# Introduction to the Lattice Crypto Day

Phong Nguyễn

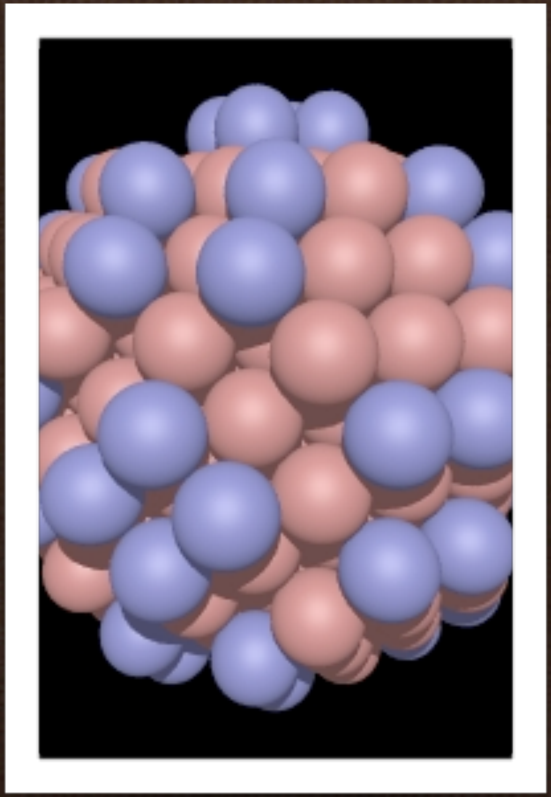
http://www.di.ens.fr/~pnguyen

*May 2010*

# Summary

- History of Lattice-based Crypto
- Background on Lattices
- Lattice-based Crypto vs. "Classical" PKC
- Program of the Day

# Lattice-Based Crypto: A long story



# Lattices and Cryptology

- Two years stand out:
  - 1982
  - 1996

Math. Ann. 261, 515–534 (1982)

Mathematische Annalen
© Springer-Verlag 1982

**Factoring Polynomials with Rational Coefficients**

A. K. Lenstra[1], H. W. Lenstra, Jr.[2], and L. Lovász[3]

1 Mathematisch Centrum, Kruislaan 413, NL-1098 SJ Amsterdam, The Netherlands
2 Mathematisch Instituut, Universiteit van Amsterdam, Roetersstraat 15, NL-1018 WB Amsterdam, The Netherlands
3 Bolyai Institute, A. József University, Aradi vértanúk tere 1, H-6720 Szeged, Hungary

In this paper we present a polynomial-time algorithm to solve the following problem: given a non-zero polynomial $f \in \mathbb{Q}[X]$ in one variable with rational coefficients, find the decomposition of $f$ into irreducible factors in $\mathbb{Q}[X]$. It is well

ADVANCES IN CRYPTOLOGY

Proceedings of Crypto 82

ON BREAKING THE ITERATED MERKLE-HELLMAN PUBLIC-KEY CRYPTOSYSTEM

Leonard M. Adleman*

Our method of attack uses recent results of Lenstra and Lovacz [2]. We treat the cryptographic problem as a lattice problem, rather than a linear programming problem as in Shamir's result. Like Shamir, we are unable to present a rigorous proof that the algorithm works. However,

Publication of LLL

1982

First use of lattices in cryptanalysis

**ECCC**
TR96-007

FTP: ftp.eccc.uni-trier.de:/pub/eccc/
WWW: http://www.eccc.uni-trier.de/eccc/
Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

## Generating Hard Instances of Lattice Problems

Extended abstract

M. Ajtai
IBM Almaden Research Center
650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

ABSTRACT. We give a random class of lattices in $\mathbf{Z}^n$ so that, if there is a probabilistic polynomial time algorithm which finds a short vector in a random lattice with a probability of at least $\frac{1}{2}$ then there is also a probabilistic polynomial time algorithm which solves the following three lattice problems in *every* lattice in $\mathbf{Z}^n$ with a probability exponentially close to one. (1) Find the length of a shortest nonzero vector in an $n$-dimensional lattice, approximately, up to a polynomial factor. (2) Find the shortest nonzero vector in an $n$-dimensional lattice $L$ where the shortest vector $v$ is unique in the sense that any other vector whose length is at most $n^c\|v\|$ is parallel to $v$, where $c$ is a sufficiently large absolute constant. (3) Find a basis $b_1, \ldots, b_n$ in the $n$-dimensional lattice $L$ whose length, defined as $\max_{i=1}^{n} \|b_i\|$, is the smallest possible up to a polynomial factor.

