Guía docente
230988 - QCRYP - Criptografía Cuántica

Última modificación: 08/05/2025

Unidad responsable: Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona
Unidad que imparte: 739 - TSC - Departamento de Teoría de la Señal y Comunicaciones.

Titulación: MÁSTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIÓN (Plan 2013). (Asignatura optativa).
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS AVANZADAS DE TELECOMUNICACIÓN (Plan 2019). (Asignatura optativa).
MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD (Plan 2020). (Asignatura optativa).

Curso: 2025 **Créditos ECTS:** 5.0 **Idiomas:** Inglés

PROFESORADO

Profesorado responsable: JAVIER RODRIGUEZ FONOLLOSA

Otros:

CAPACIDADES PREVIAS

Conocimientos sólidos de álgebra lineal y teoría de la probabilidad.

METODOLOGÍAS DOCENTES

- Cases de teoría.
- Probremas a resolver individualmente o en grupo por el estudiante.
- Prácticas de laboratorio y ejercicios.

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

Esta asignatura combina dos de las ramas más importantes de la ciencia del siglo XX, la teoría cuántica desarrollada en los años veinte y treinta por científicos como Planck, Einstein, Bohr, Heisenberg, Schrödinger, Pauli, Dirac y von Neumann, y la teoría de la información, nacida tras los trabajos de Shannon en 1948. Se presentarán los postulados básicos de los sistemas cuánticos, así como su modelo matemático. A continuación se tratan los protocolos de distribución cuántica de claves, que pueden utilizarse para implementar un criptosistema clásico de clave privada con seguridad garantizada. Para ello es necesario introducir la corrección cuántica de errores y los conceptos de seguridad de la capa física. La última parte del curso introduce el área de la computación cuántica como el marco algorítmico regido por las leyes de la mecánica cuántica que promete, entre otros logros notables, romper el criptosistema de clave pública RSA.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas grupo grande	26,0	20.80
Horas aprendizaje autónomo	86,0	68.80
Horas grupo pequeño	13,0	10.40

Dedicación total: 125 h

CONTENIDOS

Introducción a la teoría de la información cuántica.

Descripción:
a) Introducción a la Mecánica Cuántica: el artículo EPR, el Big Bell Test y esquema del curso.
b) Estados cuánticos: la esfera de Bloch, la descomposición espectral, la evolución, la medida reversible y la regla del Born, el experimento y la medida de Stern-Gerlach basado en POVM.
c) Sistemas cuánticos compuestos: descripción del producto de Kronecker, teorema de no clonación, estados separables y entrelazados, la descomposición de Schmidt, traza parcial, purificación, entrelazamiento como recurso y la violación de la desigualdad CHSH.
d) Protocolos cuánticos: distribución de entrelazamiento, codificación súper densa y teletransportación cuántica.

Actividades vinculadas:
Práctica de laboratorio de medidas, entrelazamiento, tomografía y protocolos.

Dedicación: 12h
Grupo grande/Teoría: 8h
Grupo mediano/Prácticas: 4h

Criptografía cuántica.

Descripción:
a) Corrección de error cuántico: códigos de repetición y el código Shor, revisión de códigos lineales clásicos y códigos CSS.
b) Seguridad de la capa física: el canal wiretap, comunicación de clave secreta, acuerdo de clave secreta para el modelo de fuente, clave de destilación secuencial y el modelo del canal.
c) Distribución de claves cuánticas: los protocolos BB84, B92 y EPR y los protocolos seguros CSS y BB84.

Actividades vinculadas:
Prácticas de laboratorio de códigos de corrección de errores y QKD.

Dedicación: 15h
Grupo grande/Teoría: 10h
Grupo mediano/Prácticas: 5h

Computación cuántica

Descripción:
a) Transformada cuántica de Fourier.
b) Estimación de fase, búsqueda de orden y algoritmo de Shor para la factorización de enteros.

Actividades vinculadas:
Prácticas de laboratorio de estimación de fase y algoritmo de Shor.

Dedicación: 12h
Grupo grande/Teoría: 8h
Grupo mediano/Prácticas: 4h

SISTEMA DE CALIFICACIÓN

- La asistencia es obligatoria.
- Problemas (15%), prácticas de laboratorio (50%) y presentación final en grupo o individual (35%).

NORMAS PARA LA REALIZACIÓN DE LAS PRUEBAS.

No hay examen final.

BIBLIOGRAFÍA

Básica:
- Nielsen, Michael A; Chuang, Isaac L. Quantum computation and quantum information. 10th anniversary ed. Cambridge, UK: Cambridge University Press, cop. 2010. ISBN 9781107002173.
- Bloch, Matthieu; Barros, João. Physical-layer security : from information theory to security engineering. Cambridge: Cambridge University Press, cop. 2011. ISBN 9780521516501.
- Wilde, Mark. Quantum information theory. Second edition. 2017. ISBN 9781107176164.