abstract

COMPUTER SCIENCE AND DISCRETE MATHEMATICS SEMINAR II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

In this talk, I will give new proofs for the hardness amplification of fficiently samplable predicates and of weakly verifiable puzzles. More oncretely, in the first part of the talk, I will give a new proof of Yao's XOR-Lemma as well as related theorems in the cryptographic setting. This proof seems simpler than previous ones, yet immediately generalizes to statements similar in spirit such as the extraction lemma used to obtain pseudo-random generators from one-way functions [Hastad, Impagliazzo, Levin, Luby, SIAM J. on Comp. 1999].

In the second part of the talk, I will give a new proof of hardness amplification for weakly verifiable puzzles, which is more general than previous ones in that it gives the right bounds for arbitrary monotone function applied to the checking circuit of the underlying puzzle.

Both of the aforementioned proofs are applicable in many settings of interactive cryptographic protocols because they satisfy a property that we call non-rewinding. In particular, I will show that any weak cryptographic protocol whose security is given by the unpredictability of single bits can be strengthened with a natural information theoretic protocol. As an example, I'll show how these theorems solve the main open question from [Halevi and Rabin, TCC2008] concerning bit commitment.

Joint work with Thomas Holenstein.