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

Cryptography with Streaming Devices

By
Prof. Periklis Papakonstantinou
Assistant Professor, IIIS/ITCS Tsinghua University

February 21, 2013, Thursday
10:30am – 11:30am
Room 121, 1/F., Ho Sin Hang Engineering Building, CUHK

Abstract:
We ask whether Cryptography can be done using a streaming device. Streaming devices have access to read/write external memory (e.g. hard drives) limited to be scanned sequentially, and also to an internal memory which is limited in size. Is it possible to compute cryptographic primitives with such a device when the hard disks can be scanned in total a small constant (e.g. 4-5 times) and the internal memory is as small as logarithmic.

In this setting none of the popular intractability assumption can be computed (because streaming devices provably cannot do simple computations such as multiplying two integers). How to do Cryptography based on the assumption that factoring a large composite is hard, using a device that cannot multiply numbers? Surprisingly enough we show that this can be done. We employ
non-black-box techniques borrowed from the field of multi-party computation (MPC) using the concept of randomizing polynomials which appears in the work of Applebaum-Ishai-Kushilevitz on Cryptography in NC^0 (the main concepts date back to Yao's garbled circuit). Our work is different than the [AIK] in several senses. For example, under a variant of the Learning With Errors assumption we construct Public-Key Encryption whereas no such thing is possible for NC^0.

This is joint work with Guang Yang.

Biography:
Prof. Papakonstantinou is an Assistant Professor at the Institute for Theoretical Computer Science of the Institute for Interdisciplinary Information Sciences, Tsinghua University. Right before that he did a PhD in Computer Science, an MSc in Mathematics (simultaneously to the PhD), and before that an MSc in Computer Science, all from the University of Toronto. His undergraduate studies were in Computer Engineering and Science, University of Patras, and he is a licensed Electronics Engineer with the Technical Chamber of Greece.

His research biases are towards Cryptography, Computational Complexity, computational problems with engineering motivation -- in particular their intersection with Algebra, Combinatorics, and Randomness.

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

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