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

Title: Compact Adversary Structures

Martin Hirt, ETH Zurich, Switzerland

MPC protocols in the literature either cope with threshold adversaries and are reasonably efficient, or cope with general adversaries and are unreasonably inefficient. This inefficiency of general-adversary protocols is no coincidence, as the size of an adversary structure is typically exponential in the number of parties.

In this talk, we ask the question whether there are "natural" general adversaries that allow for efficient MPC protocols. We present a (rather naive) description language of general adversaries and construct MPC protocols which are polynomial in the size of the description of the general adversary. It is an open problem to come up with more expressive languages to characterize general adversaries which both are natural and allow for efficient protocols