



DATOS IDENTIFICATIVOS

Comunicacións cuánticas avanzadas

Materia	Comunicacións cuánticas avanzadas			
Código	V05M198V01111			
Titulación	Máster Universitario en Ciencia e tecnoloxías de información cuántica			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	3	OP	1	1c
Lingua de impartición	Castelán Galego			
Departamento				
Coordinador/a	Curty Alonso, Marcos			
Profesorado				
Correo-e				
Web	http://moovi.uvigo.gal			
Descrición xeral	Este curso describe e analiza a seguridade das canles de comunicación cuánticas e presenta técnicas para determinar a taxa de xeración de claves secretas nun sistema cuántico de distribución de claves.			

Resultados de Formación e Aprendizaxe

Código				
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
Capacidade para demostrar a seguridade dos sistemas cuánticos de distribución de claves e calcular a súa taxa de xeración de claves secretas.	A11 A12 B11 B12 C1 C2 C3

Coñecementos xerais de hackeo cuántico, e sobre a seguridade práctica dos sistemas experimentais.	A11 A12 B11 B12 C1 C2 C3
Coñecemento das redes de distribución cuántica de claves e capacidade para comprender e avaliar o seu rendemento.	A11 A12 B11 B12 C1 C2 C3
Coñecemento de dispositivos cuánticos para xerar números aleatorios e capacidade para comprender e avaliar o seu rendemento.	A11 A12 B11 B12 C1 C2 C3

Contidos

Tema	
1. Seguridade da distribución cuántica de clave.	1.1. Escalamiento da taxa clave. 1.2. Proba de seguridade baseada na entropía. 1.3. Outras probas de seguridade: Shor-Preskill e baseadas na complementariedade.
2. Hackeo cuántico.	2.1. Ataques pasivos e ataques activos. 2.2. Hackear os transmisores. Ataques usando cabalos de Troia. 2.3. Hackear os receptores. Ataques a detectores. 2.4. Seguridade das implementacións experimentais.
3. Distribución cuántica de clave independente dos dispositivos.	3.1. Principio de funcionamento. Desigualdades de Bell. 3.2. Seguridade e beneficios. 3.3. Plataformas experimentais.
4. Redes de distribución cuántica de clave.	4.1. Arquitecturas de rede. Redes baseadas en nodos fiables e redes vía satélite. 4.2. Compatibilidade con redes de comunicación óptica. 4.3. Normalización e certificación.
5. Xeradores cuánticos de números aleatorios.	5.1. Principio de funcionamento. 5.2. Estimación da entropía cuántica. 5.3. Plataformas experimentais e comerciais.

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.
Resolución de problemas	O alumnado poderá asistir a titorías personalizadas no despacho do profesorado ou a través de medios telemáticos.

Probas	Descrición
Traballo	O alumnado poderá asistir a titorías personalizadas no despacho do profesorado ou a través de medios telemáticos.

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

V. Scarani et al, **The security of practical quantum key distribution**, <https://doi.org/10.1103/RevModPhys.81.1301>, Rev. Mod. Phys. 81, 1301, American Physical Society, 2009

H.-K. Lo, M. Curty, and K. Tamaki, **Secure quantum key distribution**, <https://doi.org/10.1038/nphoton.2014.149>, Nat. Photonics 8, 595, Springer Nature, 2014

F. Xu, X. Ma, Q. Zhang, H.-K. Lo, J.-W. Pan, **Secure quantum key distribution with realistic devices**, <https://doi.org/10.1103/RevModPhys.92.025002>, Rev. Mod. Phys. 92, 025002, American Physical Society, 2020

M. Razavi, **An Introduction to Quantum Communication Networks**, 978-1-6817-4653-1, IOP Concise Physics, 2018

M. Tomamichel, **Quantum Information Processing with Finite Resources**, 978-3-319-21890-8, Springer, 2016

Recomendacións

Materias que se recomenda ter cursado previamente

Fundamentos de comunicacións cuánticas/V05M198V01105