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

Title: TinyTable - 2-party secure computation made simple

Author: Ivan Damgård, Aarhus University

We present an extremely simple 2-party secure computation protocol in the preprocessing model. It computes a Boolean circuit with malicious security while communicating only 1 bit in either direction for each AND-gate, whereas linear gates are communication-free. The cost of the precomputation is essentially the same as that of the TinyOT protocol [Nielsen et al., Crypto 2011]. TinyTable adapts easily to the case where the non-linear parts of the target function take only small inputs, as is the case for the S-boxes of AES. A variant of TinyTable specially crafted for AES was implemented and on a fast Amazon cloud set-up, it executes with a latency of about 1 ms, and has amortized cost about 0.5 microseconds per AES block.