CFEM workshop: Theory and Practice of Multiparty Computation
4 to 8 June, 2012
Aarhus University, Denmark

Speaker: Marcel Keller, University of Bristol

Title: AES in MPC on FHE is 10^5 faster than AES in FHE

We describe an implementation of the protocol of Damgård, Pastro, Smart and Zakarias (SPDZ/Speedz) for multi-party computation in the presence of a dishonest majority of active adversaries. We present a number of modifications to the protocol; the first reduces the security to covert security, but produces significant performance enhancements; the second enables us to perform bit-wise operations in characteristic two fields.

As a benchmark application we present the evaluation of the AES cipher, a now standard benchmarking example for multi-party computation. We need examine two different implementation techniques, which are distinct from prior MPC work in this area due to the use of MACs within the SPDZ protocol. Furthermore, we examine two implementation choices for the finite fields; one based on finite fields of size 2^8 and one based on embedding the AES field into a larger finite field of size 2^40.

Our implementation allows us to encrypt up to 4 AES blocks per second with active security and up to 7 blocks with covert security, both excluding the so-called offline phase.

This is joint work with Ivan Damgård, Enrique Larraia, Christian Miles, and Nigel Smart.