“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Christopher Peikert

(Georgia Institute of Technology) **)**

"Pseudorandom Functions and Lattices."

Dec 8, 12:00pm (New York Time).

Abstract:

Pseudorandom function (PRF) families are a workhorse of symmetric cryptography, implying efficient solutions to most encryption and authentication problems. Existing constructions of PRFs fall into two broad classes: (1) heuristic designs like AES that withstand known cryptanalytic attacks and (2) theoretically sound ones where security is rigorously provable under simple assumptions, like the existence of one-way functions or the hardness of number-theoretic problems (e.g., factoring or computing discrete logs). All known constructions of the latter type, however, are either inherently sequential with large circuit depth, or have huge circuits and are breakable with quantum algorithms.

In this work we give "direct" constructions of pseudorandom function (PRF) families based on conjectured hard *lattice* problems and *learning* problems. Our constructions are asymptotically efficient and highly parallelizable in a practical sense, i.e., they can be computed by simple, relatively *small* low-depth arithmetic or boolean circuits (e.g., in NC^{1} or even TC^{0}). In addition, they are the first (theoretically sound) low-depth PRFs that have no known attack by efficient quantum algorithms. Central to our results is a new ``derandomization" technique for the learning with errors (LWE) problem which, in effect, generates the error terms deterministically.

This is recent joint work with Abhishek Banerjee (Georgia Tech) and Alon Rosen (IDC Herzliya).

Next presentation:

Algebraic Cryptography Center