“Symbolic Computations and Post-Quantum Cryptography” Online Seminar

Ludovic Perret

(Laboratoire d'Informatique de Paris 6)

"Groebner bases techniques in Cryptography. ."

Mar 30, 12:00am (New York Time).

Abstract:

Algebraic cryptanalysis can be described as a general framework allowing to asses the security of a wide range of cryptographic schemes. The recent proposal and development of algebraic cryptanalysis is now widely considered as an important breakthrough in the analysis of cryptographic primitives. It is a powerful technique that applies potentially to a wide range of cryptosystems.

The basic principle of such cryptanalysis is to model a cryptographic primitive by a set of algebraic equations. The system of equations is constructed in such a way as to have a correspondence between the solutions of this system, and a secret information of the cryptographic primitive (for instance, the secret key of a block cipher).

The most efficient method for solving algebraic equations over a finite field is to compute a Gröbner basis. In the first part of this talk, we will give the definition/properties of such bases, and briefly recall the complexity of efficient algorithms for computing these bases, i.e. Faugère's F4 or F5 algorithms.

In the second part of the talk, we will focus our attention on the MinRank problem. This is a basic linear algebra problem: given a set of several matrices, the goal of MinRank is to find a linear combination of these matrices having a small rank. Suprisingly enough, MinRank has many applications in cryptography and coding theory. In the last part of my talk, we will present an algebraic attack against an authentication scheme based on MinRank as well as cryptanalysis of Multivariate and Odd-Characteristic HFE.

(joint work with L. Bettale, J.-C. Faugère, and F. Levy-dit-Vehel)

Next presentation: **Apr 13, 2011.** Groebner bases for non-commutative polynomials and applications
to cryptography
Martin Kreuzer *(Universitat Passau)*

Algebraic
Cryptography
Center