In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering

Seminar

Statistically-secure Oblivious RAMs with Improved Efficiency

by
Dr. Kai-Min Chung
Institute of Information Science (IIS)
Academia Sinica
Taiwan

Date : 12 Jan., 2015 (Mon.)
Time : 4:15 - 5:15pm
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract
We demonstrate a simple, statistically secure, ORAM with computational overhead O ($\log^2$ n); previous ORAM protocols achieve only computational security (under computational assumptions) or require Ω ($\log^3$ n) overheard. An additional benefit of our ORAM is its conceptual simplicity, which makes it easy to implement in both software and (commercially available) hardware.

Our construction is based on recent ORAM constructions due to Shi, Chan, Stefanov, and Li (Asiacrypt 2011) and Stefanov and Shi (ArXiv 2012), but with some crucial modifications in the algorithm that simplifies the ORAM and enable our analysis. A central component in our analysis is reducing the analysis of our algorithm to a "supermarket" problem; of independent interest (and of importance to our analysis,) we provide an upper bound on the rate of "upset" customers in the "supermarket" problem.

Joint work with Zhenming Liu and Rafael Pass

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 with recent focus on developing cryptographic solutions suitable for cloud environments, and techniques for post-quantum cryptography against quantum side information. 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 ****

Host: Professor Sherman S.M. Chow (Tel: 3943-8376, Email: smchow@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)