CFEM & CTIC workshop:
Theory and Practice of Secure Multiparty Computation
May 30 to June 3, 2016
Aarhus University, Denmark

Title: Efficient Constant-Round Multiparty Computation

Yehuda Lindell, Bar Ilan University, Israel

Over the last decade, the efficiency of secure \emph{two-party} computation has advanced in leaps and bounds, with speedups of some orders of magnitude, making it fast enough to be of use in practice. In contrast, progress on the case of multiparty computation (with more than two parties) has been much slower, with very little work being done. In this talk, we discuss recent results for the setting of multiparty computation, both for semi-honest and malicious adversaries. Our results are based on making the constant-round BMR protocol (Beaver et al., STOC 1990), concretely efficient. We present protocol improvements as well as experimental results, some of which are very surprising.