Introduction to lattices and their applications in Computer Science/Cryptography – Seminar:

References:

The seminar talks will be based on three excellent sets of course notes, namely:

- Oded Regev's course notes "Lattices in Computer Science" (from 2004) from the Tel Aviv University that are accessible via the link:
  https://cims.nyu.edu/~regev/teaching/lattices_fall_2009/
- Daniele Micciancio's course notes "Lattices Algorithms and Applications" (from 2010) from the University of California San Diego that are accessible via the link:
  http://cseweb.ucsd.edu/classes/wi10/cse206a/
- Chi's, Choi's, Kim's and Kim's lecture notes "Lattice Based Cryptography for Beginners" accessible via the link:

  https://eprint.iacr.org/2015/938.pdf

Furthermore, we will use Steven D. Galbraith's book "Mathematics of public key cryptography".

Topics:

During the introductory session, we will discuss the formal definition of lattices, some basic properties, successive minima, the Minkowski bounds and the computational problems (here we follow loosely Oded Regev's first lecture).

Then, during the next sessions, the participants need to prepare a talk about lattices or a lattice related topic. The talk topics for the participants can be any of the topics below or any related lattice oriented topic (the talks that need absolutely to be addressed are marked by a star):

- (*) The LLL-algorithm
  [A. Lenstra, H. Lenstra et L. Lovász - Factoring polynomials with rational coefficients]
- (*) Algorithms to solve the Closest Vector Problem (e.g Babai's nearest plane algorithm)
  [L. Babai - On Lovász' lattice reduction and the nearest lattice point problem]
- (*) Finding small solutions to small degree polynomials and attacks on low exponent RSA
  [Don Coppersmith - Finding small solutions to small degree polynomials]
- Integer programming in fixed dimension
  [A.I. Barvinok - A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed]
- (*) Algorithms to solve the Shortest Vector Problem (e.g. Ajtai-Kumar-Sivakumar)

[M. Ajtai, R. Kumar, and D. Sivakumar - A sieve algorithm for the shortest lattice vector problem]

- (*) Dual lattices and lattice completion
- Banaszczyk's transference theorems
  [W. Banaszczyk - New bounds in some transference theorems in the geometry of numbers]
- (*) Lattice cryptoschemes (Ajtai, NTRU, LWE,…)
  [Ajtai, Miklós (1996) - Generating Hard Instances of Lattice Problems]
  [Hoffstein, Jeffrey; Pipher, Jill; Silverman, Joseph H. - NTRU: A ring-based public key cryptosystem. Algorithmic Number Theory]
  [Regev, Oded - On Lattices, Learning with Errors, Random Linear Codes, and Cryptography.]
- Complexity results on lattice problems (CVP, GapCVP, SVP…)
  [O. Goldreich, D. Micciancio, S. Safra, and J.-P. Seifert - Approximating shortest lattice vectors is not harder than approximating closest lattice vectors]
  [D. Micciancio - The shortest vector problem is NP-hard to approximate to within some constant]
  [S. Khot - Hardness of approximating the shortest vector problem in lattices.]
- Finding short lattice vectors
  [N. Gama - Finding short lattice vectors within Mordell's Inequality]
- Lattice reduction algorithms (other than LLL) (e.g. BKZ, RSR, PDR)
- Reduction proofs based on the hardness of lattice problems (SIS…)

Luxembourg National Research Fund

Supported by the Luxembourg National Research Fund through grant PRIDE15/10621687/SPsquared.