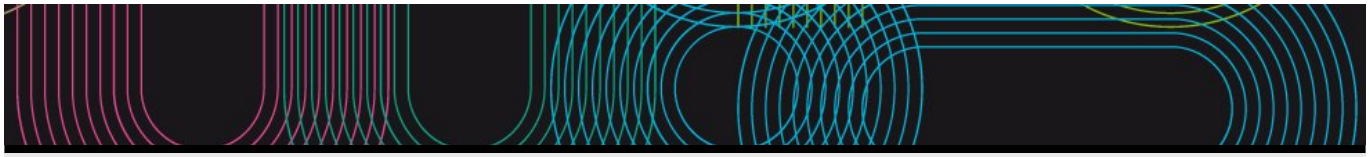

DATOS IDENTIFICATIVOS				
Fundamentos de comunicaciones cuánticas				
Asignatura	Fundamentos de comunicaciones cuánticas			
Código	V05M198V01105			
Titulacion	Máster Universitario en Ciencia e tecnoloxías de información cuántica			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	3	OB	1	1c
Lengua Impartición	Castellano Gallego			
Departamento				
Coordinador/a	Curty Alonso, Marcos			
Profesorado	Curty Alonso, Marcos			
Correo-e	mcurty@com.uvigo.es			
Web	http://moovi.uvigo.gal			
Descripción general	Esta asignatura proporciona al alumno los conceptos y técnicas básicas de operación de los sistemas de comunicaciones cuánticos, con especial énfasis en la construcción de canales de comunicaciones seguras y en el análisis de los protocolos en que se fundamentan. Se tratarán la distribución cuántica de claves, las diferentes posibilidades de implementación tecnológica y las técnicas de análisis de la seguridad de estos esquemas.			

Resultados de Formación y Aprendizaje	
Código	
A3	Comprensión y conocimiento de los fundamentos de la Teoría Cuántica de la Información, así como los aspectos básicos de los cuatro tipos de tecnologías cuánticas: computación, comunicaciones, metrología, simulación.
A6	Conocer y comprender la naturaleza de las plataformas físicas para el procesado de la información cuántica en sistemas fotónicos: óptica cuántica, sistemas ópticos integrados, sistemas opto-atómicos, sistemas de detección y medida, fotónica de semiconductores.
A11	Adquirir una base sólida sobre la teoría cuántica de la información en su aplicación a las comunicaciones cuánticas, asi como sobre la tecnología de dispositivos fotónicos empleados en comunicaciones cuánticas, tanto terrestres como aéreas y vía satélite.
A12	Adquirir destrezas para el diseño y la estimación de recursos que permitan el desarrollo de canales y redes de comunicación cuánticas y de computación distribuida. Conocer el estado de desarrollo y de implementación actual de redes cuánticas, y los planes para su expansión.
B11	Conocimientos sobre comunicaciones cuánticas, los principios teóricos, y las implementaciones experimentales, tanto terrestres como aéreas y vía satélite.
B12	Tener conocimientos sobre criptografía cuántica, sus bases teóricas, las implementaciones existentes y los retos y desafíos que afrontan.
C1	Analizar y descomponer un concepto complejo, examinar cada parte y observar cómo encajan entre sí
C2	Clasificar e identificar tipos o grupos, mostrando cómo cada categoría es distinta de las demás
C3	Comparar y contrastar y señalar las similitudes y diferencias entre dos o más temas o conceptos

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Conocimiento de los principales tipos de protocolos de distribución cuántica de clave, así como de los fundamentos teóricos sobre su seguridad.	A3 A6 A11 A12 B11 B12 C1 C2 C3
Conocimiento de las tecnologías fotónicas empleadas en estos sistemas, así como de las principales plataformas experimentales, y capacidad para comprender y evaluar sus prestaciones.	A3 A6 A11 A12 B11 B12 C1 C2 C3
Conocimiento y capacidad para aplicar y deducir resultados de protocolos de comunicaciones cuánticas.	A3 A6 A11 A12 B11 B12 C1 C2 C3

