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 | Written |
| Workload | 60h |
| **Hours** | **28** |
| Courses | 20 |
| Exercises | 8 |
| **Number of positions** | **30** |

## Frequency

Only this year

## 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 secret communication. We will ask very basic theoretical questions like:
- "What does it mean to keep information secret? and "How do we model secrecy mathematically?
- "What kinds of resources (randomness, computation, communication, etc.) are needed to achieve secrecy?
- "What are the fundamental limits of secrecy preserving systems?

Specifically, there are two types of cryptographic security: security that relies on computational infeasibility of breaking the system and security that relies on theoretical infeasibility of breaking the system (even given a computationally unbounded adversary). The later is called "information-theoretic" security, and this is what we focus on in this course.
We will start with Shannon's notion of perfect secrecy and see how perfect secrecy is either expensive, or infeasible. It is expensive in the communication setting since it requires a large shared secrete key between the two parties; and, it is infeasible in the privacy setting, for example, where the goal is to publish a privacy preserving dataset for public use. We will then compare and contrast this kind of information-theoretic security with computational security approaches such as semantic security.
We will spend the rest of the semester addressing these two problems that come out of our study of perfect secrecy: secret key generation, and notions of partial secrecy. We first turn to the problem of secret key generation starting with randomness extraction and moving on to generating secret keys from common randomness over communication channels. We then look at ways to quantify partial secrecy with 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.)