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

Physical Randomness Extractors:
Generating Random Numbers with Minimal Assumptions

By

Dr. Kai-Min Chung

Assistant Research Fellow, Institute of Information Science, Academia Sinica

August 7, 2014, Thursday

11:00 am – 12:00 noon

Room 121, 1/F, Ho Sin Hang Engineering Building, CUHK

Abstract:

How can one be certain that the output of an alleged random number generator is indeed random? This question is important not only for the efficiency and the security of information processing, but also for understanding how extremely unpredictable events are possible in Nature. All existing solutions require a certain form of independence among two or more sources of randomness, an assumption impossible to test and difficult to guarantee.

In this talk, we show how this fundamental limit can be circumvented based on the validity of physical laws. We envision to extract randomness from physical systems that consists of a single classical source and a set of non-communicating quantum devices whose inner-workings are unknown or may even be malicious. As long as the classical source has sufficient (min-)entropy (say, 1000 bits) with respect to the devices, we are able to extract a constant fraction of entropy out from the physical system, and produce a close-to-uniform string of arbitrary length as long as the devices supply sufficient entropy. Additionally, our physical extractor is efficient and tolerates a constant level of implementation imprecision.

Our method enables practical provably secure random number generation with minimal assumptions. It also implies that close-to-uniform randomness either does not exist in Nature or exist in abundance. Our explicit construction also provides both a practical and the strongest known method for mitigating the Freedom-of-Choice loophole for refuting local hidden variable theories.

No quantum background is assumed in this talk. The talk is based on a joint work with Yaoyun Shi and Xiaodi Wu.

Biography:

Kai-Min Chung is an assistant research fellow at Institute of Information Science (IIS), Academia Sinica in Taiwan. Prior to joining IIS, he was a postdoc at Cornell University supported by Simons Postdoctoral Fellowship in 2010-2013, and received his Ph.D. in computer science at Harvard University. His research interests are in the fields of cryptography, complexity theory, and quantum cryptography. His work on parallel repetition for interactive arguments received a best student paper award from Theory of Cryptography Conference (TCC) in 2010. He has served on the program committees of cryptography conferences including CRYPTO, TCC, and Asiacrypt.

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

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