SEMINARIO DE ANÁLISIS Y APLICACIONES

Viernes, 12 de febrero de 2021

11:30 h., ONLINE - URL: https://zoom.us/j/99697372954

David Pérez García

Universidad Complutense de Madrid

Sobolev-type Inequalities in Position Based Cryptography

Resumen:

The goal of this talk is to present a new setup where quantum information, high energy physics and functional inequalities meet: position based cryptography. In the field of position based cryptography one aims to develop cryptographic tasks using the geographical position of an agent as its only credential. Once the agent proved to the verifier that he/she is in fact at the claimed position, they interact considering the identity of the agent as guaranteed. This proposal is appealing for practical applications and it is also of fundamental interest since it presents a way to prevent man-in-the-middle attacks without the need of a secure private channel. Furthermore, since the study of position based cryptography entered into the quantum domain approximately a decade ago, beautiful and striking connections were established with topics ranging from classical complexity theory to the AdS/CFT holographic correspondence. I this talk, I will present a new connection with geometric functional analysis that allows us to use a Sobolev-type inequality due to Pisier for vector-valued functions on the boolean hypercube. Using it as a key tool, we will provide new lower bounds on the entanglement consumption needed to break position based cryptography.

(Joint work with Marius Junge, Aleksander M. Kubicki and Carlos Palazuelos.)

ICMAT CSIC-UAM-UC3M-UCM
Departamento de Matemáticas. U.A.M.