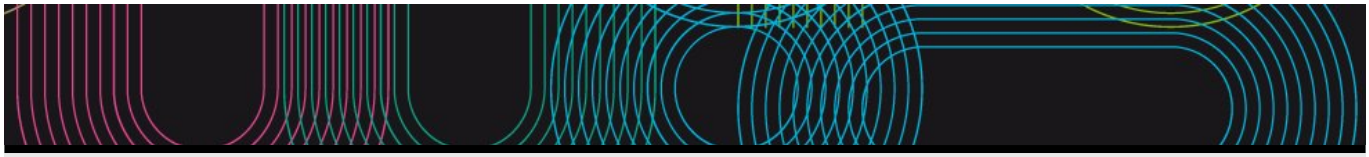
Universidade Vigo

Subject Guide 2023 / 2024



IDENTIFYING DATA				
Advanced quantum communications				
Subject	Advanced quantum communications			
Code	V05M198V01111			
Study programme	(*)Máster Universitario en Ciencia e tecnoloxías de información cuántica			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	1st
Teaching language	Spanish Galician			
Department				
Coordinator	Curty Alonso, Marcos			
Lecturers				
E-mail				
Web	http://moovi.uvigo.gal			
General description	This course describes and analyzes the security of quantum communication channels, and presents techniques for determining the secret key generation rate in a quantum key distribution system.			

Training and Learning Results	
Code	
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
Ability to demonstrate the security of quantum key distribution systems, and to calculate their secret key generation rate.	A11 A12 B11 B12 C1 C2 C3
General knowledge of quantum hacking, and about the practical security of experimental systems.	A11 A12 B11 B12 C1 C2 C3

Knowledge of quantum key distribution networks and the ability to understand and evaluate their performance.	A11 A12 B11 B12 C1 C2 C3
Knowledge of quantum random number generators and the ability to understand and evaluate their performance.	A11 A12 B11 B12 C1 C2 C3

Contents

Topic	
1. Security of the quantum key distribution.	1.1. Key rate scaling. 1.2. Proof of security based on entropy. 1.3. Other security proofs: Shor-Preskill and that based on complementarity.
2. Quantum hacking.	2.1. Passive attacks and active attacks. 2.2. Hacking the transmitters. Attacks using Trojan Horses. 23. Hacking the receivers. Attacks on detectors. 2.4. Security of experimental implementations.
3. Device-independent quantum key distribution.	3.1. Operating principle. Bell's inequalities. 3.2. Security and benefits. 3.3. Experimental platforms.
4. Quantum key distribution networks.	4.1. Network architectures. Networks based on trusted nodes and satellite networks. 4.2. Compatibility with optical communication networks. 4.3. Standardization and certification.
5. Quantum random number generators.	5.1. Operating principle. 5.2. Estimation of the quantum entropy. 5.3. Experimental and commercial platforms.

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 professor□s office or through telematic means.
Problem solving	Students will be able to attend personalized tutoring sessions in the professor□s office or through telematic means.
Tests	**Description**
Essay	Students will be able to attend personalized tutoring sessions in the professor□s office or through telematic means.

Assessment

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

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

Recommendations

Subjects that it is recommended to have taken before

Fundamentals of quantum communications/V05M198V01105