# abstract

COMPUTER SCIENCE/DISCRETE MATH SEMINAR, I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

The goal of hardness amplification is to take a function f : {0,1}^n --> {0,1} that is mildly average-case hard (i.e., very "small" circuit fails to compute f on at least a 1/poly(n) fraction of inputs), and produce a new function f' that is very hard on average (i.e., every "small" circuit fails to compute f' on nearly half of its inputs).

In this work we study hardness amplification within NP -- this problem was first studied by O'Donnell (STOC 2002). He showed how to take a mildly average-case hard function f in NP, and produce a function f', also in NP, such that every "small" circuit fails to compute f' on roughly a (1/2 - 1/n) fraction of inputs. O'Donnell also showed that constructions of a certain general form cannot amplify beyond hardness (1/2 - 1/n).

In this work we prove hardness amplification up to (1/2 - 1/2^{\sqrt{n}}) within NP. That is, starting from a mild average-case hard f in NP, we produce f' in NP such that every "small" circuit fails to compute f' on a (1/2 - 1/2^{\sqrt{n}}) fraction of inputs.

To bypass the barrier shown in O'Donnell's work, we employ two new techniques. First, we show how to derandomize O'Donnell's construction using a certain "pseudorandom generator". Second, we show how to use nondeterminism in the hardness amplification -- this is in contrast to previous hardness amplifications which are deterministic.

Joint work with Alex Healy and Salil Vadhan.