DEPARTAMENTO DE
ANÁLISIS MATEMÁTICO

Conferencia
Seminario de Información Cuántica

Instituto de
Matemática
Interdisciplinar

Lluis Masanes
ICFO, Barcelona

Key distribution from causality constrains

By assuming the impossibility of arbitrarily-fast signaling, secret key distribution can be implemnted from correlations that sufficiently violate a Bell inequality. A general security proof is presented according to the strongest notion of security, the so called universally-composable security. The no-signaling assumption is imposed at the level of outcome probabilities only, therefore, the protocol remains secure in situations where the honest parties distrust their quantum apparatuses. In our scheme, Bell inequalities play the role usually associated to entropies, and randomness is extracted by processing outcomes of Bell-violating measurements with a constant hash function. This contrasts with previous schemes in classical/quantm information theory (e.g. two-universal hashing, extractors), where the hash function is necessarily random.

9 de julio de 2008
12:00 horas, Seminario 222
Facultad de Matemáticas, UCM