**Course guide**  
**230336 - QTC - Quantum Technologies for Cybersecurity: Networks and Systems**

**Unit in charge:** Barcelona School of Telecommunications Engineering  
**Teaching unit:** 230 - ETSETB - Barcelona School of Telecommunications Engineering.  
**Degree:**  
- BACHELOR’S DEGREE IN ENGINEERING PHYSICS (Syllabus 2011). (Optional subject).  
- BACHELOR’S DEGREE IN TELECOMMUNICATIONS TECHNOLOGIES AND SERVICES ENGINEERING (Syllabus 2015). (Optional subject).  
- BACHELOR’S DEGREE IN ELECTRONIC ENGINEERING AND TELECOMMUNICATION (Syllabus 2018). (Optional subject).  

**Academic year:** 2022  
**ECTS Credits:** 2.0  
**Languages:** English

---

**LECTURER**

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

**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, information & probability theory, telecommunication systems.

---

**TEACHING METHODOLOGY**

- Expositive and participative lectures together with example exercises solved in-class.  
- Learning based on problems and projects solved individually or in groups by the student.

---

**LEARNING OBJECTIVES OF THE SUBJECT**

This seminar combines the theoretical principles of quantum information and technologies applied to quantum cybersecurity.

Objectives:  
1. Understand the basic implementation principles of quantum information and technologies, applied to quantum cybersecurity and secure systems.  
2. Ability to critically analyze the strengths and weaknesses of various quantum cybersecurity solutions.  
3. Familiarization with the current hardware and infrastructures for real-world quantum systems, in terms of security, efficiency, and scalability.  
4. Awareness of the potential applications of cybersecurity quantum technologies in various fields, such as cryptography, networking and communication systems.
## STUDY LOAD

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self study</td>
<td>30,0</td>
<td>60.00</td>
</tr>
<tr>
<td>Hours large group</td>
<td>20,0</td>
<td>40.00</td>
</tr>
</tbody>
</table>

**Total learning time:** 50 h
CONTENTS

Quantum Technologies for Cybersecurity: Networks and Systems

Description:
The "Quantum Technologies for Cybersecurity: Networks and Systems" seminar aims to provide participants with a comprehensive understanding of quantum technology and its applications in cybersecurity. The seminar is divided into seven sessions, each focusing on different aspects of quantum technology and cybersecurity: Introduction to Quantum Technologies for cybersecurity, Quantum implementation aspects, Key building blocs, Quantum Technologies Ecosystem, Quantum hardware and Systems, Quantum Security: Networking and Systems, and Quantum cybersecurity perspective.

The topics proposed for the seminar, such as fundamental practical quantum physics and quantum cybersecurity applied to general communication systems and networks, provide a unique and valuable learning experience for students.

Introduction to Quantum Technologies for cybersecurity
Description:
a) The Quantum technology revolution: Quantum supremacy/detectability and Implications (Risk and opportunities) to Cybersecurity.
b) Overview of Quantum Technology application domains: Information, Computing, Communication and Sensing, Cybersecurity.
Full-or-part-time: 7h
Theory classes: 3h
Self-study: 4h

Quantum implementation aspects
Description:
a) Quantum Information principal pillars: qubit, state-vector, superposition, measurement, interference, entanglement and no-cloning.
b) Common quantum limitations and challenges: noise and loss, indistinguishability, decoherence and fidelity.
Full-or-part-time: 8h
Theory classes: 3h
Self-study: 5h

Key building blocks
Description:
a) Eavesdropping detection: Quantum key distribution - fiber & free-space, polarization and phase encoding, discrete and continuous variables.
b) Other building blocks: teleportation and entanglement-swapping.
Full-or-part-time: 8h
Theory classes: 3h
Self-study: 5h

Quantum Technologies Ecosystem
Description:
a) Migration to Post-quantum cryptography.
b) Telecommunication systems quantum cybersecurity.
Full-or-part-time: 9h
Theory classes: 3h
Self-study: 6h

Quantum hardware and systems
Description:
a) Quantum Hardware: sources, transformation modules, detectors, time-tagging units, coincidence detectors.
b) Quantum Systems: random number generators, memories, routers, repeaters and firewalls.
Full-or-part-time: 8h
Theory classes: 3h
Self-study: 5h

Quantum Security: Networking and Systems
Description:
a) Quantum internet: networking and routing.
b) Quantum secure systems: authentication and password identification.
Full-or-part-time: 8h
Theory classes: 3h
Self-study: 5h

Quantum cybersecurity perspective
Description:
a) In-class mapping of the ecosystem of quantum technologies for cybersecurity.
b) Markets and application domains.
Full-or-part-time: 2h
Theory classes: 2h
Self-study: 0h

Full-or-part-time: 50h
Theory classes: 20h
Self study: 30h

GRADING SYSTEM
- Participation in class (20%).
- Problems and/or group or individual presentation (80%).

BIBLIOGRAPHY

Basic:

Complementary:

RESOURCES

Other resources:
Scripts  Python with examples and exercises available at:
https://github.com/marciofreProf/SeminarQuantumTechnologiesCybersecurity