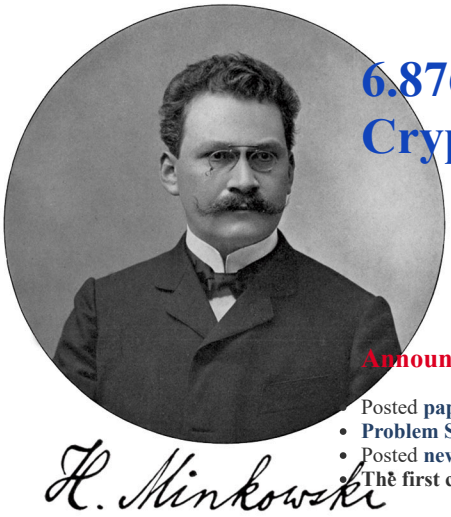

6.876J Advanced Topics in Cryptography: Lattices (Fall 2015)

Announcements

- Posted **papers** for Lectures 7-10.
- **Problem Set 1** is posted. Due October 24.
- Posted **new resources** (books/papers) related to Lecture 3.
- **The first class is on Wednesday 9/9**.

Course Information

INSTRUCTOR	**Vinod Vaikuntanathan** Office: 32-G696 E-mail: vinodv at mit
LOCATION	~~**26-328**~~ ~~**4-149**~~ **24-129 (New Room)** **(Location on the MIT map)**
TIME	**MW 2:30 - 4pm** , Office Hours by appointment
TEXTBOOK	There are *no required textbooks*. Instead, we will use material from the **references** listed below. In addition, for the first few lectures, we may refer to the book *Complexity of Lattice Problems: A Cryptographic Perspective* by Daniele Micciancio and Shafi Goldwasser. (**available online from MIT libraries**)
GRADING	Based on 1-2 problem sets, Scribing 1-2 Lectures and a Final Project.

The course counts for Grad-H Credit as well as the M.Eng. Theory of Computation Concentration.

Course Description

Integer lattices are powerful mathematical objects that have found applications in many diverse facets of computer science, most notably in the areas of cryptography and combinatorial optimization. This course gives an introduction to the theory of integer lattices -- their algorithms and applications to combinatorial optimization, their recent use in cryptography culminating in the first construction of a fully homomorphic encryption scheme, and the fascinating complexity landscape associated with lattice problems. We will discuss the recent exciting developments in these areas, as well as a number of open problems.

Prerequisites: 6.045 and 6.046 (or equivalent). Basic Linear Algebra. Knowledge of basic cryptography is a plus.

Project Ideas

We will maintain the list of open problems and project ideas **here**. This will be updated frequently -- please check back often.

Schedule (subject to change)

Lecture	Topic	Scribe Notes (Unedited)
Lecture 1 (Sep 9)	Overview of the Course, Definitions of Lattices, Minkowski's Convex Body Theorem, Minkowski's First Theorem.	**Lecture 1**
Lecture 2 (Sep 14)	Minkowski's Second Theorem. Gram-Schmidt Orthogonalization and a Lower Bound on λ_1. Applications in Number Theory. Hermite Normal Form and Easy Lattice Problems.	**Lecture 2**
Lecture 3 (Sep 16)	Computational Problems on Lattices -- the Shortest Vector Problem and friends, the LLL algorithm.	**Lecture 3** Itay Berman
Lecture 4 (Sep 21)	LLL algorithm (contd.) and analysis. Exact shortest vector in $2^{O(n^2)}$ time. Babai's approximate closest vector algorithms.	**Lecture 4** Akshay Degwekar
Lecture 5 (Sep 23)	Coppersmith's Method: Finding small Solutions to polynomial equations, Breaking various special cases of the RSA encryption.	**Lecture 5** Rio LaVigne
Lecture 6 (Sep 28)	Goldreich-Goldwasser coAM Protocol for GapCVP	**Lecture 6** Gaurav Singh
Lecture 7 (Sep 30)	Ajtai-Kumar-Sivakumar Algorithm for Exact Shortest Vectors.	**Lecture 7** Adam Sealfon
Lecture 8 (Oct 5)	Micciancio-Voulgaris CVP algorithm. Lattice Algorithms: Summary and Open Problems	**Lecture 8** Ofer Grossman
Lecture 9 (Oct 7)	Complexity of Lattice Problems: NP-hardness of (approximate) CVP.	**Lecture 9** Adam Suhl
Lecture 10 (Oct 14)	Complexity of Lattice Problems: NP-hardness of (approximate) SVP, and open problems.	**Lecture 10** Lauren de Meyer and Prashant Vasudevan

