Lattice based cryptography

Abderrahmane Nitaj (LMNO)

Lattice reduction is important in the cryptanalysis of various schemes such as RSA and NTRU. On the other side, the security of many cryptosystems is based on the hardness of specific problems in lattices. In this talk, we briefly review the theory of lattice reduction and present some applications in cryptanalysis and discuss the security of some cryptosystems and their connection to hard problems in lattices.