# Crypto '96 Rump Session

### New constructions II

9:21 Daniele Micciancio
An oblivious data structure and its applications to cryptography
9:26 Ran Canetti and Rosario Gennaro
Incoercible multi-party computation
9:31 Jeffrey Hoffstein, Jill Pipher, and Joseph Silverman
A ring-based public-key cryptosystem

Ajtai's worst-case to average-case reduction

Invention of NTRU

1996

# Lattices and Cryptology

- Two years stand out:
  - 1982: First use of lattices in cryptanalysis
  - 1996: First crypto schemes based on hard lattice problems

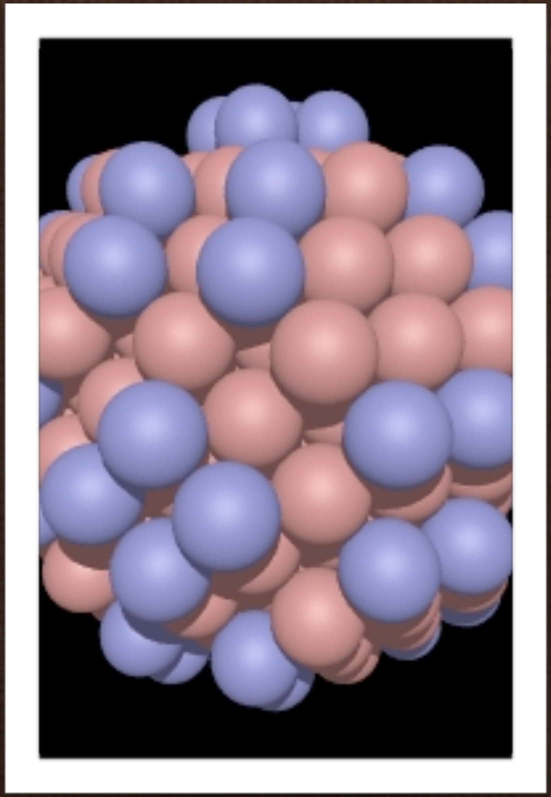
# Lattice-based Crypto

- Somewhat a revival of knapsack crypto (MerkleHellman78,...)
- Two Families:
  - "Theoretical": [Ajtai96...] focus on security proofs.
  - "Applied": [NTRU96...] focus on efficiency.
- They "interact" more and more: [Micc02,GPV08,Gentry09,Peikert10,LPR10,...]

# Lattice Problems in Crypto

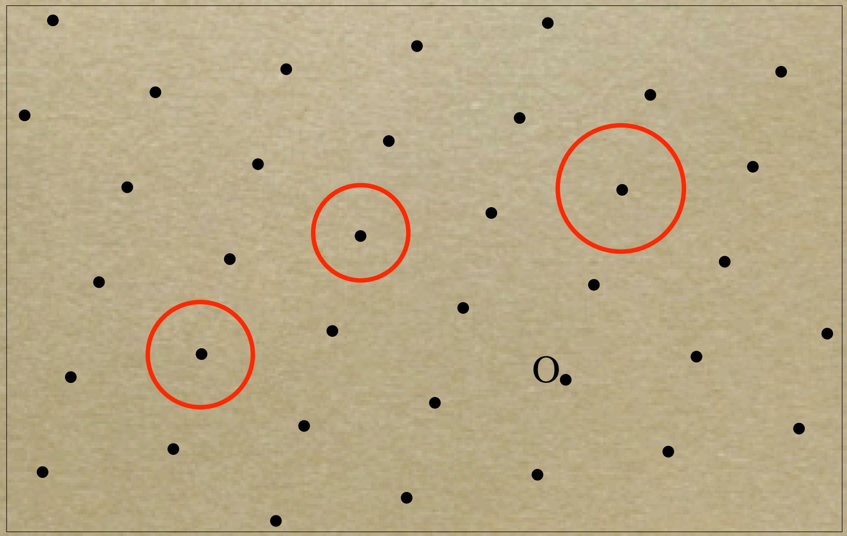
- In many crypto schemes, one actually deals with problems not defined using lattices:
  - SIS. ‘minicrypt’: OWF, hashing, signatures, identification.
  - LWE. ‘cryptomania’: pk-encryption, (H)IBE, oblivious transfer.
- Both are connected to lattice problems.

