UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Course guide
230998 - QCRIP - Quantum Computing and Cryptography

Last modified: 10/11/2022

Unit in charge:	Barcelona School of Telecommunications Engineering
Teaching unit:	739 - TSC - Department of Signal Theory and Communications.
Degree:	MASTER'S DEGREE IN CYBERSECURITY (Syllabus 2020). (Optional subject).

Academic year: 2022 **ECTS Credits:** 3.0 **Languages:** English

LECTURER

Coordinating lecturer: JAVIER RODRIGUEZ FONOLLOSA

Others: Segon quadrimestre:
JAVIER RODRIGUEZ FONOLLOSA - 30

PRIOR SKILLS

Solid knowledge of linear algebra and probability theory.

TEACHING METHODOLOGY

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

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. Quantum error correction are introduced first which are described both from a theoretical and a practical implementation perspective. The last part of the course introduces the concept of quantum computing as the algorithmic framework governed by the quantum mechanical laws which promises to break break the RSA public-key cryptosystem.

STUDY LOAD

Type	Hours	Percentage
Hours large group	24,0	32.00
Self study	51,0	68.00

Total learning time: 75 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.

Full-or-part-time: 24h
Theory classes: 8h
Self study : 16h

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.

Full-or-part-time: 30h
Theory classes: 10h
Self study : 20h

Quantum Computing

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

Full-or-part-time: 18h
Theory classes: 6h
Self study : 12h

GRADING SYSTEM

- Attendance is mandatory.
- Participation in class (20%).
- Problems and/or group or individual presentation (80%).

EXAMINATION RULES.

There is no final exam.

BIBLIOGRAPHY

Basic:
- Nielsen, Michael A; Chuang, Isaac L. Quantum computation and quantum information. 10th anniversary ed. Cambridge, UK: Cambridge University Press, cop. 2010. ISBN 9781107002173.
- Wilde, Mark. Quantum information theory. Second edition. Cambridge, UK ; New York: Cambridge University Press, 2017. ISBN 9781107176164.
- Bloch, Matthieu; Barros, João. Physical-layer security : from information theory to security engineering. Cambridge: Cambridge University Press, cop. 2011. ISBN 9780521516501.
- El-Gamal, Abbas; Kim, Young-Han. Network information theory. Cambridge: Cambridge University Press, 2011. ISBN 9781107008731.