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

Title: Efficient OT Extension and its Impact on Secure Computation

Michael Zohner, TU Darmstadt, Germany

Secure two-party computation allows two mutually distrusting parties to jointly evaluate a function on their private inputs while maintaining the privacy of their inputs. A fundamental primitive for secure computation is oblivious transfer (OT), where a sender offers two messages of which a receiver is allowed to obtain only one message without the sender learning which message was chosen and without the receiver learning any information about the other message. Recently, OT extension protocols, which are used to arbitrarily extend few costly OTs, have been subject to drastic computational improvements. Communication improvements, on the other hand, have been more scarce, making the time for transferring data the main bottleneck in current OT extension protocols.

In this talk, we present ideas on how to work around this communication boundary to improve the efficiency of secure computation protocols in the semi-honest model. We first describe a mixed-protocol framework called ABY and outline how to achieve better complexity by mixing Boolean and Arithmetic function representations. We then show how to efficiently abstract from the traditional Boolean representation to more complex functions, which enables us to reduce the communication complexity of various secure computation functionalities.