Course guide
230988 - QCRYP - Quantum Cryptography

Last modified: 08/06/2023

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 739 - TSC - Department of Signal Theory and Communications.

Degree: MASTER'S DEGREE IN TELECOMMUNICATIONS ENGINEERING (Syllabus 2013). (Optional subject).
MASTER'S DEGREE IN ADVANCED TELECOMMUNICATION TECHNOLOGIES (Syllabus 2019). (Optional subject).
MASTER'S DEGREE IN CYBERSECURITY (Syllabus 2020). (Optional subject).

Academic year: 2023 **ECTS Credits:** 5.0 **Languages:** English

LECTURER

Coordinating lecturer: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/responsables-assignatura

Others: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/professorat-assignat-idioma

PRIOR SKILLS

Solid knowledge of linear algebra and probability theory.

TEACHING METHODOLOGY

- Lectures.
- Problems solved individually or in groups by the student.
- Laboratory exercises.

LEARNING OBJECTIVES OF THE SUBJECT

This subject combines two of the most important branches of science of the 20th century, the quantum theory developed in the 1920s and 1930s by scientists such as Planck, Einstein, Bohr, Heisenberg, Schrödinger, Pauli, Dirac and von Neumann, and the information theory, born after the work of Shannon in 1948. The basic postulates of quantum systems as well as their mathematical model will be presented. We then cover Quantum Key Distribution protocols, which can be used to implement a classical private key cryptosystem with guaranteed security. This requires introducing Quantum error correction and Physical-Layer Security concepts. The last part of the course introduces the area of quantum computing as the algorithmic framework governed by the quantum mechanical laws which promises, among other remarkable achievements, to break the RSA public-key cryptosystem.

STUDY LOAD

Type	Hours	Percentage
Hours small group	13,0	10.40
Self study	86,0	68.80
Hours large group	26,0	20.80

Total learning time: 125 h

CONTENTS

Introduction to Quantum Information Theory.

Description:
a) Introduction to Quantum Mechanics: The EPR paper, the Big Bell Test and course outline.
b) Quantum states: the Bloch sphere, spectral decomposition, reversible evolution, measurement and the Born rule, the Stern-Gerlach experiment and measurement based on POVM.
c) Composite quantum systems: Kronecker product description, the no-cloning theorem, separable and entangled states, the Schmidt decomposition, partial trace, purification, entanglement as a resource and the violation of the CHSH inequality.
d) Quantum protocols: Entanglement distribution, super-dense coding and quantum teleportation.

Related activities:
Laboratory exercises on quantum protocols.

Full-or-part-time: 12h
Theory classes: 8h
Practical classes: 4h

Quantum cryptography.

Description:
a) Quantum error correction: Repetition codes and the Shor code, review of classical linear codes and CSS codes.
b) Physical-Layer Security: The wiretap channel, secret key communication, secret key agreement by the source model, sequential key distillation and the channel model.
c) Quantum Key distribution: The BB84, B92 and EPR protocols and secure CSS and BB84 protocols.

Related activities:
Laboratory exercises of error correcting codes and QKD.

Full-or-part-time: 15h
Theory classes: 10h
Practical classes: 5h

Quantum computing

Description:
a) Quantum Fourier Transform.
b) Phase estimation, order finding and Shor’s Algorithm for integer factorization.

Related activities:
Laboratory exercises of phase estimation and Shor algorithm.

Full-or-part-time: 12h
Theory classes: 8h
Practical classes: 4h

GRADING SYSTEM

- Attendance is mandatory.
- Participation in class (10%).
- Problems, lab exercises and/or group or individual presentation (90%).

EXAMINATION RULES.

There is no final exam.

BIBLIOGRAPHY

Basic:
- Wilde, Mark. Quantum information theory. Second edition. 2017. ISBN 9781107176164.
- Bloch, Matthieu; Barros, João. Physical-layer security : from information theory to security engineering. Cambridge: Cambridge University Press, cop. 2011. ISBN 9780521516501.
- Nielsen, Michael A; Chuang, Isaac L. Quantum computation and quantum information. 10th anniversary ed. Cambridge, UK: Cambridge University Press, cop. 2010. ISBN 9781107002173.