FEO3320 Informationsteoretisk säkerhet 8,0 hp

Information Theoretic Security

När kurs inte längre ges har student möjlighet att examineras under ytterligare två läsår.

Fastställande

Kursplan för FEO3320 gäller från och med HT13

Betygsskala

Utbildningsnivå

Forskarnivå

Särskild behörighet

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

EO3210 Information Theory 12,0 hp

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

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

Kursinnehåll

· 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)

Kursupplägg

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

Kurslitteratur

"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

Examinator beslutar, baserat på rekommendation från KTH:s handläggare av stöd till studenter med funktionsnedsättning, om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning.

Examinator får medge annan examinationsform vid omexamination av enstaka studenter.

Övriga krav för slutbetyg

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.)

Etiskt förhållningssätt

- Vid grupparbete har alla i gruppen ansvar för gruppens arbete.
- Vid examination ska varje student ärligt redovisa hjälp som erhållits och källor som använts.
- Vid muntlig examination ska varje student kunna redogöra för hela uppgiften och hela lösningen.