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

Compressing Communication in Distributed Protocols

By
Mr. Ilan Komargodski
Weizmann Institute

September 23, 2015, Wednesday
11:00 am – 12:00 noon
Room 121, 1/F, Ho Sin Hang Engineering Building, CUHK

Abstract:
We show how to compress communication in distributed protocols in which parties do not have private inputs. More specifically, we present a generic method for converting any protocol in which parties do not have private inputs, into another protocol where each message is "short" while preserving the same number of rounds, the same communication pattern, the same output distribution, and the same resilience to error. Assuming that the output lies in some universe of size M, in our resulting protocol each message consists of only polylog(M,n,d) many bits, where n is the number of parties and d is the number of rounds. Our transformation works in the full information model, in the presence of either static or adaptive Byzantine faults.

In particular, our result implies that for any such poly(n)-round distributed protocol which generates outputs in a universe of size poly(n), long messages are not needed, and messages of length polylog(n) suffice. In other words, in this regime, any distributed task that can be solved in the LOCAL model, can also be solved in the CONGEST model with the same round complexity and security guarantees.

As a corollary, we conclude that for any poly(n)-round collective coin-flipping protocol, leader election protocol, or selection protocols, messages of length polylog(n) suffice (in the presence of either static or adaptive Byzantine faults).

The talk is based on joint work with Yael Tauman Kalai.

Biography:
Ilan Komargodski is a Ph.D student at the Weizmann Institute working with Moni Naor. Ilan completed his Master degree at the Weizmann Institute under the guidance of Ran Raz.

Ilan is interested in various areas of foundations of theoretical computer science including complexity theory and cryptography.

Most recently, Ilan has been working in the exciting field of program obfuscation.

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

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