abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Amplifying the difficulty of a somewhat hard function is a central technique in complexity, cryptography and pseudorandomness. By far the most common method of amplification is by repetition - asking to compute the original function in many independent inputs (and return all answers, or some combination thereof. e.g. their XOR). The fact that the new function is much harder than the original received many different proofs since Yao's original statement in 1982. Each proof has certain advantage over the others in different contexts. I will attempt to describe a few of these, and discuss their utilities.