Criptografía y comunicación cuánticas

MÁSTER UNIVERSITARIO EN TECNOLOGÍAS CUÁNTICAS

UNIVERSIDAD INTERNACIONAL MENÉNDEZ PELAYO

Másteres Universitarios

Este documento puede utilizarse como documentación de referencia de esta asignatura para la solicitud de reconocimiento de créditos en otros estudios. Para su plena validez debe estar sellado por la Secretaría de Estudiantes UIMP.

DATOS GENERALES

Título asignatura

Criptografía y comunicación cuánticas

Código asignatura

102771

Curso académico

2024-25

Planes donde se imparte

MÁSTER UNIVERSITARIO EN TECNOLOGÍAS CUÁNTICAS

Créditos ECTS

6

Carácter de la asignatura

OPTATIVA

Duración

Cuatrimestral

Idioma

Inglés

CONTENIDOS

Contenidos

Esta asignatura ofrece un programa completo sobre la capacidad de los sistemas cuánticos para transmitir información y distribuir claves para la comunicación segura de datos por medios clásicos. La asignatura cubre los aspectos teóricos más importantes, protocolos fundamentales, aplicaciones en sistemas físicos concretos y la integración de esta tecnología en las redes digitales ya existentes.

- Introducción a la criptografía clásica y cuántica.
- Protocolos de distribución cuántica de clave.
- Seguridad de la distribución cuántica de clave.
- Implementaciones tecnológicas.
- Limitaciones físicas y fundamentales.
- Redes de distribución cuántica de clave.
- Seguridad de las implementaciones y hackeo cuántico.
- Repetidores cuánticos.
- Otras aplicaciones de la criptografía cuántica.

RESULTADOS DE APRENDIZAJE Y DE FORMACIÓN

Generales

RFA a nivel de Contenidos

RFA2 Entender el procesado de la información usando sistemas cuánticos, como qubits, puertas cuánticas, medidas, entrelazamiento, correlación, y limitaciones fundamentales y complejidad cuántica de algoritmos y operaciones.

RFA3 Identificar conceptos avanzados en el estudio mecano-cuántico de sistemas físicos de muchos cuerpos, fundamentos de interacción luz-materia, elementos de sistemas abiertos y topología.

RFA5 Conocer las principales implementaciones físicas de las tecnologías cuánticas y comprender sus principios de funcionamiento.

RFA a nivel de Competencias

RFA6 Diseñar, organizar e implementar un evento científico para la presentación del estado del arte en un campo de investigación.

RFA7 Atender, comprender e interpretar una charla científica en un ámbito de investigación de frontera de las tecnologías cuánticas, así como desarrollar una exposición crítica de los resultados presentados.

RFA9 Desarrollar capacidad de análisis, razonamiento crítico y resolución de problemas.

RFA10 Trabajar en equipo de forma activa compartiendo información y tareas para lograr la consecución de los objetivos previstos.

RFA11 Desarrollar proyectos básicos de investigación de forma autónoma.

RFA12 Redactar documentos científicos y técnicos, en particular artículos científicos.

RFA13 Realizar presentaciones sobre una investigación o proyecto científico ante públicos especializados.

RFA14 Buscar, obtener, procesar, comunicar información y transformarla en conocimiento.

RFA15 Conocer las herramientas metodológicas necesarias para desarrollar proyectos de investigación.

RFA a nivel de Habilidades o destrezas

RFA16 Aplicar conocimiento teórico relacionado con las tecnologías cuánticas en el ámbito de la investigación básica.

RFA17 Aplicar conocimiento teórico relacionado con las tecnologías cuánticas en el ámbito de la

investigación aplicada y el desarrollo tecnológico.

RFA18 Aplicar conocimiento práctico relacionado con las tecnologías cuánticas en el ámbito de la investigación básica.

RFA19 Aplicar conocimiento práctico relacionado con las tecnologías cuánticas en el ámbito de la investigación aplicada y el desarrollo tecnológico.

