FACULTAD DE
CC. MATEMÁTICAS

COLOQUIO MATEMÁTICO

Instituto de Matemática Interdisciplinar

Ronald Cramer

CWI, Amsterdam & Mathematical Institute, Leiden University

Algebraic Geometric Secret Sharing Schemes and Secure Computation over Small Fields

The Algebraic geometry has had a tremendous impact on the theory of error correcting codes in the 1980s and 1990s through Goppa-codes based oncurves with many rational points. Our results show a novel, similar impactof algebraic geometry on an important but complex cryptographic primitive,secure computation.

3 de mayo de 2007. 13:00

Aula Miguel de Guzmán (S-118)