In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

## *ITCSC Seminar*

# Combinatorial Constructions of One-way Functions and Their Security

By
**Prof. Andrej Bogdanov**
*Assistant Professor, Computer Science and Engineering Department, CUHK*

***November 19, 2009 (Thursday)***

***4:30pm - 5:30pm***

***Rm. 121, Ho Sin Hang Engineering Building, CUHK***

**Abstract:**

A one-way function is a function that is easy to compute, but computationally hard to invert. One-way functions enable cryptographic tasks such as symmetric key encryption, message authentication, and zero-knowledge proofs.

Goldreich (ECCC 2000) suggested a simple combinatorial construction of a candidate one-way function where each bit of output is a fixed predicate P of a constant number d of (random) input bits. We investigate the security of this construction in the regime m = Dn, where D(d) is a sufficiently large constant. (In contrast, Goldreich looked at the regime m = n.) We prove that for any predicate P that correlates with either one or two of its variables, f can be inverted with high probability, thus it is not one-way.

***** ALL ARE WELCOME *****

Host & Enquiries : Institute of Theoretical Computer Science and Communications Tel: 2696 1257