PLAN DE APRENDIZAJE

Actividades formativas

Lección magistral

Clase práctica

Tutorías individuales y/o colectivas

Estudio individual y trabajo autónomo del estudiante

Elaboración de trabajos individuales y/o en grupo

Metodologías docentes

Clases magistrales

Resolución de casos prácticos

Prácticas de programación o de laboratorio

Ponencias sobre los trabajos o entregables de problemas

Seminarios y conferencias

Tutorías individuales y/o colectivas

SISTEMA DE EVALUACIÓN

Descripción del sistema de evaluación

Valoración de la participación en tutorías (ponderación mínima 10.0 y ponderación máxima 30.0)

Valoración de informe, prácticas y trabajos individuales o en grupo (ponderación mínima 20.0 y ponderación máxima 50.0)

Valoración de exposiciones orales de trabajos (ponderación mínima 20.0 y ponderación máxima 50.0)

Valoración del examen final oral o escrito (ponderación mínima 40.0 y ponderación máxima 80.0)

PROFESORADO

Profesor responsable

Curty Alonso, Marcos

DOCTOR INGENIERO DE TELECOMUNICACIÓN
DOCTOR EN FÍSICA.
CATEDRÁTICO DE UNIVERSIDAD (AREA TEORIA DE LA SEÑAL Y COMUNICACIONES).
UNIVERSIDAD DE VIGO.

Profesorado

Fernández Mármol, Verónica

Científica titular
ITEFI-CSIC

Martín Ayuso, Vicente

Doctor en Ciencias Físicas.
Catedrático (Ciencias de la Computación).
Univ. Politécnica de Madrid /Center for Computational simulation.

Balado Souto, Daniel

DOCTOR EN FÍSICA.
CONTRATADO MOMENTUM CSIC.
Instituto de Tecnologías Físicas y de la Información ¿Leonardo Torres Quevedo¿ (ITEFI)

Faba García, Javier

Doctor en Física.
Profesor Ayudante Doctor.
Universidad Politécnica de Madrid / ETS de Ingenieros Informáticos / DATSI.

Currás Lorenzo, Guillermo

Doctor
Investigador Postdoctoral

Vigo Quantum Communication Center, Universidad de Vigo

HORARIO

Horario

28/10/2024

10:00 - 13:00

UD1.1 Public-key and symmetric key classical cryptography. Introduction to post-quantum cryptography (video)

Vicente Martín Ayuso

Doctor en Ciencias Físicas.
Catedrático (Ciencias de la Computación).
Univ. Politécnica de Madrid /Center for Computational simulation.

04/11/2024

10:00 - 10:30

UD 2.1 Quantum cryptography (vídeo)

Marcos Curty Alonso

DOCTOR INGENIERO DE TELECOMUNICACIÓN
DOCTOR EN FÍSICA.
CATEDRÁTICO DE UNIVERSIDAD (AREA TEORIA DE LA SEÑAL Y COMUNICACIONES).
UNIVERSIDAD DE VIGO.

10:30 - 11:30

UD 2.2 Introduction to QKD protocols: Prepare and measure (vídeo)

Marcos Curty Alonso

DOCTOR INGENIERO DE TELECOMUNICACIÓN
DOCTOR EN FÍSICA.

CATEDRÁTICO DE UNIVERSIDAD (AREA TEORIA DE LA SEÑAL Y COMUNICACIONES).
UNIVERSIDAD DE VIGO.

11:30 - 12:30

UD 2.3 Entanglement-based and interference-based QKD protocols (video)

Marcos Curty Alonso

DOCTOR INGENIERO DE TELECOMUNICACIÓN
DOCTOR EN FÍSICA.
CATEDRÁTICO DE UNIVERSIDAD (AREA TEORIA DE LA SEÑAL Y COMUNICACIONES).
UNIVERSIDAD DE VIGO.

