“Symbolic Computations and Post-Quantum Cryptography” Online Seminar

Pierre-Jean Spaenlehauer

(LIP6-Universite Paris 6)

“Groebner bases of structured systems and their applications in Cryptology.”

Mar 08, 12:00pm (New York Time).

Abstract:

In this talk, we present new complexity bounds for solving bilinear and determinantal polynomial systems with Groebner bases algorithms. In particular, under genericity assumptions the exponential part of the complexity of solving an affine bilinear system f_1(X,Y)=...=f_{n_x+n_y}(X,Y)=0 (where X and Y are two sets of variables of cardinalities n_x and n_y) depends on min(n_x,n_y). This permits to identify families of bilinear systems which can be solved in complexity polynomial in the number of variables. We give similar complexity estimates for solving determinantal systems (systems of minors of a matrix whose entries are linear forms) by providing sharp bounds on the maximal degree in Groebner bases of such systems. Under genericity assumptions, we also identify subclasses of determinantal systems which can be solved in time polynomial in the size of the input.

Then we show how these complexity results can be used to measure the efficiency of algebraic attacks on HFE, on the MinRank authentication scheme and on some compact variants of the McEliece PKC. In particular, we give precise estimates of the computing effort needed to solve a challenge from the MinRank authentication scheme which seemed intractable so far.

Joint work with Jean-Charles Faugere and Mohab Safey El Din.

Next presentation: **Mar 22, 2012.** Confusing Eavesdroppers with Algebraic Number Theory
Camilla Hollanti (Aalto University, Finland)

Algebraic
Cryptography
Center