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

Speaker: Martin Hirt, ETH

Title: On the Intrinsic Complexity of Broadcast

We consider a setting with n parties, any number of them being corrupted (i.e., $t<n$). The parties are connected by secure pairwise channels. Furthermore, a restricted broadcast primitive is available, which is limited in the number of bits it can broadcast overall.

How many bits of broadcast are needed through this broadcast primitive (in addition to the communication over the bilateral channels) in order to broadcast an l-bit message?

We show that for $n=3$ parties, broadcasting one 1.6-bit message through the broadcast primitive is necessary and sufficient to broadcast an arbitrary long message, with perfect security.

Furthermore, for $n>3$ parties, broadcasting in total $8n log n$ bits through the primitive is sufficient for broadcasting an arbitrary long message, whereas $n-3$ bits are not sufficient.

This is joint work with Ueli Maurer and Pavel Raykov.