# Background on Lattices



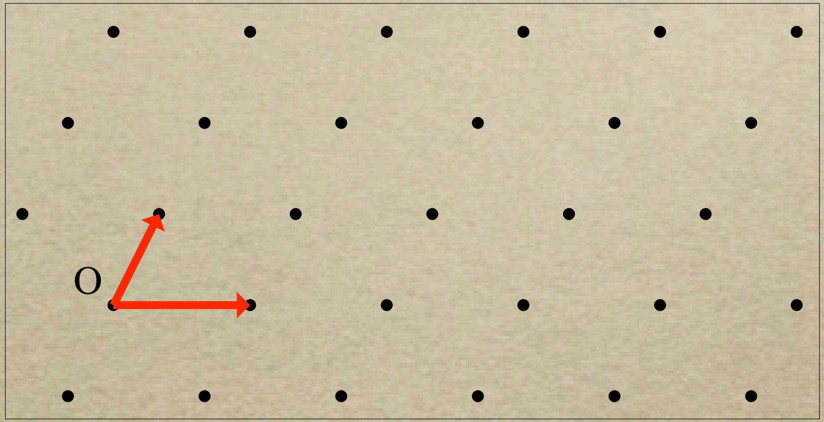
# Lattices

- Consider $\mathbf{R}^n$ with the usual topology of a Euclidean space: let $\langle u,v \rangle$ be the dot product and $||w||$ the norm.
- A lattice is a discrete subgroup of $\mathbf{R}^n$.
- Ex: $\mathbf{Z}^n$ and its subgroups.



# Equivalent Definition

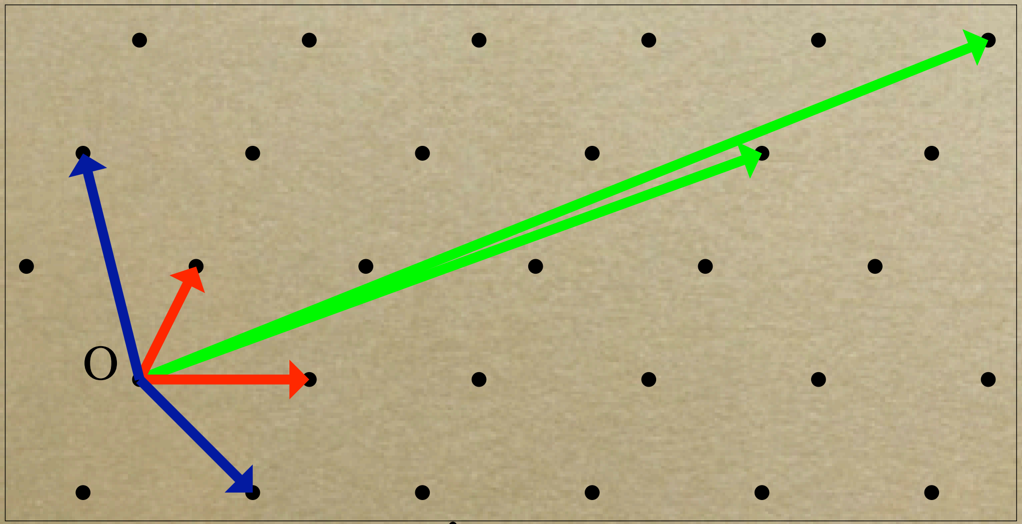
- Let L be a non-empty set of $\mathbf{R}^n$. There is equivalence between:
  - L is a lattice.




  - There exist linearly independent vectors $b_1, b_2, \ldots b_d$ such that $L = L(b_1, b_2, \ldots b_d) = \mathbf{Z}b_1 + \mathbf{Z}b_2 + \ldots + \mathbf{Z}b_d$.
- Such vectors form a basis of a lattice L.

# Volume of a Lattice

- Each basis spans a parallelepiped, whose volume only depends on the lattice. This is the lattice volume.




- By scaling, we can always ensure that the volume is 1 like $\mathbf{Z}^n$.

# Lattices in Crypto

- Most of the time, lattice-based crypto restricts to full-rank integer lattices, and sometimes even more (Ajtai's lattices)...
- For a full-rank lattice L in $\mathbf{Z}^n$, the quotient $\mathbf{Z}^n/L$ is a finite group and $\mathrm{vol}(L)=[\mathbf{Z}^n:L]$.

