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

Speaker: Serge Oliver Fehr, CWI Amsterdam

Title: Near-Linear Unconditionally-Secure Multiparty Computation with a Dishonest Minority

In this presentation, I will show two new tricks that are useful for MPC with unconditional security against t out of n=2*t+1 corrupt players: one is a new batch multiplication-verification scheme, and the other is a mini MPC for securely computing authentication tags. In combination with known techniques, these new techniques lead to a MPC scheme with unconditional security against t out of n=2*t+1 corrupt players, with amortized communication complexity of O(n*log(n)+k) bits per multiplication gate (for binary circuits), where k is the security parameter. This improves over the previously best known scheme which required an amortized O(n^2*k) bits of communication per multiplication gate.

This is joint work with Eli Ben-Sasson and Rafail Ostrovsky.