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

Speaker: Tal Rabin, IBM Research

Title: Perfectly-Secure Multiplication for Any $t < n/3$

In the setting of secure multiparty computation, a set of n parties with private inputs wish to jointly compute some functionality of their inputs. One of the most fundamental results of informationtheoretically secure computation was presented by Ben-Or, Goldwasser and Wigderson (BGW) in 1988. They demonstrated that any n-party functionality can be computed with *perfect security*, in the private channels model. The most technically challenging part of this result is a protocol for multiplying two shared values, with perfect security in the presence of up to $t < n/3$ malicious adversaries. In this paper we provide a full specification of the BGW perfect multiplication protocol and prove its security. This includes one new step for the perfect multiplication protocol in the case of $n/4 \leq t < n/3$. As in the original BGW protocol, this protocol works whenever the parties hold univariate (Shamir) shares of the input values. In addition, we present a new multiplication protocol that utilizes *bivariate* secret sharing in order to achieve higher efficiency while maintaining a round complexity that is constant per multiplication. Both of our protocols are presented with full proofs of security.