Fall 2021 – COM 622

Title: Topics in Information-Theoretic Cryptography

Time and Location: Thursdays 8:15-10am, BC03
Instructor: Yanina Shkel
Office Hours: By Appointment, INR 131 **Email:** yanina.shkel@epfl.ch
Course Webpage: Moodle (contact the instructor for enrollment)

Special Course Notes: The target audience for this course is graduate students in information theory and communications, as well as theoretically minded student in privacy and security. This course may also be of interest to students in theoretical computer science. **The first lecture** will take place **on September 30**, and the last lecture is expected to take place on December 16. We will cover a selection of papers from the provided reading list. You are welcome to audit the course, even if you already took it last semester, since the sets of papers covered each semester will have a very small intersection.

Overview: This semester we will do a survey of a large body of work on statistical measures of information. Our particular focus will be on understanding the motivation behind some of the more commonly used notions that relate to capturing and measuring information. For example, many classical information-theoretic measures (e.g. entropy, mutual information) arise as answers to specific engineering questions (how well could we compress this data? how much data could we send over this noisy communication channel?). This provides a strong justification for their use and imbues them with meaning. At the same time, many measures of information leakage for privacy and secrecy applications (e.g. differential privacy, maximal leakage) are postulated as the 'correct' measure of leakage first, and then applied as a performance gauge to the design of actual algorithms and systems.

Some of the topics may include: traditional information-theoretic notions like entropy, mutual information, and relative entropy; their extensions to Renyi entropy, Renyi divergence, alpha-mutual information; various notions of common information; 'operationally' defined measures of information leakage like differential privacy and maximal leakage; and a closely related question of statistical measures of fairness. We will discuss the motivation behind these measures, their mathematical properties, as well as their strengths and weaknesses.

Course Format: The format is based on paper reading and presentation during lecture. The instructor will present the papers, but an active participation from class is encouraged. We expect to have 10-12 lectures total with 1-2 reading assignments per lecture. Lectures will be in person as much as possible given the current epidemiological situation. However, an option to view them online through Zoom will be available. Lectures will not be recorded.

Grading: The final grade will be based 20% on course participation and 80% on the final project. Course participation includes completing reading assignments, attending lectures, and asking questions in lecture. The final project will include a scientific assignment based on another chosen article. Choices for project assignments include extension of existing results, implementation tasks, critical summary of a paper, etc. Students may use a paper from the provided reading list or suggest their own paper. You should communicate your final project topic to the instructor a month before the final due date.