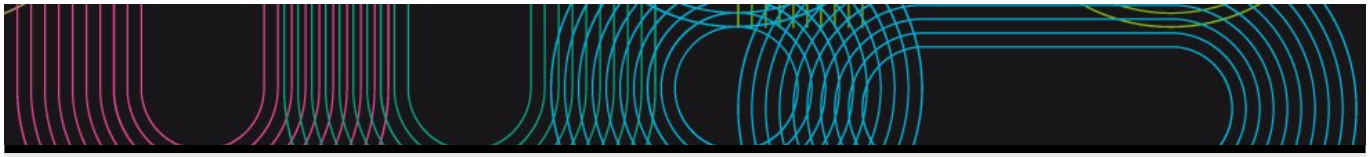

DATOS IDENTIFICATIVOS				
Fundamentos de comunicacións cuánticas				
Materia	Fundamentos de comunicacións cuánticas			
Código	V05M198V01105			
Titulación	Máster Universitario en Ciencia e Tecnoloxías de Información Cuántica			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	3	OB	1	1c
Lingua de impartición	Castelán Galego Inglés			
Departamento	Dpto. Externo Teoría do sinal e comunicacións			
Coordinador/a	Curty Alonso, Marcos			
Profesorado	Curty Alonso, Marcos Zapatero Castrillo, Víctor			
Correo-e	mcurty@com.uvigo.es			
Web	http://moovi.uvigo.gal			
Descrición xeral	Esta materia proporciona ao alumno os conceptos e técnicas básicas de funcionamento dos sistemas de comunicación cuántica, facendo especial fincapé na construción de canles de comunicación seguras e na análise dos protocolos nos que se basean. Debaterase a distribución cuántica de claves, as diferentes posibilidades de implantación tecnolóxica e as técnicas de análise de seguridade destes esquemas.			

Resultados de Formación e Aprendizaxe	
Código	
A3	Comprensión e coñecemento dos fundamentos da Teoría da Información Cuántica, así como dos aspectos básicos dos catro tipos de tecnoloxías cuánticas: informática, comunicacións, metroloxía, simulación.
A6	Coñecer e comprender a natureza das plataformas físicas para o procesamento da información cuántica en sistemas fotónicos: óptica cuántica, sistemas ópticos integrados, sistemas optoatómicos, sistemas de detección e medida, fotónica de semicondutores.
A11	Adquirir unha base sólida sobre a teoría cuántica da información na súa aplicación ás comunicacións cuánticas, así como sobre a tecnoloxía dos dispositivos fotónicos empregados nas comunicacións cuánticas, tanto terrestres como aéreas e vía satélite.
A12	Adquirir habilidades para o deseño e estimación de recursos que permitan o desenvolvemento de canles e redes de comunicación cuántica e de computación distribuída. Coñecer o estado de desenvolvemento e implantación actual das redes cuánticas, e os plans para a súa expansión.
B11	Coñecemento das comunicacións cuánticas, principios teóricos e implementacións experimentais, tanto terrestres como aéreas e vía satélite.
B12	Ter coñecementos sobre a criptografía cuántica, as súas bases teóricas, as implementacións existentes e os retos aos que se enfrontan.
C1	Analizar e desglosar un concepto complexo, examinar cada parte e observar como encaixan
C2	Clasificar e identificar tipos ou grupos, mostrando como cada categoría é diferente das demais
C3	Comparar e contrastar e sinalar semellanzas e diferenzas entre dous ou máis temas ou conceptos

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Coñecemento dos principais tipos de protocolos de distribución de claves cuánticas, así como os fundamentos teóricos da súa seguridade.	A3 A6 A11 A12 B11 B12 C1 C2 C3
Coñecemento das tecnoloxías fotónicas empregadas nestes sistemas, así como das principais plataformas experimentais, e capacidade para comprender e avaliar o seu rendemento.	A3 A6 A11 A12 B11 B12 C1 C2 C3
Coñecemento e capacidade para aplicar e derivar resultados de protocolos de comunicación cuántica.	A3 A6 A11 A12 B11 B12 C1 C2 C3

