“Symbolic Computations and Post-Quantum Cryptography” Online Seminar

Jintai Ding

(University of Cincinnati)

“Algebraic methods to solve lattice problems.”

Feb 23, 12:00pm (New York Time).

Abstract:
In this talk, we present a new algorithm to solve algebraically the following lattice-related problems:

1) the small integer solution (SIS) problem under the condition: if the solution is bounded by an integer β in l_∞ norm, which we call a bounded SIS (BSIS) problem, (and if the difference between the row dimension n and the column dimension m of the corresponding base matrix is relatively small with respect the row dimension m);
2) the learning with errors (LWE) problems under the condition: if the errors are bounded -- the errors do not span the whole prime finite field F_q but a fixed known subset of size D (D less than q), which we call a learning with bounded errors (LWBE) problem.

We will show that we can solve these problems with polynomial complexity.

Next presentation: **Mar08, 2012.** Grobner bases of structured systems and their applications in Cryptology
Pierre-Jean Spaenlehauer (LIP6-Universite Paris 6)

Algebraic
Cryptography
Center