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

Jueves 21 de julio de 2016, **13:00**, Seminario 238

Jintai Ding

University of Cincinnati

Impartirá la conferencia

Multivariate public key cryptosystems

Resumen.

Multivariate public key cryptosystems (MPKC) are one of the four main families of post-quantum public key cryptosystems. In a MPKC, the public key is given by a set of quadratic polynomials and its security is based on the hardness of solving a set of multivariate polynomials. This lecture gives a general introduction to the multivariate public key cryptosystems including the main designs, the main attack tools and the mathematical theory behind. We will present state of the art research in the area.