DPTO. DE ANÁLISIS MATEMÁTICO

Seminario Informal de Información Cuántica

Instituto de Matemática Interdisciplinar

Serge Fehr

(CWI, Amsterdam)

Secure Identification in the Bounded-Quantum-Storage Model

How do you convince an ATM that you know your PIN? You type it into the ATM! From a security point of view, this common practice is very vulnerable: it allows a malicious ATM to immediately learn your PIN. Phrased in a general context, we consider the following problem: how can a user U "prove" to a server S that he knows an agree-upon key (or password or PIN) W, in such a way that a malicious server does not learn W? Even stronger, we require that in every execution, a dishonest server can exclude at most one possibility for W. We propose a solution in the bounded-quantum-storage model, which is a very reasonable assumption. In this talk, I will gradually build up our scheme and provide some intuition for why it is secure and how the formal security proof looks like.

11 de julio de 2007, 12h00

Seminario (222)

Dpto. de Análisis Matemático

Facultad de CC. Matemáticas