1071-42-247 **Ludovic Perret*** (ludovic.perret@lip6.fr), LIP6 University Paris 6, 4, place Jussieu, 75005 Paris, France. *Groebner Bases Techniques in Cryptography.*

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 principle of efficient algorithms, i.e. F4/F4, for computing these bases.

In the second part of the talk, we will review recent appliactions of such techniques in public key cryptography. (Received March 07, 2011)