“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Vadim Lyubashevsky

(École Normale Supérieure, Paris)

"Efficient cryptography from generalized compact knapsacks."

Mar 16, 12:00am (New York Time).

Abstract:
I will first give a brief survey on the role of the knapsack problem in lattice-based cryptography and its relationship to all the problems upon which lattice-based protocols are based. Then I will describe a new lattice-based signature scheme which is based on the conjectured hardness of a natural average-case problem which can be seen as a hybrid between the Ring-LWE and the NTRU assumptions. The assumption roughly states that if we pick a polynomial r uniformly at random from a particular polynomial ring R, and polynomials s_1,s_2 at random from a small subset of R, then the pair (r,rs_1+s_2) is computationally indistinguishable from a uniformly random element in R x R. The resulting signature length of the signature scheme is under 9000 bits, which is a factor of six shorter than any previous lattice-based scheme of comparable security that also possesses a security reduction.

Next presentation: **Mar 30, 2011.** Groebner bases techniques in Cryptography
Ludovic Perret *(Laboratoire d'Informatique de Paris 6)*

Algebraic Cryptography Center