# Lattice Problems

# Complexity of Lattice Problems

- Since 1996, lattices are very trendy in complexity: classical and quantum.
- Depending on the approximation factor with respect to the dimension:

  $1$

  - NP-hardness $O(1)$
  - non NP-hardness (NP∩co-NP) $\sqrt{n}$
  - worst-case/average-case reduction $O(n \log n)$
  - polynomial-time algorithms $2^{O(n \log \log n / \log n)}$

  $\infty$

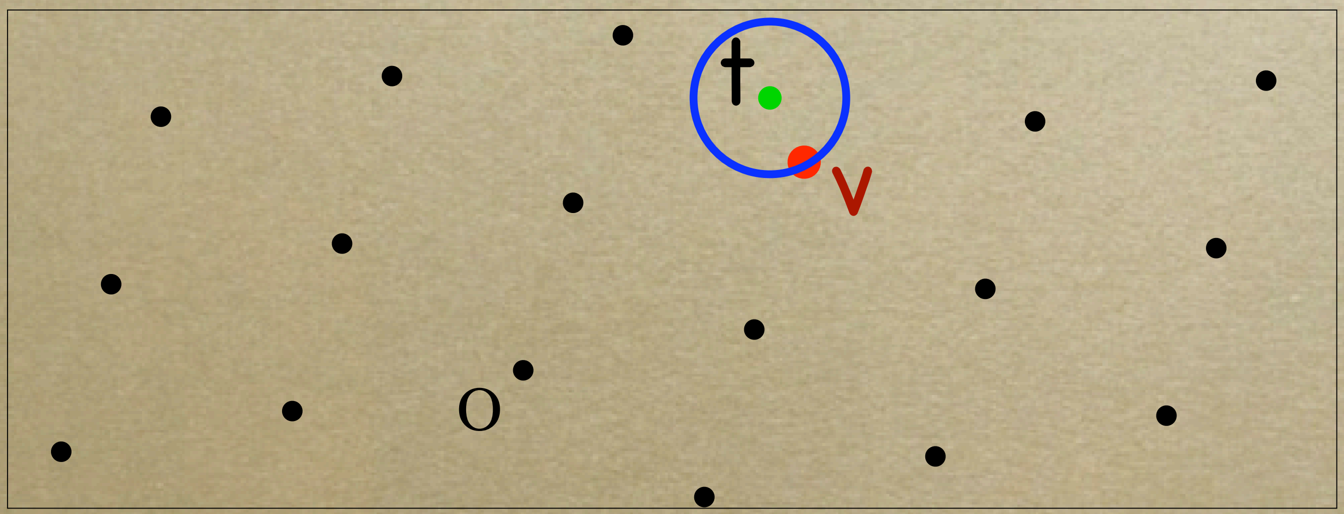
# The Shortest Vector Problem (SVP)

- Input: a basis of a d-dim lattice L
- Output: nonzero v∈L minimizing ||v||.


| | | | | |
|---|---|---|---|---|
| 2 | 0 | 0 | 0 | 0 |
| 0 | 2 | 0 | 0 | 0 |
| 0 | 0 | 2 | 0 | 0 |
| 0 | 0 | 0 | 2 | 0 |
| 1 | 1 | 1 | 1 | 1 |

# The Closest Vector Problem (CVP)

- Input: a basis of a lattice L of dim d, and a target vector t.
- Output: v∈L minimizing ||v-t||.




- Bounded Distance Decoding (BDD): CVP where t is close to L.

# Lattice-based Crypto vs Classical PKC

# Analogy

- Certain lattice crypto schemes somewhat look alike certain schemes from the "classical" PKC world (RSA, DL, Pairings).
- This is especially the case for the emerging lattice IBE family (vs. pairing crypto): [GPV08], [CHKP10], [B10], [ABB10], ...

# Differences

- Finitely generated groups
- Noise
- Probability distributions
- Many parameters: selection?

# Lattices and Probability

# Probability and PKC

- Security proofs require (rigorous) probability distributions and efficient sampling.
- In classical PKC, a typical distribution is the uniform distribution over a finite group.
- Ex: The lack of nice probability distribution was problematic for braid cryptography.

# Lattices and Probability

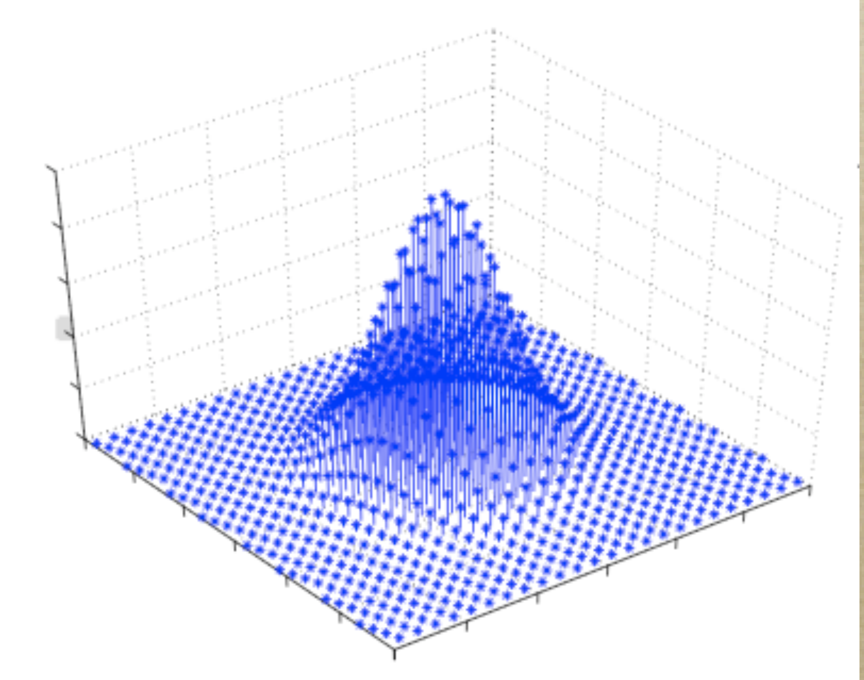
- Distributions on Lattice Points
- Distributions on Lattices

