



香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

ITCSC-CSE Joint Seminar

An Algebraic Approach to Non-Malleability

By

Prof. Alon Rosen

Associate Professor, School of Computer Science, Herzliya Interdisciplinary Center

August 7, 2014, Thursday

12:00 noon – 1:00 pm

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

Abstract:

In their seminal work on non-malleable cryptography, Dolev, Dwork and Naor, showed how to construct a non-malleable commitment with logarithmically-many "rounds"/"slots", the idea being that any adversary may successfully maul in some slots but would fail in at least one. Since then new ideas have been introduced, ultimately resulting in constant-round protocols based on any one-way function. Yet, in spite of this remarkable progress, each of the known constructions of non-malleable commitments leaves something to be desired.

We propose a new technique that allows us to construct a non-malleable protocol with only a single "slot", and to improve in at least one aspect over each of the previously proposed protocols. Two direct byproducts of our new ideas are a four round non-malleable commitment and a four round non-malleable zero-knowledge argument, the latter matching the round complexity of the best known zero-knowledge argument (without the non-malleability requirement). The protocols are based on the existence of one-way functions and admit very efficient instantiations via standard homomorphic commitments and sigma protocols.

Our analysis relies on algebraic reasoning, and makes use of error correcting codes in order to ensure that committers' tags differ in many coordinates. One way of viewing our construction is as a method for combining many atomic sub-protocols in a way that simultaneously amplifies soundness and non-malleability, thus requiring much weaker guarantees to begin with, and resulting in a protocol which is much trimmer in complexity compared to the existing ones.

Joint work with Vipul Goyal, Silas Richelson and Margarita Vald

Biography:

Alon Rosen is an associate professor in the School of Computer Science at the Herzliya Interdisciplinary Center. Before that he spent two years as a postdoc in the Cryptography Group of MIT's Computer Science and AI Lab, and two years as a postdoc in the Center for Research on Computation and Society at Harvard's department of Electrical Engineering and Computer Science. He has a Ph.D. in Computer Science from the Weizmann Institute of Science, and B.Sc. in Computer Science and Mathematics from the Hebrew University. Alon's primary fields of interest are Cryptography and Computational Complexity.

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