Learning With Errors (LWE) and Short Integer Solution (SIS). Algorithms for LWE and Worst-case to Average-case Reduction for SIS.
- Basic cryptographic applications: pseudorandom functions, collision-resistant hashing, public and private-key encryption.
- Lattice Trapdoors and Discrete Gaussian Sampling. Digital Signatures.
- Identity-based Encryption (IBE), Hierarchical IBE. Attribute-based Encryption.
- Fully Homomorphic Encryption, more efficient attribute-based encryption, fully homomorphic signatures.

- Post-Quantum Cryptography.

Grading Policy:

- (40%) Homework assignments (about 4), due approximately every two weeks. Collaboration and external sources are allowed and encouraged; see academic honesty policy for details.
- (20%) Lecture scribing. The primary considerations in grading the scribe notes will be accuracy and clarity. The notes should contain a clear exposition of the material taught in the class.
- (40%) Research-oriented project and presentation. The projects do not need to be purely theoretical.

Academic Honesty: You are free to discuss the problem sets with others. However, the actual writeup of your assignments must be done ONLY by yourself (and without copying from notes or other sources!). In addition, you must acknowledge your sources and the discussions in your submission.

Please read the Academic Integrity Policy (http://academicintegrity.rutgers.edu/) for full details. If you are having trouble with the course, come speak to me!