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

Speaker: Janus Dam Nielsen, the Alexandra Institute

Title: An introduction to FRESCO - Framework for Realizing Efficient Secure Computations

A number of frameworks and languages have been designed and implemented for secure multiparty computation. However, it is still an open question how to structure secure computation in the most efficient manner. We give another solution to the problem by introducing FRESCO - a Framework for Realizing Efficient Secure Computations. The design of FRESCO is based on lessons learned from implementing and using multiple runtimes like SCET, SMCR, VIFF, and FairPlay.

FRESCO is in particular designed to reduce excessive memory usage for large circuits, while still utilizing the network to its full capacity (one of the key benefits of VIFF). This is achieved by implicitly representing the structure of the circuit as code and introducing rounds of evaluation. A fixed number of gates are made explicit and evaluated in parallel in a round. A gate is only allowed to send and receive once over the network. The structure of evaluation relieves the programmer from handling scheduling of gate evaluation explicitly. Another benefit from this setup is a plug-able architecture for evaluation strategies, which allows us to test multiple different evaluation strategies without reimplementing the different MPC protocols. We have used this for investigations into different strategies for pushing data through the network.

As for previous framework FRESCO allows us to experiment with and compare different MPC protocols in a fair environment. We have implemented a number of protocols using FRESCO and the timing results looks promising and confirms that we are moving in the right direction.

This is joint work with the Cryptography and Security group at the University of Aarhus.