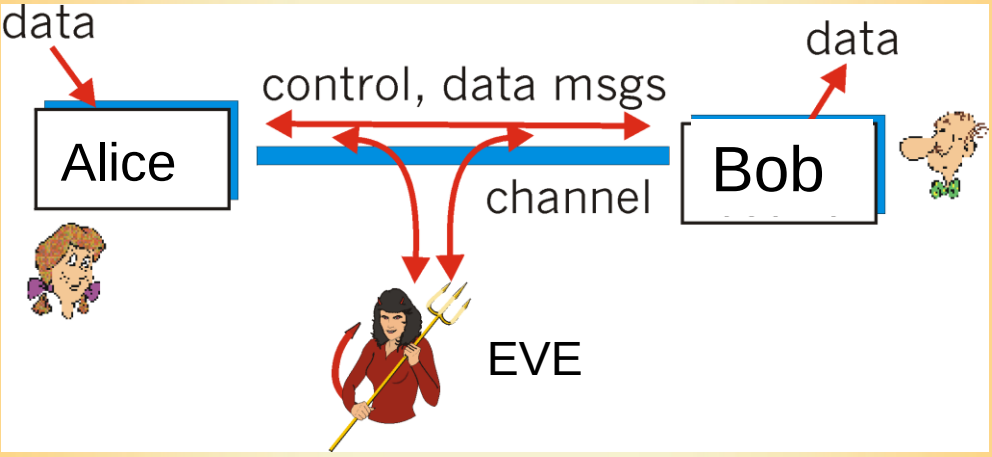
Seminários de Física
Centro de Física da Universidade do Minho

Quarta-Feira, 8 de Fevereiro às 14:30h
Auditório da Escola de Ciências

A Universal Quantum Layer

Armando Nolasco Pinto;
Departamento de Eletrónica, Telecomunicações e Informática,
Universidade de Aveiro
Instituto de Telecomunicações, Aveiro



Resumo: **S**ecurity and privacy in communication networks is nowadays provided by classical cryptography. Classical cryptography is based on computational complexity which is known to be vulnerable to attacks after some processing delay. The length of this delay can nowadays be made extremely large, making possible to make virtually all attacks useless, however the rise of quantum computers is going to shrink this delay making possible, if nothing is done, almost real-time attacks. Quantum cryptography can solve this problem by building cryptographic schemes that take advantage of quantum theory that has been tested and validated for more than a century. Nevertheless, quantum cryptography still presents several limitations as the reach, speed and possibility of co-existence in the already installed infra-structures. In this talk we are going to present the basis ideas behind quantum cryptography, showing the state-of-the-art technologies and discuss the major topics under research.