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

Title: On the Computational Overhead of MPC with Dishonest Majority

Author: Samuel Ranellucci, Aarhus University, Denmark

We consider the situation where a large number n of players want to securely compute a large function f with security against an adaptive, malicious adversary which might corrupt $t < c n$ of the parties for some given $c \in [0,1)$. In other words, only some arbitrarily small constant fraction of the parties are assumed to be honest. For any fixed c, we consider the asymptotic complexity as n and the size of f grows.

We are in particular interested in the computational overhead, defined as the total computational complexity of all parties divided by the size of f.

We show that it is possible to achieve poly-logarithmic computational overhead for all $c < 1$.

Prior to our result it was only known how to get poly-logarithmic overhead for $c < \frac12$. We therefore significantly extend the area where we can do secure multiparty computation with poly-logarithmic overhead. Since we allow that more than half the parties are corrupted, we can only get security with abort, i.e., the adversary might make the protocol abort before all parties learn their outputs.

We can, however, for all c make a protocol for which there exists $d > 0$ such that if at most $d n$ parties are actually corrupted in a given execution, then the protocol will not abort. Our result is solely of theoretical interest. It has not practical implications whatsoever.