E2 213 Jan. 3:0

Information-Theoretic Security

Instructor

Navin Kashyap
Email: nkashyap@iisc.ac.in

Teaching Assistant

Email:

Department: Electrical Communication Engineering

Course Time:

Lecture venue:

Detailed Course Page:

Announcements

Brief description of the course

Information-theoretic security is an "unconditionally" secure alternative to cryptography. The security guarantees provided within this paradigm are "unconditional" in the sense that they do not rely on any assumptions on the computational resources available to the adversary. Nevertheless, information-theoretic security has struggled to become a viable alternative to cryptography in practice because it makes other assumptions that are difficult to validate in a practical setting.

This course offers a comprehensive introduction to the subject of information-theoretic security, starting with the groundbreaking work of Claude Shannon in 1949. The intended audience consists of graduate students with a good background in information theory. The course aims to expose students to topics of current research in the field.

Prerequisites

A first course in information theory (E2 201 or equivalent).

Syllabus

The course covers the following broad topics:

1. Shannon's model of perfect secrecy.

2. Wiretap channels. Wyner's channel model, rate-equivocation region, secrecy capacity, from weak to strong secrecy using hash functions, polar coding for wiretap channels

3. Secret key agreement via public discussion. Results for the two-terminal model by Maurer and Ahlswede-Csiszar, extension to the multiterminal model by Csiszar and Narayan, multivaritate mutual information, the leftover hash lemma.

Course outcomes

A student taking this course is expected to learn the basic tools and techniques needed to carry out research in information-theoretic security. The student will also understand the practical barriers that prevent this paradigm from becoming a viable alternative to mainstream cryptography.

Grading policy

10% for attendance, 40% for homework assignments, 50% for a project presentation.

Assignments

Homework assignments consist primarily of exercises given during lectures.

Resources

Books:

M. Bloch and J. Barros, Physical-Layer Security. Cambridge Univ Press, 2011.

P. Narayan and H. Tyagi, Multiterminal Secrecy by Public Discussion, NOW Publishers, Sept. 2016.