# abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

A given function f(x) is "hard on average" with respect to an algorithm A , if A(x) disagrees with f(x) on "many" inputs x. Applications in cryptography and derandomization require functions that are "very hard on average" (essentially unpredictable) with respect to any efficient algorithm. An algorithmic procedure of converting a "somewhat hard on average" function f(x) into a "much harder on average" function g(x) is called hardness amplification.

A primary tool for hardness amplification is the classical Direct Product Theorem that essentially says the following: If a function f(x) is "somewhat hard on average", then the function f^k(x_1,...,x_k)=f(x_1)...f(x_k) (required to compute the value of f on each of k independent inputs x_1,...,x_k) is "much harder on average", where the amount of hardness increases exponentially fast with the parameter k. In the language of error-correcting codes this
basically means that the truth table of the direct-product function f^k can "tolerate" many more corruptions than the truth table of f . Of special interest is an efficient error-correcting (decoding) algorithm for such "Direct Product Codes".

Our main result is a simple, efficient decoding algorithm for Direct Product codes, which achieves information-theoretically optimal parameters (up to constant factors); thus it significantly improves on an earlier result of [Impagliazzo, Jaiswal, and Kabanets; FOCS'06]. We also define a more general class of "direct product"-like codes with efficient decoding algorithms, which in particular yields a certain "derandomized" version of the Direct Product Theorem.

Joint work with Russell Impagliazzo (UCSD & IAS), Ragesh Jaiswal (UCSD), and Avi Wigderson

(IAS).