1 General Information

Point lattices in $\mathbb{R}^n$ have proven remarkably useful in cryptography, both for cryptanalysis (breaking codes) and more recently for constructing cryptosystems with unique security and functionality properties.

This graduate-level seminar will cover classical results, exciting recent developments, and important open problems. Specific topics, depending on time and level of interest, will be drawn from:

- Mathematical background and basic results
- The LLL algorithm, Coppersmith's method, and applications to cryptanalysis
- Complexity of lattice problems: NP-hardness, algorithms and other upper bounds
- Gaussians, harmonic analysis, and the smoothing parameter
- Worst-case-to-average-case reductions and the SIS/LWE problems
- Basic cryptographic constructions: one-way functions, encryption schemes, digital signatures
- "Exotic" cryptographic constructions: ID-based encryption, fully homomorphic encryption, and more
- "Algebraic" (ring-based) cryptographic reductions and primitives

1.1 Materials

The public course web page with lecture notes, homeworks, and other materials is at `https://github.com/cpeikert/LatticesInCryptography`. For assignment submission, grading, discussions, etc., we will use the course Canvas site at `https://umich.instructure.com/courses/559604`.

There is no required textbook for this class; lectures, notes, and research papers are the main sources of content. Students may also wish to refer to the following excellent sources:

- Oded Regev's course *Lattices in Computer Science*
- Micciancio and Goldwasser's book *Complexity of Lattice Problems: A Cryptographic Perspective*

Instructor office hours will be held on **Tuesdays at 11am** (with some exceptions, to be announced ahead of time), or by appointment.

1.2 Prerequisites

There are no formal prerequisite classes. However, this course is mathematically rigorous and fast-paced, hence the main requirement is *mathematical maturity*. Specifically, students should be comfortable with devising and writing correct formal proofs (and finding the flaws in incorrect ones!), devising and analyzing algorithms, and working with probability.

A previous course in cryptography (e.g., Applied or Theoretical Cryptography) is very helpful but is not required. No previous familiarity with lattices will be assumed. *Highly recommended* courses—the more the better—include: EECS 477 or 586 (Algorithms), EECS 574 (Computational Complexity Theory), EECS 475/575 (Introduced to/Advanced Cryptography). The instructor reserves the right to limit enrollment to students who have the necessary background.

2 Course Policies

2.1 Grading

Grades will be determined roughly as follows:

(50%) Homework assignments (about 4), due approximately every two weeks. Collaboration and external sources are allowed and encouraged; see academic honesty policy for details.

(30%) Research-oriented project and presentation.

(20%) Participation (including scribe notes) and homework peer review.

All submitted work will be graded on *correctness* and *clarity*, and must be typeset in LaTeX (templates will be made available). It is good practice to start any longer solution with an informal (but accurate) "proof summary" that describes the core idea — this will help the reader (and you!) understand your solution better.

There are no predetermined score thresholds for A/B/C/etc. Your primary focus should be on *learning the material*, not your grade.

2.2 Academic Honesty

On homework assignments, collaboration and consultation with external sources is allowed and encouraged, subject to the following conditions:

- You must submit your own individually written solution, and you must list your collaborators and/or external sources for each problem.
- You may not submit a problem solution that you cannot explain orally.

There is no hard-and-fast list of (dis)honest conduct. When in doubt, err on the side of caution, or ask the instructor. Dealing with academic dishonesty is unpleasant for everyone involved, so please follow these policies!