Universidad Carlos III de Madrid
Department of Mathematics

COLLOQUIA

Jueves, 12 de marzo de 2015.

María Isabel González Vasco (Universidad Rey Juan Carlos)

Multi-Party Computation: Cryptography for the not so good, the not so bad and the not so ugly

Resumen:

In this talk, our goal is to present the field of *Multiparty Computation* (MPC), providing a glimpse of its multiple application scenarios and illustrating the wide variety of mathematical areas that come into play within this field. Multiparty Computation surfaces whenever we have a number of parties, each possessing some private data, which want to cooperatively perform some computation needing this data as input while keeping their private data as confidential as possible. Different (general, or dedicated) protocols have been proposed in this field since the eighties. Sometimes, no computational assumption on the parties is made, thus, many MPC protocols are proven secure in an information theoretical sense. Often, the presence of a *trusted third party* needs to be assumed in order to achieve an effective solution. After reviewing some central results in the field, we will comment on some cryptographic constructions closely related to MPC, like secret sharing, coin tossing or oblivious transfer and provide some insight of the mathematical primitives they are build upon. To conclude, we will devote some time to the so called *Private Set Intersection Problem* (PSI), which deals with 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 $\boldsymbol{S}$ and Client $\boldsymbol{C}$, with respective private input sets $\mathcal{C} = \{c_1, \ldots, c_v\}$, $\mathcal{S} = \{s_1, \ldots, s_w\}$, both drawn from a ground set $\mathcal{U}$. At the end of the interaction, $\boldsymbol{C}$ learns $\mathcal{S} \cap \mathcal{C}$ and $|\mathcal{S}|$, while $\boldsymbol{S}$ learns nothing beyond $|\mathcal{C}|$. We will revise some of the solutions available for this problem 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.

Univ. Carlos III de Madrid

Coordenadas

Hora 11:00 - 12:00
Lugar Seminario del Departamento de Matemáticas
2.2 D08 Edificio Sabatini.

Dirección

Avda. de la Universidad 30
28911, Leganés, Madrid

Department of Mathematics