DEPARTAMENTO DE
ANÁLISIS MATEMÁTICO

Instituto de
Matemática
Interdisciplinar

Curso de QI

M. Curty

Universidad de Vigo

"Sistemas cuánticos de comunicaciones para distribución de claves criptográficas"

Debido al crecimiento continuo de las redes abiertas de ordenadores, con millones de usuarios accediendo a las mismas desde terminales diferentes, la protección de la información se ha vuelto imprescindible, especialmente en las operaciones de índole comercial y financiero que realizan las empresas a través de la red. La protección de la información está fuertemente relacionada con uno de los principales servicios criptográficos: La confidencialidad. Su objetivo es garantizar la transmisión de información secreta a través de una canal de comunicaciones abierto.

En este curso se introducen diversos sistemas cuánticos de comunicaciones que permiten garantizar confidencialidad absoluta en la transmisión de información, gracias a la explotación de efectos cuánticos de la luz. Asimismo, se presenta el principal protocolo implementado en los prototipos comerciales, denominado protocolo BB84. Se analiza su seguridad, tanto en el caso de una realización fotónica ideal, como en el caso de una implementación basada en pulsos de luz coherente fuertemente atenuados. Finalmente, se evalúan diversos prototipos comerciales desarrollados recientemente por las principales empresas de Telecomunicación.

Organizado por el Grupo "Matemáticas e Información Cuántica" de la UCM
en colaboración con el IMI.

12-16 de abril de 2010, de10:30 a 12:30 horas

Seminario 222

Facultad de Ciencias Matemáticas, UCM.