abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Pseudo-random generators that are secure against constant depth polynomial size circuits have been known since the seminal paper by Ajtai and Wigderson (1985). All available constructions of such generators, however, appear to be somewhat special and ad hoc. In 1990, Linial and Nisan made a bold and elegant conjecture stating that this property is in fact possessed by any generator in which any selection of polylogarithmically many output bits is independent; examples of such generators are abundant. This conjecture turned out surprisingly difficult, and it was only the last year that Bazzi proved it for the case of DNF formulas. The main purpose of our talk is to present a substantially simplified version of his proof.