FEO3320 Information Theoretic Security 8.0 credits

Informationsteoretisk säkerhet

This is a translation of the Swedish, legally binding, course syllabus.

If the course is discontinued, students may request to be examined during the following two academic years

Establishment

Course syllabus for FEO3320 valid from Autumn 2013

Grading scale

Education cycle

Third cycle

Specific prerequisites

Prerequisite for this course is the basic course on information theory:

EO3210 Information Theory 12,0 hp

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

After the course, the student should be able to:

- describe the general principles of information theoretic security☐
- explain fundamental concepts and tools of information theoretic security such as perfect secrecy, wiretap codebook, secret sharing codebook, secrecy capacity, secret key capacity etc.☐
- prove the most fundamental theorems in the subject of information theoretic security☐
- describe how the fundamental tools of information theoretic security can be exploitedin the other areas of modern communication technology
- using the concepts and tools in the area to formulate the problem and solve them in other setups other than the fundamental works such as different channel models or advanced problems

Course contents

· Introduction to the course + Recapitulation (AEP, strong typicality) (1

session)

· Shannon secrecy system (Perfect security principle and notions+ introduction on security) (1 session)

· Wiretap channel (secrecy capacity, wiretap codebook, converse proof methods) (1 session)

· Secret key agreement (secret key capacity in source and channel model, secret sharing codebook, converse proof methods), (2 sessions)

· Introduction on secrecy capacity (region) of different channel models (with emphasis on discrete memoryless channels and Gaussian channels), (1 or 2 sessions)

· Source coding with security constraint (1 session)

· Secure network coding (1 session)

Disposition

Lectures (mainly given by Somayeh Salimi), homework problems (done in an individual base), presentation/review of a journal paper in the field

Course literature

"Information Theoretic Security", Y. Liang, H. V. Poor and S. Shamai (Now publishers Inc.

2009: ISBN-10: 1601982402).

"Lecture Notes on Network Information Theory", A. El Gamal and Y. -H. Kim

(available under http://arxiv.org/abs/1001.3404).

"Physical-Layer Security: From Information Theory to Security Engineering", M. Bloch, J. Barros (Cambridge 2011: ISBN-10: 0521516501).

Examination

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

Other requirements for final grade

The main focus is on homework problems and the final presentation based on reviewing a journal paper in the field.

☐

Homework: The students have to hand in every homework. A minimum number of points must be achieved for each homework along with the sum of all achieved points.

☐

Final presentation: Some journal papers will be suggested and each student should select one. The students can suggest other paper related to information theoretic security but it should be adjusted with the teacher. Based on the selected topic, each student should review the paper and present it in a 30-min talk. It is expected that the students understand the technical details of the chosen paper. Furthermore they should try to evaluate the paper in a wide context (How reasonable is the scenario? what are the new concepts and insight introduced? how reasonable are the assumptions? etc.)

Ethical approach

- All members of a group are responsible for the group's work.
- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.