CFEM workshop: Theory and Practice of Multiparty Computation
4 to 8 June, 2012
Aarhus University, Denmark

Speaker: Eyal Kushilevitz, Technion

Title: On the Power of Correlated Randomness in Secure Computation

We investigate the extent to which correlated secret randomness can help in secure two-party computation and multiparty computation with no honest majority. It is known that correlated randomness can be used to evaluate any circuit of size s with perfect security against semi-honest parties or statistical security against malicious parties, where the communication complexity grows linearly with s. This leaves open two natural questions:

(1) Is it possible to obtain *perfect* security against malicious parties?

(2) Can the communication complexity be made independent of the circuit size?

We present both positive and negative results on unconditionally secure computation with correlated randomness, essentially settling the above questions.

Joint work with Yuval Ishai, Sigurd Meldgaard, Claudio Orlandi and Anat Paskin-Cherniavsky.