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

Speaker: Serge Fehr, CWI Amsterdam

Title: Reconstructing a shared secret in the presence of faulty shares - a survey

I consider the problem of reconstructing a shared secret in the presence of faulty shares, with unconditional security. We require that any t shares give no information on the shared secret, and reconstruction is possible even if up to t out of the n shares are incorrect. The interesting setting is n/3 <= t < n/2, where reconstruction of a shared secret in the presence of faulty shares is possible, but only with an increase in the share size, and only if one admits a small failure probability.

In this talk, I give an overview over the different known solutions. The first one, which is due to Rabin and Ben-Or (1989), suffers from relatively large shares of size Omega(k*n), where k is the security parameter. The second one, due to Cramer, Damgard and Fehr (2001), has close to optimal share size O(k + n) but is computationally inefficient. Finally, I will present a more recent solution by Cevallos, Fehr, Ostrovsky and Rabani (2012) that combines the advantages of the two: it has short shares of size O(k + n log(n)) and runs in polynomial time.

Whether the linear dependency of the share size on n is necessary remains an open question.