RELATORE

Prof. Massimo Palma (Università di Palermo)

LUOGO e ORA

Aula C, martedì 29 novembre 2011, ore 16:30

TITOLO

Quantum Key Distribution:

Il contributo della meccanica quantistica alla sicurezza

ABSTRACT:

Le leggi della meccanica quantistica consentono l'implementazione di protocolli di codifica, elaborazione e trasmissione dell'informazione privi di analogo classico. Il più celebrato di tali protocolli è la crittografia quantistica – o più propriamente Quantum Key Distribution (QKD). Tale successo è dovuto in parte alla relativa semplicità concettuale degli aspetti fondamentali del protocollo e in parte al fatto che esistono già dispositivi “plug and play” che consentono la distribuzione di chiavi crittografiche su reti di fibre ottiche cittadine. L'analisi della sicurezza nei protocolli di QKD ha raggiunto notevoli livelli di sofisticatezza e tocca aspetti fondamentali della meccanica quantistica.

In questo seminario verranno illustrati le idee di fondo alla base del protocollo di QKD e verranno illustrate le sue principali versioni.

La presentazione sarà il più possibile autoconsistente e non si presuppone alcuna conoscenza della meccanica quantistica.