COM-622

Topics in information-theoretic cryptography

Shkel Yanina

Cursus	Sem.	Type
Computer and Communication Sciences		Opt.

Language of teaching	English
Credits	2
Session	
Exam	Term paper
Workload	60h
Hours	**28**
Courses	28
Number of positions	

Frequency

Every year

Remark

Next time: Fall 2021

Summary

Information-theoretic methods and their application to secrecy & privacy. Perfect information-theoretic secrecy. Randomness extraction & privacy amplification. Secret key generation from common randomness. Measures of information leakage incl. differential privacy, perfect privacy, & mutual info.

Content

This is a theoretical course that will survey the interaction between information theory, cryptography, security, and privacy. It will provide a historic perspective on the interplay of these fields, as well as introduce some new and emerging developments. This course will mainly focus on questions related to secrecy and information. We will ask very basic theoretical questions like:
- What is information?
- ##What does it mean to keep information secret?
- How do we model informatoin secrecy mathematically?
- What kinds of resources (randomness, computation, communication, etc.) are needed to achieve this?
- and so on.

Topics covered in the course include perfect secrecy, information-theoretic secret key generation, randomness extraction, information leakage measures like differential privacy, mutual information, as well as some emerging approaches like maximal leakage and perfect privacy.

Learning Prerequisites

Required courses

Probability Theory, General Mathematical Maturity, Information Theory and Coding or equivalent (for MSc students)

Recommended courses

(Information Theory and Coding or equivalent are recommended, but not required for PhD students.)