abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Ideally, one would want to base the security of standard cryptographic primitives (such as pseudorandom generators) on widely believed worst-case complexity assumptions like P does not equal NP. However, it is currently not known if this is possible, and several obstacles have been pointed out in the last few years. We propose to study relaxed definitions of cryptographic primitives where some of the honest parties may be given more resources than the adversary. While such definitions are useless for common cryptographic applications, they may shed more light on the relation between worst-case complexity, average-case complexity, and cryptography. As an initial step, we show that "quasi-one-way functions" may be realized from worst-case assumptions such as P does not equal NP, but standard techniques to turn these into "quasi-pseudorandom generators" fail in our setting.

(Joint work with Kunal Talwar and Andrew Wan.)