12:30 - 13:30

UD 2.4 Security framework of QKD and quantum optics tools (video)

Marcos Curty Alonso

DOCTOR INGENIERO DE TELECOMUNICACIÓN
DOCTOR EN FÍSICA.
CATEDRÁTICO DE UNIVERSIDAD (AREA TEORIA DE LA SEÑAL Y COMUNICACIONES).
UNIVERSIDAD DE VIGO.

08/11/2024

17:00 - 19:00

UD. 1.2 Exercice class on Public-key and symmetric key classical cryptography. Introduction to post-quantum cryptography (streaming)

Vicente Martín Ayuso

Doctor en Ciencias Físicas.

Catedrático (Ciencias de la Computación).
Univ. Politécnica de Madrid /Center for Computational simulation.

11/11/2024

10:00 - 11:00

UD 2.5 Linear optical elements in QKD protocols (video)

Marcos Curty Alonso

DOCTOR INGENIERO DE TELECOMUNICACIÓN
DOCTOR EN FÍSICA.
CATEDRÁTICO DE UNIVERSIDAD (AREA TEORIA DE LA SEÑAL Y COMUNICACIONES).
UNIVERSIDAD DE VIGO.

11:00 - 12:30

UD 2.6.1 QKD with coherent states (video)

Marcos Curty Alonso

DOCTOR INGENIERO DE TELECOMUNICACIÓN
DOCTOR EN FÍSICA.
CATEDRÁTICO DE UNIVERSIDAD (AREA TEORIA DE LA SEÑAL Y COMUNICACIONES).
UNIVERSIDAD DE VIGO.

18/11/2024

10:00 - 11:00

UD 3.1 Security of QKD I (video)

Guillermo Currás Lorenzo

Doctor

Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

11:00 - 12:00

UD 3.2 Security of QKD II (video)

Guillermo Currás Lorenzo

Doctor
Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

20/11/2024

16:15 - 17:15

UD 2.6.2 Exercise class on QKD with practical signals I (streaming)

Marcos Curty Alonso

DOCTOR INGENIERO DE TELECOMUNICACIÓN
DOCTOR EN FÍSICA.
CATEDRÁTICO DE UNIVERSIDAD (AREA TEORIA DE LA SEÑAL Y COMUNICACIONES).
UNIVERSIDAD DE VIGO.

22/11/2024

16:15 - 17:15

UD 2.6.3 Exercise class on QKD with practical signals II (streaming)

Marcos Curty Alonso

DOCTOR INGENIERO DE TELECOMUNICACIÓN
DOCTOR EN FÍSICA.
CATEDRÁTICO DE UNIVERSIDAD (AREA TEORIA DE LA SEÑAL Y COMUNICACIONES).

UNIVERSIDAD DE VIGO.

26/11/2024

10:00 - 11:00

UD 4.1.1 Single-photon sources and detectors, and entanglement sources (vídeo)

Daniel Balado Souto

DOCTOR EN FÍSICA.
CONTRATADO MOMENTUM CSIC.
Instituto de Tecnologías Físicas y de la Información ¿Leonardo Torres Quevedo¿ (ITEFI)

11:00 - 12:00

UD 4.1.2 Generation and detection of coherent light (vídeo)

Daniel Balado Souto

DOCTOR EN FÍSICA.
CONTRATADO MOMENTUM CSIC.
Instituto de Tecnologías Físicas y de la Información ¿Leonardo Torres Quevedo¿ (ITEFI)

16:15 - 17:45

UD 2.6.4 Exercise class on performance of decoy-state QKD (streaming)

Marcos Curty Alonso

DOCTOR INGENIERO DE TELECOMUNICACIÓN
DOCTOR EN FÍSICA.
CATEDRÁTICO DE UNIVERSIDAD (AREA TEORIA DE LA SEÑAL Y COMUNICACIONES).
UNIVERSIDAD DE VIGO.

