Guia docent
230988 - QCRYP - Criptografia Quàntica

Última modificació: 08/05/2025

Unitat responsable: Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
Unitat que imparteix: 739 - TSC - Departament de Teoria del Senyal i Comunicacions.

Titulació: MÀSTER UNIVERSITARI EN ENGINYERIA DE TELECOMUNICACIÓ (Pla 2013). (Assignatura optativa).
MÀSTER UNIVERSITARI EN TECNOLOGIES AVANÇADES DE TELECOMUNICACIÓ (Pla 2019). (Assignatura optativa).
MÀSTER UNIVERSITARI EN CIBERSEGURETAT (Pla 2020). (Assignatura optativa).

Curs: 2025 **Crèdits ECTS:** 5.0 **Idiomes:** Anglès

PROFESSORAT

Professorat responsable: JAVIER RODRIGUEZ FONOLLOSA

Altres:

CAPACITATS PRÈVIES

Coneixements sòlids d'àlgebra lineal i teoria de la probabilitat.

METODOLOGIES DOCENTS

- Classes de teoria.
- Problemes teòrics a resoldre individualment o en grup per l'estudiant.
- Pràctiques de laboratori i exercicis.

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

Aquesta assignatura combina dues de les branques més importants de la ciència del segle XX, la teoria quàntica desenvolupada als anys vint i trenta per científics com Planck, Einstein, Bohr, Heisenberg, Schrödinger, Pauli, Dirac i von Neumann, i la teoria de la informació, nascuda després dels treballs de Shannon el 1948. Es presentaran els postulats bàsics dels sistemes quàntics, així com el seu model matemàtic. A continuació es tracten els protocols de distribució quàntica de claus, que es poden utilitzar per implementar un criptosistema clàssic de clau privada amb seguretat garantida. Per fer-ho, cal introduir la correcció quàntica d'errors i els conceptes de seguretat de la capa física. L'última part del curs introdueix l'àrea de la computació quàntica com a marc algorítmic regit per les lleis de la mecànica quàntica que promet, entre d'altres fites notables, trencar el criptosistema de clau pública RSA.

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores grup petit	13,0	10.40
Hores grup gran	26,0	20.80
Hores aprenentatge autònom	86,0	68.80

Dedicació total: 125 h

CONTINGUTS

Introducció a la teoria de la informació quàntica.

Descripció:
a) Introducció a la Mecànica Quàntica: l'article EPR, el Big Bell Test i esquema del curs.
b) Estats quàntics: l'esfera de Bloch, la descomposició espectral, l'evolució, la mesura reversible i la regla del Born, l'experiment i la mesura de Stern-Gerlach basat en POVM.
c) Sistemes quàntics compostos: descripció del producte de Kronecker, teorema de no clonació, estats separables i entrellaçats, la descomposició de Schmidt, traça parcial, purificació, entrellaçament com a recurs i la violació de la desigualtat CHSH.
d) Protocols quàntics: distribució d'entrellaçament, codificació súper densa i teletransportació quàntica.

Activitats vinculades:
Pràctica de laboratori de mesures, entrellaçament, tomografia i protocols.

Dedicació: 12h
Grup gran/Teoria: 8h
Grup mitjà/Pràctiques: 4h

Criptografia quàntica.

Descripció:
a) Correcció quàntica d'errors: codis de repetició i el codi Shor, revisió de codis lineals clàssics i codis CSS.
b) Seguretat de capes físiques: el canal wiretap, comunicació de claus secreta, acord de clau secreta pel model font, destil·lació seqüencial de claus i model de canal.
c) Distribució de claus quàntiques: els protocols BB84, B92 i EPR i protocols CSS i BB84 segurs.

Activitats vinculades:
Pràctiques de laboratori de codis de correcció d'errors i QKD.

Dedicació: 15h
Grup gran/Teoria: 10h
Grup mitjà/Pràctiques: 5h

Computació quàntica

Descripció:
a) Transformada quàntica de Fourier.
b) Estimació de fases, càlcul d'ordre i algorisme de Shor per a la factorització entera.

Activitats vinculades:
Pràctiques de laboratori d'estimació de fase i algorisme de Shor.

Dedicació: 12h
Grup gran/Teoria: 8h
Grup mitjà/Pràctiques: 4h

SISTEMA DE QUALIFICACIÓ

- L'assistència és obligatòria.
- Problemes (15%), pràctiques de laboratori (50%) i presentació final en grup o individual (35%).

NORMES PER A LA REALITZACIÓ DE LES PROVES.

No hi ha examen final.

BIBLIOGRAFIA

Bàsica:
- 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.