Lattices and Cryptography: NTRUEncrypt

Danilo Ciaffi

May 26, 2016, 9:30, Room 1BC45

Abstract

The goal of the talk is to present the NTRUEncrypt method as a lattice-based method. This will be done in four steps:

- a brief introduction to lattices and their basic properties;
- which computational hard problems arise from lattices, namely SVP and CVP;
- the implementation of NTRUEncrypt;
- the connection between NTRUEncrypt and lattices.

References

[1] C. Bachoc, *Réseaux et Cryptographie*, Cryptanalyse course notes, `here`;

[2] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, Springer, 1979;

[3] J. Hoffstein, J. Pipher and J. H. Silverman, *An Introduction to Mathematical Cryptography*, Undergraduate Text in Mathematics, Springer, 2014.