18:00 - 19:00

UD1. Tutoring

Vicente Martín Ayuso

Doctor en Ciencias Físicas.
Catedrático (Ciencias de la Computación).
Univ. Politécnica de Madrid /Center for Computational simulation.

28/11/2024

17:30 - 18:30

UD 3.3 Exercise class on security of QKD (streaming)

Guillermo Currás Lorenzo

Doctor
Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

02/12/2024

10:00 - 11:00

UD 4.2.1 Encoding in QKD protocols I (vídeo)

Verónica Fernández Mármol

Científica titular
ITEFI-CSIC

11:00 - 12:00

UD 4.2.1 Encoding in QKD protocols II (vídeo)

Verónica Fernández Mármol

Científica titular
ITEFI-CSIC

16:15 - 17:15

UD 4.1.3 Exercise class on experimental aspects of QKD I - Generation and detection (streaming)

Daniel Balado Souto

DOCTOR EN FÍSICA.
CONTRATADO MOMENTUM CSIC.
Instituto de Tecnologías Físicas y de la Información ¿Leonardo Torres Quevedo¿ (ITEFI)

04/12/2024

16:15 - 17:15

UD 4.2.3 Exercise class on experimental aspects of QKD II - Encoding (streaming)

Verónica Fernández Mármol

Científica titular
ITEFI-CSIC

09/12/2024

12:00 - 13:00

UD 4.3.1 Quantum channel: fiber, air and space (vídeo)

Verónica Fernández Mármol

Científica titular
ITEFI-CSIC

13:00 - 14:00

UD 4.3.2 Optical design of QKD protocols (vídeo)

Verónica Fernández Mármol

Científica titular
ITEFI-CSIC

15:45 - 16:45

UD2. Tutoring

Marcos Curty Alonso

DOCTOR INGENIERO DE TELECOMUNICACIÓN
DOCTOR EN FÍSICA.
CATEDRÁTICO DE UNIVERSIDAD (AREA TEORIA DE LA SEÑAL Y COMUNICACIONES).
UNIVERSIDAD DE VIGO.

10/12/2024

17:00 - 18:00

UD3. Tutoring

Guillermo Currás Lorenzo

Doctor
Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

16/12/2024

10:00 - 11:00

UD 4.4.1 Integrated photonics for QKD (vídeo)

Daniel Balado Souto

DOCTOR EN FÍSICA.
CONTRATADO MOMENTUM CSIC.
Instituto de Tecnologías Físicas y de la Información ¿Leonardo Torres Quevedo¿ (ITEFI)

11:00 - 12:00

UD 4.4.2 Experimental platforms (vídeo)

Verónica Fernández Mármol

Científica titular
ITEFI-CSIC

16:15 - 17:15

UD 4.3.3 Exercise class on experimental aspects of QKD III - Transmission and design (streaming)

Verónica Fernández Mármol

Científica titular
ITEFI-CSIC

18/12/2024

16:15 - 17:15

UD 4.4.3 Exercise class on experimental aspects of QKD IV - Transmission and design -

Integrated photonics (streaming)

Daniel Balado Souto

DOCTOR EN FÍSICA.
CONTRATADO MOMENTUM CSIC.
Instituto de Tecnologías Físicas y de la Información ¿Leonardo Torres Quevedo¿ (ITEFI)

07/01/2025

16:15 - 17:15

UD4. Tutoring

Daniel Balado Souto

DOCTOR EN FÍSICA.
CONTRATADO MOMENTUM CSIC.
Instituto de Tecnologías Físicas y de la Información ¿Leonardo Torres Quevedo¿ (ITEFI)

08/01/2025

10:00 - 12:30

UD 5.1 Quantum communication networks: QKD & QIN networks I (video)

Vicente Martín Ayuso

Doctor en Ciencias Físicas.
Catedrático (Ciencias de la Computación).
Univ. Politécnica de Madrid /Center for Computational simulation.

