Title: Semantic Security versus Active Eavesdroppers

Speaker: Ziv Goldfeld

Time and location: Thursday, March 10, 2016 11:00 a.m., ECE 202

Abstract:

Information theoretic security has adopted the weak- and strong-secrecy metrics as a standard for measuring security. Respectively, weak- and strong-secrecy refer to the normalized and unnormalized mutual information between the secret message and the channel symbol string observed by the eavesdropper. From a cryptographic point of view, however, both these metrics are insufficient to provide security of applications. Their main drawback lies is the assumption that the message is random and uniformly distributed, as real-life messages are neither (messages may be files, votes or any type of structured data, often with low entropy). Semantic-security (SS) is a cryptographic gold standard that demands negligible mutual information between the message and the eavesdropper's observations even when maximized over all message distributions.

However, finding one sequence of codes that simultaneously satisfies the vanishing information leakage requirement for all message distributions requires stronger tools than currently available. To resolve this prerequisite we introduce a novel and stronger version of Wyner's soft-covering lemma, which sharpen the claim by moving away from an expected value analysis. Instead, we show that a random codebook achieves the soft-covering phenomenon with probability that is doubly-exponentially (in the blocklength) close to 1. Through the union bound, this enables security proofs in settings where many security constraints must be satisfied simultaneously.

As a first application of the stronger soft-covering lemma we solve the open problem of the type II wiretap channel (WTC II) with a noisy main channel by deriving its SS-capacity and showing that it is equal to its weak-secrecy capacity. In this setting, the legitimate users communicate via a discrete-memoryless (DM) channel in the presence of an eavesdropper that has perfect access to a subset of its choosing of the transmitted symbols, constrained to a fixed fraction of the blocklength. The SS criterion demands negligible mutual information between the message and the eavesdropper's observations for all possible eavesdropper subset choices and message distributions. Since the combined number of messages and subsets grows only exponentially with the blocklength, the stronger soft-covering lemma is sharp enough to imply the desired security performance. Another application is a single-letter characterization of the correlated-random-assisted SS-capacity of an arbitrarily varying wiretap channel (AVWTC) with type constrained states.

(Joint work with Prof. Paul Cuff from Princeton University and Prof. Haim Permuter from Ben-Gurion University.)

Bio:

Ziv Goldfeld received his B.Sc. (summa cum laude) and M.Sc. (summa cum laude) degrees in Electrical and Computer Engineering from the Ben-Gurion University, Israel, in 2012 and 2014, respectively. He is currently a student in the direct Ph.D. program for honor students in Electrical and Computer Engineering at that same institution supervised by Prof. Haim Permuter.

In 2014 Ziv was awarded the IEEE 28-th Convention of Electrical and Electronics Engineers in Israel best student paper award for his work titled “Semi-Deterministic Broadcast Channels with Cooperation”.

Ziv is a recipient of several awards, among them a Feder Award, the Lev-Zion fellowship, a Minerva Short-Term Research Grant (MRG), Dean's List Award and the Basor Fellowship for honor students in the direct Ph.D. program.