CFEM workshop:
Theory and Practice of Secure Multiparty Computation
May 5 to 9, 2014
Aarhus University, Denmark

Speaker: Yuval Ishai, Technion

Title: Circuits Resilient to Additive Attacks with Applications to Secure Computation

We study the question of protecting arithmetic circuits against additive attacks that can add an arbitrary fixed value to each wire in the circuit. We show how to transform an arithmetic circuit C into a functionally equivalent, randomized circuit C' of comparable size, such that the effect of any additive attack on the wires of C' can be simulated (up to a small statistical distance) by an additive attack on just the inputs and outputs of C.

Our study of this question is motivated by the goal of simplifying and improving protocols for secure multiparty computation (MPC). It is typically the case that securing MPC protocols against active adversaries is much more difficult than securing them against passive adversaries. We observe that in simple MPC protocols that were designed to protect circuit evaluation only against passive adversaries, the effect of any active adversary corresponds precisely to an additive attack on the circuit's wires. Thus, to securely evaluate a circuit C in the presence of active adversaries, it suffices to apply the passive-case protocol to a corresponding circuit C' which is secure against additive attacks. We use this methodology to simplify feasibility results and obtain efficiency improvements in several standard MPC models.

Joint work with Daniel Genkin, Manoj Prabhakaran, Amit Sahai, and Eran Tromer.