10/01/2025

10:00 - 12:00

UD 5.2 Quantum communication networks: QKD & QIN networks II (video)

Vicente Martín Ayuso

Doctor en Ciencias Físicas.
Catedrático (Ciencias de la Computación).
Univ. Politécnica de Madrid /Center for Computational simulation.

14/01/2025

10:00 - 11:30

UD 6.1 Quantum hacking (video)

Guillermo Currás Lorenzo

Doctor
Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

11:30 - 12:30

UD 6.2 QKD implementation security I (video)

Guillermo Currás Lorenzo

Doctor
Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

12:30 - 13:30

UD 6.3 QKD implementation security II (video)

Guillermo Currás Lorenzo

Doctor

Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

15/01/2025

14:00 - 15:30

UD 5.3 Exercise class on quantum communication networks (streaming)

Javier Faba García

Doctor en Física.
Profesor Ayudante Doctor.
Universidad Politécnica de Madrid / ETS de Ingenieros Informáticos / DATSI.

15:30 - 16:30

UD 5.3 Exercise class on quantum communication networks (streaming)

Vicente Martín Ayuso

Doctor en Ciencias Físicas.
Catedrático (Ciencias de la Computación).
Univ. Politécnica de Madrid /Center for Computational simulation.

20/01/2025

10:00 - 11:00

UD 7.1 Quantum cryptography beyond QKD I (video)

Guillermo Currás Lorenzo

Doctor
Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

11:00 - 12:00

UD 7.2 Quantum cryptography beyond QKD I (video)

Guillermo Currás Lorenzo

Doctor
Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

12:00 - 13:00

UD 8.1 Quantum repeaters (video)

Guillermo Currás Lorenzo

Doctor
Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

16:15 - 18:15

UD 6.4 Exercise class on performance of practical QKD implementations (streaming)

Guillermo Currás Lorenzo

Doctor
Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

28/01/2025

16:15 - 17:45

UD 8.2 Exercise class on the performance of quantum repeaters (streaming)

Guillermo Currás Lorenzo

Doctor
Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

29/01/2025

18:45 - 19:15

UD5. Tutoring

Javier Faba García

Doctor en Física.
Profesor Ayudante Doctor.
Universidad Politécnica de Madrid / ETS de Ingenieros Informáticos / DATSI.

19:15 - 19:45

UD5. Tutoring

Vicente Martín Ayuso

Doctor en Ciencias Físicas.
Catedrático (Ciencias de la Computación).
Univ. Politécnica de Madrid /Center for Computational simulation.

30/01/2025

16:15 - 17:15

UD2. Tutoring

Marcos Curty Alonso

DOCTOR INGENIERO DE TELECOMUNICACIÓN

DOCTOR EN FÍSICA.
CATEDRÁTICO DE UNIVERSIDAD (AREA TEORIA DE LA SEÑAL Y COMUNICACIONES).
UNIVERSIDAD DE VIGO.

31/01/2025

15:00 - 16:00

UD6. Tutoring

Guillermo Currás Lorenzo

Doctor
Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

05/02/2025

14:00 - 15:30

UD4. Tutoring

Verónica Fernández Mármol

Científica titular
ITEFI-CSIC

15:30 - 16:30

UD7/UD8 Tutoring

Guillermo Currás Lorenzo

Doctor
Investigador Postdoctoral
Vigo Quantum Communication Center, Universidad de Vigo

BIBLIOGRAFÍA Y ENLACES RELACIONADOS

Bibliografía

V. Scarani et al, Rev. Mod. Phys. 81, 1301 (2009).

H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photonics 8, 595 (2014).

F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. 92, 025002 (2020).

M. Razavi, An Introduction to Quantum Communication Networks, IOP Concise Physics (2018).

M. Tomamichel, Quantum Information Processing with Finite Resources, Springer (2016).