# EECS 598: Lattices in Cryptography (2015)

**Meeting:** Mondays and Wednesdays, 10:30a-12p, G. G. Brown Lab 1363
**First meeting:** Wednesday, Sep 9
**Instructor:** Chris Peikert (`cpeikert ATHERE umich DOTHERE edu`)
**Office Hours:** Beyster 3601, by appointment

### Resources

- Syllabus
- Course Canvas site
- A Decade of Lattice Cryptography (Survey)

### Homeworks

- Homework 1, due Wed 23 Sep. [PDF, LaTeX template, macros]
- Homework 2, due Wed 7 Oct. [PDF, LaTeX template, macros]
- Homework 3, due Web 4 Nov. [PDF, LaTeX template, macros]
- Homework 4, due Web 23 Nov. [PDF, LaTeX template, macros]

### Lecture notes Updated/additional lecture notes are now kept **here**.

- Lecture 1: Mathematical Background
- Lecture 2: SVP, Gram-Schmidt, LLL
- Lecture 3: LLL, Coppersmith
- Lecture 4: Coppersmith, Cryptanalysis
- Lecture 5: Cryptanalysis of Knapsack Cryptography
- Lecture 6: Algorithms for SVP, CVP

---

### Course description

Point lattices are remarkably useful in cryptography, both for cryptanalysis (breaking codes) and, more recently, for constructing cryptosystems with unique security and functionality properties. This seminar will cover classical results, exciting recent developments, and several important open problems. Specific topics, depending on time and level of interest, include:

- 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/average-case reductions, and the SIS/LWE problems
- Basic cryptographic constructions: one-way functions, encryption schemes, digital signatures
- ``Exotic" cryptographic constructions: identity-based encryption, fully homomorphic encryption and more
- Ring-based cryptographic reductions and primitives

### Prerequisites

There are no formal prerequisite classes. However, this course is mathematically rigorous, hence the main requirement is *mathematical maturity*. Students should be comfortable with devising and writing correct and clear 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/Theoretical Cryptography) is 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 575 (Advanced Cryptography). The instructor reserves the right to limit enrollment to students who have the necessary background.