COM-440

Introduction to quantum cryptography

Liu Yupan, Vidick Thomas

Cursus	Sem.	Type
Computer science	MA1, MA3	Opt.
Cyber security minor	H	Opt.
Cybersecurity	MA1, MA3	Opt.
Data Science	MA1, MA3	Opt.
Quantum Science and Engineering	MA1, MA3	Opt.

Language of teaching	English
Credits	6
Session	Winter
Semester	Fall
Exam	Oral
Workload	180h
Weeks	14
Hours	**4 weekly**
Courses	3 weekly
Exercises	1 weekly
Number of positions	

Remark

This course is a « depth » for Cyber Security master program and Cyber Security minor

Summary

In this course we discover some cryptographic tasks for which quantum information provides a decisive advantage. In each case we model the task and define security precisely, and then develop the mathematical techniques required to show security.

Content

It has been known since the 1980s that the use of quantum information could enable certain cryptographic tasks, such as quantum money or quantum key distribution, that are impossible classically without making computational assumptions.

- Quantum money: Wiesner's scheme and attacks on it
- The quantum one-time pad
- Entanglement and non-local games
- Quantum key distribution: the BB'84 protocol
- Ekert's protocol and device independence
- Two-party cryptography: bit commitment, oblivious transfer, coin-flipping
- The noisy storage model
- Quantum encryption
- Delegated computation

Learning Prerequisites

Required courses

- An introduction to quantum computation, such as CS-308 Introduction to quantum computation, COM-309 Introduction to quantum information processing, PHYS-541 Quantum computing or PHYS-550 quantum information theory.

Recommended courses

- A course in cryptography such as COM-401 Cryptography and Security can help engage with the material, but is not required

Important concepts to start the course

- Basics of quantum computing, including qubits, density matrices, POVM, quantum gates and circuits
- Discrete mathematics techniques in computer science, such as asymptotic estimates, Chernoff (concentration) bounds
- Algorithmic reasoning

No prior knowledge of cryptography is required, but some familiarity with the principles of quantum information, as well as some background in algorithms or complexity, are highly recommanded.

Learning Outcomes

By the end of the course, the student must be able to:

- Design , analyse and show security of cryptographic protocols that make use of quantum information to implement novel tasks with strong security guarantees
- Assess / Evaluate the (theoretical) security of a quantum cryptographic scheme and investigate possible attacks on it
- Learn or solidify your knowledge of quantum computing

Teaching methods

- Ex-cathedra
- Project

Expected student activities

- Attend lecture and participate orally
- Perform the required reading and homework exercises
- Project work: prepare an oral presentation on a topic in quantum cryptography

Assessment methods

- Written midterm, based on solving mathematical problems
- Presentation of project and oral examination

Supervision

Office hours	Yes
Assistant.e.s	Yes
Forum	Yes

Resources

Bibliography

Vidick and Wehner, Introduction to Quantum Cryptography, Cambridge University Press, 2023.

Ressources en bibliothèque

- Find the references at the Library

Moodle Link

- https://go.epfl.ch/COM-440