Lecture 11 (Oct 19)	Average-case Hardness of Lattice Problems, Ajtai's Worst-case to Average-case Reduction.	**Lecture 11** Tianren Liu
Lecture 12 (Oct 21)	The Smoothing Lemma. One-way and Collision-resistant Hash functions.	**Lecture 12** Srinivasan Raghuraman
Lecture 13 (Oct 26)	Learning with Errors (LWE), Search and Decisional versions of LWE and a Reduction.	**Lecture 13** Sunoo Park
Lecture 14 (Oct 28)	Fully Homomorphic Encryption.	**Lecture 14** Victor Balcer
Lecture 15 (Nov 2)	Worst-case to Average-case Reduction for LWE	**Lecture 15** Asra Ali
Lecture 16 (Nov 4)	Trapdoors for Lattices.	**Lecture 16** Aloni Cohen
Lecture 17 (Nov 9)	Gaussian Sampling and Digital Signatures.	**Lecture 17** Alex Grinman
Nov 11	Veterans' Day (No Classes)	
Lecture 18 (Nov 16)	Identity-based Encryption.	**Lecture 18** Adam Hesterberg
Lecture 19 (Nov 18)	Attribute-based Encryption.	**Lecture 19** Adam Hesterberg
Lecture 20 (Nov 23)	No Lecture; Office Hours in G-696.	NA
Nov 25	Thanksgiving (No Lecture)	
Lecture 21 (Nov 30)	Key-Homomorphic Functions and Predicate Encryption.	Farhana Khan
Lecture 22 (Dec 2)	Ideal Lattices, Ring SIS and Ring LWE.	Omer Cerrahoglu and Jeffrey
Lecture 23 (Dec 7)	project presentations 2:30-5pm.	
Lecture 24 (Dec 9)	-- ditto --	

References

For the first half of the course (Foundations, Algorithms and Complexity of Lattice Problems):

- Oded Regev's course at **Tel-Aviv University**. The material in this course will be our primary reference.
- Daniele Micciancio's course at **UCSD**.
- Cynthia Dwork's course at **Stanford**.
- Chris Peikert's course at **Georgia Tech**.

Lecture 3

- The "LLL+25" book commemmorating the 25th anniversary of the LLL algorithm is **available** via MIT libraries. Check it out for several cool papers on the state of the art (ca. 2007) in lattice basis reduction and the complexity of lattice problems.
- The **Goldreich-Micciancio-Safra-Seifert paper** on an approximation preserving reduction from SVP to CVP.
- Micciancio's **reductions paper** from SODA is cool and has a comprehensive overview of reductions between several lattice problems.

Lecture 5

- Dan Boneh's **Survey** on Cryptanalysis of RSA variants
- Alexander May's **survey** is a bit more up to date. This is also a chapter in the LLL+25 book.
- Coppersmith's original **paper**.

Lectures 7 and 8

- The **Voronoi Walk SVP algorithm** of Micciancio and Voulgaris.
- **Shorter paths on the Voronoi graph**.
- Two new papers (from STOC and FOCS this year) that solve **Shortest** and **Closest** Vectors respectively in 2^n time.
- Two heuristic algorithms (**here** and **here**) for SVP and CVP that are conjectured to run better than 2^n.

Major Open Questions: Integer programming in 2^{O(n)} time, Shortest Vectors in n^{o(n)} time and 2^{o(n)} space.

Lectures 9 and 10

- **Haviv-Regev** randomized quasi-NP-hardness of SVP within $2^{(\log n)^{1-\varepsilon}}$ factor.
- **Dinur-Kindler-Raz-Safra** NP-hardness of CVP within $2^{(\log n)^{1-\varepsilon}}$ factor.
- Towards **derandomizing** the SVP NP-hardness reduction.
