In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

Crypto Day

January 4, 2010 (Monday)
Room 121, Ho Sin-Hang Eng., Bldg., CUHK

2:00 – 2:45pm

Non-uniform Attacks Against One-way Functions and Pseudorandom Generators

Prof. Luca Trevisan, Professor, UC Berkeley

Abstract
We study the power of non-uniform attacks against one-way functions and pseudorandom generators. Fiat and Naor show that for every function f:[N]- > [N] there is an algorithm that inverts f everywhere using (ignoring lower order factors) time, space and advice at most N^{3/4}.

We show that an algorithm using time, space and advice at most

max { (epsilon*N)^{1/2} , epsilon^{5/4} * N^{3/4} }

exists that inverts f on at least an epsilon fraction of inputs. A lower bound of (epsilon*N)^{1/2} also holds, making our result tight in the ``low end'' of small epsilon.

We also show that for every length-increasing generator G:[N]->[2N] there is a algorithm that achieves distinguishing probability epsilon between the output of G and the uniform distribution and that can be implemented in polynomial (in logN) time and with advice and space O(epsilon2 * NlogN). Alternatively, it can be implemented as a circuit of size O(epsilon2 * N). We prove a lower bound of

ST > epsilon2 * N

where T is the time used by the algorithm and S is the amount of advice. We prove stronger lower bounds in the common random string model, for families of one-way permutations and of pseudorandom generators.

(Joint work with Anindya De and Madhur Tulsiani.)

Biography
Luca Trevisan is a professor of electrical engineering and computer science at U.C. Berkeley. Luca received his PhD in 1997 from the University of Rome La Sapienza. Before coming to Berkeley in 2000, Luca was a post-doc at MIT and at DIMACS, and an assistant professor at Columbia University.

Luca's research is in theoretical computer science, and most of his work has been in two areas: (i) the study of randomness and pseudorandomness in computation and in combinatorics; and (ii) the theory of probabilistically checkable proofs and its relation to the approximability of combinatorial optimization problems.

Luca received the STOC'97 Danny Lewin (best student paper) award, the 2000 Oberwolfach Prize, and the 2000 Sloan Fellowship. He was an invited speaker at the 2006 International Congress of Mathematicians in Madrid.

In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

3:00 – 3:45pm
Optimal Quantum Strong Coin Flipping

Prof. Iordanis Kerenidis, Senior Researcher, Universite de Paris

Abstract
Coin flipping is a fundamental cryptographic primitive that enables two distrustful and far apart parties to create a uniformly random bit. Quantum information allows for protocols in the information theoretic setting where no dishonest party can perfectly cheat. The previously best-known quantum protocol by Ambainis achieved a cheating probability of at most 3/4. On the other hand, Kitaev showed that no quantum protocol can have cheating probability less than 1/sqrt(2). Closing this gap has been one of the important open questions in quantum cryptography.

In this talk, we will present a quantum strong coin flipping protocol with cheating probability arbitrarily close to 1/sqrt(2). More precisely, we will show how to use any weak coin flipping protocol with cheating probability 1/2 + eps as a subroutine in a purely classical protocol in order to achieve a strong coin flipping protocol with cheating probability 1/sqrt(2) + O(eps). The optimal quantum strong coin flipping protocol follows from our construction and the optimal quantum weak coin flipping protocol described by Mochon.

No knowledge of any quantum information is necessary for the talk. This is joint work with Andre Chailloux and appeared at FOCS 2009.

Biography
Iordanis Kerenidis received his PhD from the Computer Science department at the University of California, Berkeley. After a two-year postdoctoral position at the Massachusetts Institute of Technology he moved to France, where he now holds a Senior Researcher CNRS position, based at the Universite Paris-Sud. His research interests lie in the intersection of quantum computation and complexity theory.

4:00 – 4:45pm
Encryption Schemes Secure Against Selective Opening Attacks on Receivers

Prof. Hoeteck Wee, Assistant Professor, Computer Science, Queens College, City University of New York

Abstract
Consider a setting in which a single sender is transmitting encrypted data to multiple receivers. Now, suppose we have an adversary that has the power to corrupt a subset of the receivers and learn their secret keys; can we then guarantee security of the unopened ciphertexts? We present the first efficient public-key encryption schemes that achieve security against such selective opening attacks on the receivers.

Biography
Hoeteck Wee is an assistant professor at Queens College, CUNY. He received his PhD from UC Berkeley under the supervision of Luca Trevisan and his BSc from MIT. He was previously a post-doc at Columbia University and a visiting student at Tsinghua University and IPAM. His research revolves around the design and analysis of cryptographic protocols. Hoeteck lives in a Manhattan neighborhood abundant with cafes and restaurants so as to cut down on his daily commute (and carbon footprint). This is his third visit to CUHK.