“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Chris Peikert

(Georgia Institute of Technology)

"Trapdoors for Lattices: Signatures, Identity-Based Encryption, and Beyond."

Mar 2, 12:00am (New York Time).

Abstract:

Lattices have recently emerged as a very attractive foundation for cryptography. Lattice-based schemes enjoy simple, highly parallel operations and very strong 'worst-case' security guarantees, including apparent resistance to quantum computers.

In this talk I will discuss a hierarchy of lattice 'trapdoors' and accompanying algorithms, and survey how they lead to a variety of versatile and powerful cryptographic applications, including signature schemes, CCA-secure encryption, and (hierarchical) identity-based encryption.

Next presentation: **Mar 16, 2011.** Efficient cryptography from generalized compact knapsacks
Vadim Lyubashevsky *(École Normale Supérieure, Paris)*

Algebraic Cryptography Center