Contenidos

Tema	
1. Introducción a la criptografía	1.1. Cifrado y autenticación de información. 1.2. Criptografía clásica de clave simétrica. Libreta de un solo uso. 1.3. Criptografía clásica de clave pública y post-cuántica.
2. Criptografía cuántica	2.1. Distribución cuántica de clave. 2.2. Fundamentos sobre seguridad.
3. Protocolos de distribución cuántica de clave	3.1. Protocolos de preparación y medida. 3.2. Protocolos basados en entrelazamiento y en interferencia fotónica. 3.3. Protocolos basados en variable continua. 3.4. Esquemas de post-procesado de datos.
4. Seguridad de los protocolos de distribución cuántica de clave	4.1. Ataques individuales, colectivos y coherentes. 4.2. Régimen asimptótico y régimen finito. 4.3. Definición de seguridad. Componibilidad.
5. Implementaciones tecnológicas	5.1. Principales plataformas experimentales. 5.2. Limitaciones en la tasa de generación de clave secreta. Ataque basado en la división del número de fotones. 5.3. Estados señuelo.
6. Otros protocolos de comunicaciones cuánticas	6.1. Teleportación. 6.2. Codificación densa. 6.3. Bit commitment. 6.4. Quantum radar.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	18	25	43
Resolución de problemas	4	0	4
Resolución de problemas y/o ejercicios	0	7	7
Trabajo	1	10	11
Examen de preguntas de desarrollo	2	8	10

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías

	Descripción
Lección magistral	Exposición por parte del profesor de los contenidos de la materia objeto de estudio.
Resolución de problemas	Resolución de problemas en clase magistral. Resolución de problemas de forma autónoma por parte de los estudiantes.

Atención personalizada

Metodologías	Descripción
Lección magistral	Los estudiantes podrán acudir a tutorías personalizadas en el despacho del profesor o a través de medios telemáticos. Se puede consultar el horario y/o solicitar tutorías en: https://www.uvigo.gal/es/universidad/administracion-personal/pdi/marcos-curty-alonso
Resolución de problemas	Los estudiantes podrán acudir a tutorías personalizadas en el despacho del profesor o a través de medios telemáticos. Se puede consultar el horario y/o solicitar tutorías en: https://www.uvigo.gal/es/universidad/administracion-personal/pdi/marcos-curty-alonso
Pruebas	**Descripción**
Trabajo	Los estudiantes podrán acudir a tutorías personalizadas en el despacho del profesor o a través de medios telemáticos. Se puede consultar el horario y/o solicitar tutorías en: https://www.uvigo.gal/es/universidad/administracion-personal/pdi/marcos-curty-alonso

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje		
Resolución de problemas y/o ejercicios	Resolución de problemas y/o ejercicios.	30	A3 A6 A11 A12	B11 B12	C1 C2 C3
Trabajo	Realización de un trabajo en grupo guiado por el profesor.	30	A3 A6 A11 A12	B11 B12	C1 C2 C3
Examen de preguntas de desarrollo	Examen final en el que se evalúan todos los contenidos de la materia.	40	A3 A6 A11 A12	B11 B12	C1 C2 C3

Otros comentarios sobre la Evaluación

Habrá dos modalidades de evaluación en la convocatoria ordinaria: evaluación continua y evaluación global. La evaluación continua consiste en la entrega de un boletín de ejercicios resueltos individualmente por cada estudiante (30%), de un trabajo realizado en grupo y guiado por el profesor (30%), y un examen escrito al término del curso (40%). La evaluación global consistirá en un único examen escrito al final del curso. Se considerará que un estudiante opta por la evaluación global si no entrega el boletín de ejercicios. La evaluación continua impide una calificación final de no presentado.

Fuentes de información

Bibliografía Básica

Bibliografía Complementaria

Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, Hugo Zbinden, **Quantum Cryptography**, https://doi.org/10.1103/RevModPhys.74.145, Rev. Mod. Phys. 74, 145, American Physical Society, 2002

Dagmar Bruss, Norbert Lutkenhaus, **Quantum Key Distribution: from Principles to Practicalities**, https://doi.org/10.1007/s002000050137, AAECC Vol 10, 383-399, Springer, 2000

Hoi-Kwong Lo, Yi Zhao, **Quantum Cryptography**, https://doi.org/10.1007/978-0-387-30440-3_432, Encyclopedia of Complexity and Systems Science 8, 7265-7289, Springer, 2009

Recomendaciones

Asignaturas que continúan el temario

Comunicaciones cuánticas avanzadas/V05M198V01111
Comunicaciones cuánticas vía satélite/V05M198V01216
Laboratorio de comunicaciones cuánticas/V05M198V01213
Redes de comunicaciones cuánticas/V05M198V01204