Contidos	
Tema	
1. Introdución á criptografía	1.1. Cifrado e autenticación da información. 1.2. Criptografía clásica de clave simétrica. Caderno dun só uso. 1.3. Criptografía clásica de clave pública e poscuántica.
2. Criptografía cuántica	2.1. Distribución cuántica de clave. 2.2. Fundamentos de seguridade.
3. Protocolos de distribución cuántica de clave	3.1. Protocolos de preparación e medición. 3.2. Protocolos baseados en entrelazamento e interferencia fotónica. 3.3. Protocolos baseados en variable continua. 3.4. Esquemas de posprocesamento de datos.
4. Seguridade dos protocolos de distribución cuántica de clave	4.1. Ataques individuais, colectivos e coherentes. 4.2. Réxime asintótico e réxime finito. 4.3. Definición de seguridade. Composibilidade.
5. Implementacións tecnolóxicas	5.1. Principais plataformas experimentais. 5.2. Limitacións na taxa de xeración de claves secretas. Ataque baseado na división do número de fotóns. 5.3. Estados de señuelo.
6. Outros protocolos de comunicación cuántica	6.1. Teletransportación. 6.2. Codificación densa. 6.3. Bit commitment. 6.4. Radar cuántico.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	18	25	43
Resolución de problemas	4	0	4
Resolución de problemas e/ou exercicios	0	7	7
Traballo	1	10	11
Exame de preguntas de desenvolvemento	2	8	10

*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

Metodoloxía docente	
	Descrición
Lección maxistral	Exposición por parte do profesor dos contidos da materia obxecto de estudo.
Resolución de problemas	Resolución de problemas na clase maxistral. Resolución de problemas de forma autónoma por parte do alumnado.

Atención personalizada

Metodoloxías	Descrición
Lección maxistral	O alumnado poderá asistir a titorías personalizadas no despacho do profesorado ou a través de medios telemáticos.. Pódese consultar o horario e/ou solicitar as titorías en: https://www.uvigo.gal/es/universidad/administracion-personal/pdi/marcos-curty-alonso
Resolución de problemas	O alumnado poderá asistir a titorías personalizadas no despacho do profesorado ou a través de medios telemáticos.. Pódese consultar o horario e/ou solicitar as titorías en: https://www.uvigo.gal/es/universidad/administracion-personal/pdi/marcos-curty-alonso
Probas	**Descrición**
Traballo	O alumnado poderá asistir a titorías personalizadas no despacho do profesorado ou a través de medios telemáticos.. Pódese consultar o horario e/ou solicitar as titorías en: https://www.uvigo.gal/es/universidad/administracion-personal/pdi/marcos-curty-alonso

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe		
Resolución de problemas e/ou exercicios	Resolución de problemas e/ou exercicios.	30	A3 A6 A11 A12	B11 B12	C1 C2 C3
Traballo	Realización de traballos en grupo guiados polo profesor.	30	A3 A6 A11 A12	B11 B12	C1 C2 C3
Exame de preguntas de desenvolvemento	Exame final no que se avalían todos os contidos da materia.	40	A3 A6 A11 A12	B11 B12	C1 C2 C3

Outros comentarios sobre a Avaliación

Haberá dúas modalidades de avaliación na convocatoria ordinaria: avaliación continua e avaliación global. A avaliación continua consiste na entrega dun boletín de exercicios resoltos individualmente por cada alumno (30%), dun traballo realizado en grupo e guiado polo profesor (30%), e un exame escrito ao final do curso (40%). A avaliación global consistirá nun único exame escrito ao final do curso. Considerarase que un alumno optou á avaliación global se non presenta o boletín de exercicios. A avaliación continua impide unha cualificación final de non presentado.

Bibliografía. Fontes de información

Bibliografía Básica

Bibliografía Complementaria

Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, Hugo Zbinden, **Quantum Cryptography**, Rev. Mod. Phys. 74, 145, American Physical Society, 2002

Dagmar Bruss, Norbert Lutkenhaus, **Quantum Key Distribution: from Principles to Practicalities**, AAECC Vol 10, 383-399, Springer, 2000

Hoi-Kwong Lo, Yi Zhao, **Quantum Cryptography**, Encyclopedia of Complexity and Systems Science 8, 7265-7289, Springer, 2009

Recomendacións

Materias que continúan o temario

Comunicacións cuánticas avanzadas/V05M198V01111
Comunicacións cuánticas vía satélite/V05M198V01216
Laboratorio de comunicacións cuánticas/V05M198V01213
Redes de comunicacións cuánticas/V05M198V01204