COLOQUIO PRØBEMOS

Ignacio Luengo Velasco

Universidad Complutense de Madrid

Criptografía postcuántica con polinomios

Resumen: La criptografía postcuántica es la criptografía de clave pública resistente a las futuras computadoras cuánticas. En esta charla hablaremos de un criptosistema postcuántico llamado DME (*Double Matrix Exponentiation*). El sistema está basado en aplicaciones de polinomios multivariables que hemos desarrollado (usando ideas de Geometría Algebraica), patentado y presentado en el concurso NIST para elegir el futuro estándar de criptografía postcuántica.

También presentaremos algunas cuestiones y problemas de Álgebra Conmutativa relacionados con el criptoanálisis algebraico del esquema DME.

Fecha: Jueves 10 de mayo de 2018, a las 12:00 horas.
Lugar: **IMAC** **(***Seminario TI1329SD),* ESTCE. Universitat Jaume I.