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 4 de mayo de 2015, **13:00**, Seminario 238

María Isabel González Vasco

Universidad Rey Juan Carlos

Impartirá la conferencia

Size-Hiding Private Set Intersection

Resumen.
The Private Set Intersection (PSI) problem deals which a situation in which two mutually distrusting parties, each holding a set of inputs from a fixed ground set, wish to jointly compute the intersection of their sets without leaking any additional information. Typically, cryptographic solutions to PSI allow interaction between a Server $\mathcal{S}$ and Client C , with respective private input sets $\mathcal{C} = \{c_1; \dots; c_v\}; \mathcal{S} = \{s_1; \dots; s_w\}$, both drawn from a ground set $\mathcal{U}$: At the end of the interaction, $\mathcal{C}$ learns $\mathcal{S} \cap \mathcal{C}$ and $|\mathcal{S}|$, while $\mathcal{S}$ learns nothing beyond $|\mathcal{C}|$. Over the last few years, the research community has devised a number of PSI techniques under different security models. In this talk, we will revise these solutions and direct our attention to those who exhibit the extra feature of keeping the size of the input sets secret; we will in particular focus on recent results which are part of a joint work with Paolo D'Arco, Angel L. Pérez del Pozo and Claudio Soriente. In particular we we will discuss a new generic construction without random oracles for the unbalanced setting, where only the client gets the intersection and hides the size of its set of secrets. The main tool behind this design are smooth projective hash functions for languages derived from perfectly-binding commitments. We stand on the seminal ideas of Cramer - Shoup and Gennaro-Lindell, which have already found applications in several other contexts, such as password-based authenticated key exchange and oblivious transfer.