IDENTIFYING DATA

Fundamentals of quantum communications

Subject	Fundamentals of quantum communications			
Code	V05M198V01105			
Study programme	(*)Máster Universitario en Ciencia e tecnoloxías de información cuántica			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Mandatory	1st	1st
Teaching language	Spanish Galician			
Department				
Coordinator	Curty Alonso, Marcos			
Lecturers	Curty Alonso, Marcos			
E-mail	mcurty@com.uvigo.es			
Web	http://moovi.uvigo.gal			
General description	This subject provides the student with the basic concepts and techniques of operation of quantum communication systems, with special emphasis on the construction of secure communication channels and the analysis of the protocols on which they are based. This includes quantum key distribution and the different technological implementations, as well as its security analysis.			

Training and Learning Results

Code	
A3	Understanding and knowledge of the fundamentals of Quantum Information Theory, as well as two basic aspects of two four types of quantum technologies: computing, communications, metrology, simulation.
A6	Know and understand the nature of the physical platforms for the processing of quantum information in photonic systems: quantum optics, integrated optical systems, opto-atomic systems, detection and measurement systems, semiconductor photonics.
A11	Acquiring a solid foundation on quantum theory gives information on its application in quantum communications, as well as on the technology of two photonic devices used in quantum communications, both terrestrial and aerial and via satellite.
A12	Acquire skills for the design and estimation of resources that allow the development of quantum communication channels and networks and distributed computing. Know the state of development and current implementation of quantum networks, and the plans for their expansion.
B11	Knowledge of quantum communications, theoretical principles and experimental implementations, both terrestrial and aerial and via satellite.
B12	To have knowledge about quantum cryptography, its theoretical bases, existing implementations and the challenges they face.
C1	To analyze and break down a complex concept, examine each part and see how they fit together
C2	To classify and identify types or groups, showing how each category is different from the others
C3	To compare and contrast and point out similarities and differences between two or more topics or concepts

Expected results from this subject

Expected results from this subject	Training and Learning Results

Knowledge of the main types of quantum key distribution protocols, as well as the theoretical foundations of their security.	A3 A6 A11 A12 B11 B12 C1 C2 C3
Knowledge of the photonic technologies used in these systems, as well as the main experimental platforms, and the ability to understand and evaluate their performance.	A3 A6 A11 A12 B11 B12 C1 C2 C3
Knowledge and ability to apply and derive results from quantum communication protocols.	A3 A6 A11 A12 B11 B12 C1 C2 C3

Contents

Topic	
1. Introduction to cryptography	1.1. Encryption and authentication of information. 1.2. Classic symmetric key cryptography. One-time-pad scheme. 1.3. Classic public-key and post-quantum cryptography.
2. Quantum cryptography	2.1. Quantum key distribution. 2.2. Security fundamentals.
3. Quantum key distribution protocols	3.1. Prepare-and-measure protocols. 3.2. Protocols based on entanglement and photonic interference. 3.3. Protocols based on continuous variables. 3.4. Data post-processing schemes.
4. Security of quantum key distribution protocols	4.1. Individual, collective and coherent attacks. 4.2. Asymptotic regime and finite regime. 4.3. Security definition. Composability.
5. Technological implementations	5.1. Main experimental platforms. 5.2. Limitations on the secret key generation rate. Photon-number-splitting attack. 5.3. Decoy states.
6. Other quantum communication protocols	6.1. Teleportation. 6.2. Dense coding. 6.3. Bit commitment. 6.4. Quantum radar.

Planning

	Class hours	Hours outside the classroom	Total hours
Lecturing	18	25	43
Problem solving	4	0	4
Problem and/or exercise solving	0	7	7
Essay	1	10	11
Essay questions exam	2	8	10

*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.

Methodologies

	Description
Lecturing	Presentation by the professor of the contents of the subject under study.
Problem solving	Solving problems in the class. Solving problems autonomously by students.

Personalized assistance

Methodologies	Description
Lecturing	Students will be able to attend personalized tutoring sessions in the professors office or through telematic means. You can check the schedule and/or request tutoring sessions at: https://www.uvigo.gal/es/universidad/administracion-personal/pdi/marcos-curty-alonso
Problem solving	Students will be able to attend personalized tutoring sessions in the professors office or through telematic means. You can check the schedule and/or request tutoring sessions at: https://www.uvigo.gal/es/universidad/administracion-personal/pdi/marcos-curty-alonso
Tests	**Description**
Essay	Students will be able to attend personalized tutoring sessions in the professors office or through telematic means. You can check the schedule and/or request tutoring sessions at: https://www.uvigo.gal/es/universidad/administracion-personal/pdi/marcos-curty-alonso

Assessment

	Description	Qualification	Training and Learning Results		
Problem and/or exercise solving	Resolution of problems and/or exercises.	30	A3 A6 A11 A12	B11 B12	C1 C2 C3
Essay	Realization of a project in groups of students guided by the professor.	30	A3 A6 A11 A12	B11 B12	C1 C2 C3
Essay questions exam	Final exam in which all the contents of the subject are evaluated.	40	A3 A6 A11 A12	B11 B12	C1 C2 C3

Other comments on the Evaluation

There will be two evaluation modalities in the ordinary call: continuous evaluation and global evaluation. The continuous evaluation consists of the delivery of exercises solved individually by each student (30%), of a project performed in group and guided by the professor (30%), and a written exam at the end of the course (40%). The overall evaluation will consist of a single written exam at the end of the course. A student will be considered as opting for the overall assessment if they do not submit the set of exercises. The continuous evaluation prevents a final qualification of not presented.

Sources of information

Basic Bibliography

Complementary Bibliography

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

Recommendations

Subjects that continue the syllabus

Advanced quantum communications/V05M198V01111
Quantum communications via satellite/V05M198V01216
Quantum Communications Laboratory/V05M198V01213
Quantum Communications Networks/V05M198V01204