abstract

Computer Science/Discrete Mathematics Seminar I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Shannon's notion of entropy measures the amount of "randomness" in a process. However, to an algorithm with bounded resources, the amount of randomness can appear to be very different from the Shannon entropy. Indeed, various measures of "computational entropy" have been very useful in computational complexity and the foundations of cryptography. In this talk, I will describe two new measures of computational entropy ("next-bit pseudoentropy" and "inaccessible entropy") that have enabled much simpler and more efficient constructions of cryptographic primitives from one-way functions. In particular, I will discuss a construction of pseudorandom generators of seed length O(n^3) from a one-way function on n bits, improving the seed length of O(n^8) in the classic construction of Hastad, Impagliazzo, Levin, and Luby.

Joint works with Iftach Haitner, Thomas Holenstein, Omer Reingold, Hoeteck Wee, and Colin Jia Zheng.