Universidad Complutense de Madrid
Facultad de Ciencias Matemáticas
Departamento de Algebra
Teléfono: 91 394 45 70, Fax: 91 394 46 62
Correo electrónico: Algebra@mat.ucm.es

SEMINARIO DE GEOMETRÍA ALGEBRAICA

Lunes 24 de mayo de 2010, **13:00**, Seminario 238

Carlo Traverso

Università degli Studi di Pisa

Impartirá la conferencia

Lattice Polly Cracker

Resumen.
An integer lattice is a subgroup of Z_n. To a lattice L we can associate a binomial ideal I_L included in $k[X] = k[x_1, ..., x_n]$, each binomial $X^\alpha - X^\beta$ being associated to $\alpha - \beta$.

Lattice Polly Cracker (LPC) is a cryptosystem exploiting the knowledge of a Gröbner basis of I_L, in which decryption is obtained through normal form, and encryption is obtained adding to an element of Z_n that is inside the staircase an element of L.

To obtain such a Gröbner basis in reasonable time L has to be very special, and its structure has to be concealed through a change of variables, otherwise an attacker can compute it too. We discuss how this can be made, and the overall performance of LPC, that is substantially better of some cryptosystems like GGH.

GGH is similar to LPC from the public point of view, but does not use Gröbner bases, depending instead on an almost-orthogonal private lattice basis, and has much worse message expansion and key size and presumable security given the same message length.

We also show how LPC, like other lattice cryptosystems, can give origin to a signature algorithm. This, like other lattice signature schemes, is subject to a staircase learning attack that could allow to recover the change of coordinates, hence the Gröbner basis after a suitable number of signatures. We discuss how this can be avoided by perturbing the signature; this perturbation technique is different from the perturbation techniques used for other lattice signature schemes like NTRUSign.