In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

ITCSC-CSE Joint Seminar

Randomness Extraction from Generalized Santha-Vazirani Sources

By
Dr. Omid Etesami
Institute for Research in Fundamental Sciences (IPM)

April 18, 2016, Monday
3:00 pm – 4:00 pm
Room 1009, 10/F, William M. W. Mong Engineering Building, CUHK

Abstract:
Randomized algorithms and protocols require a source of randomness for their execution. However, in the real world most sources of randomness are imperfect. Randomness extraction is the process of turning a slightly random bit string into a shorter almost perfectly random string.

A Santha-Vazirani (SV) source is a sequence of random bits where the conditional distribution of each bit, given the previous bits, can be partially controlled by an adversary. We talk about a generalization of SV sources for non-binary sequences. We show using "martingales" that unlike the binary case, deterministic randomness extraction in the generalized case is sometimes possible.

We also consider a distributed version of SV sources in which the goal of the extraction is to obtain common randomness shared among different parties. We show using "maximal correlation" that randomness extraction in this distributed case essentially reduces to randomness extraction from (non-distributed) SV sources.

Biography:
Omid Etesami is a researcher at Institute for Research in Fundamental Sciences (IPM) in Iran. Previously he did his undergraduate studies at Sharif University of Technology, his PhD at University of California, Berkeley, and a postdoc at EPFL, Switzerland.

As an undergraduate, he participated in programming competitions. During his PhD, he worked at Microsoft research and was supported by their PhD fellowship. Recently, his paper has been selected as a Best of 2014 paper in Computer Science by ACM Computing Reviews.

His research interest is the use of probability and randomness in computer science, including pseudorandomness, error-correcting codes and one-way functions based on random graphs, using randomness in auction and differential privacy mechanisms, and aspects of average-case analysis.

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

Hosted & Enquiries : Institute of Theoretical Computer Science and Communications Tel: 3943 1257