# Distribution on Lattice Points

- The Discrete Gaussian
  - Mass proportional to

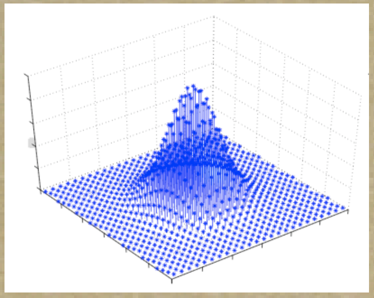
    $$\rho_{s,\mathbf{c}}(\mathbf{x}) = e^{-\pi\|(\mathbf{x}-\mathbf{c})/s\|^2}$$

  - The distribution is independent of the basis.



# Sampling Lattice Points

- This can be done by randomizing Babai's nearest plane algo [Bab86].
- [Klein00,GPV08]: given a lattice basis, one can sample lattice points according to the Gaussian discrete distribution in poly-time, as while as the mean norm is somewhat larger than the norms of the basis.



# Distributions on Lattices

- Random Lattices
  - In Crypto
  - In Mathematics

# Random Lattices in Crypto

- Let n,m,q be integers where $m \geq n \log q$.
- Let A be a m x n matrix whose coeffs have uniform distribution mod q.
- $L_A = \{x \in \mathbf{Z}^m \text{ s.t. } xA \equiv 0 \bmod q\}$. Is a full-rank lattice in $\mathbf{Z}^m$ whose volume divides $q^n$.
- [Ajtai96]: Finding extremely short vectors in a random (m-dim) $L_A$ is as hard as finding short vectors in every n-dim lattice.

# Note

- In practice, an m-dim Ajtai lattice is typically "easier than usual", because of the existence of unusual sublattices.
- See Darmstadt's lattice challenges solved in dim 500-750.

# Note: The SIS Problem

- SIS (Small Integer Solution) = finding short vectors in a random Ajtai lattice $L_A$.
- This is why several crypto schemes actually only considers such lattices. But it might be good to keep generality, for the time being.

# Random Lattices in Mathematics

- Random (Real) Lattices [Siegel1945]
- Random Integer Lattices [GoMa2003]

# Random Integer Lattices

- Let V and n be integers.
- There are only finitely many full-rank lattices in $\mathbf{Z}^n$ of volume V.
- A random full-rank integer lattice of volume V is simply one selected uniformly at random.
- Sampling random integer lattices is trivial when V is prime (see Hermite normal form).

# Interest

- This is a natural and simple distribution, used in all recent benchmarks of lattice algorithms.
- [GoldsteinMayer2003]: when V->∞ and we scale such lattices, the distribution "converges" to the "classical" distribution on random lattices of volume 1.

# Random Real Lattices

- Lebesgue's measure is the "unique" measure over $\mathbf{R}^n$ which is invariant by translation.
- In 1933, Haar generalized Lebesgue's measure to locally compact topological groups: it is the "unique" measure which is invariant by the group action (left or right multiplication).

# Random Real Lattices

- The set of lattices modulo scale can be identified with $G=SL_n(\mathbf{R})/SL_n(\mathbf{Z})$.
- The Haar measure over $SL_n(\mathbf{R})$ projects to a finite measure over G. For n=2, it is the hyperbolic measure.
- => natural probability measure over G, giving rise to random lattices, first used in [Siegel45].

# Random Real Lattices

- [Ajtai06]: one can efficiently sample for the classical distribution on random real lattices.

# Schedule

- 10h: Oded Regev on LWE
- 11h: Vadim Lyubashevsky on Ring-LWE
- 14h: Chris Peikert on IBE and beyond
- 15h: Craig Gentry on fully homomorphic encryption