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

Title: What Security Can We Achieve In Less Than 4-Rounds?

Author: Carmit Hazay, Bar Ilan University, Israel

Katz and Ostrovsky (Crypto 2004) proved that five rounds are necessary for stand-alone general black-box constructions of secure two-party protocols and at least four rounds are necessary if only one party needs to receive the output. Recently, Ostrovsky, Richelson and Scafuro (Crypto 2015) proved optimality of this result by showing how to realize arbitrary functionalities in four rounds where only one party receives the output via a black-box construction (and an extension to five rounds where both parties receive the output). In this paper we study the question of what security is achievable for stand-alone two-party computation in less than four rounds when only one party is required to learn the output.

We provide a three-round secure two-party protocol for general functionalities where only one party receives the output, that achieves 1/p-simulation security (i.e. simulation fails with probability at most 1/p+negl) against a malicious corruption of the party not receiving the output, while simultaneously guaranteeing a meaningful notion of privacy against a malicious corruption of either party. We first show how to realize coin-tossing and oblivious-transfer functionalities with similar guarantees and then show how to extend these protocols to realize general functionalities. As an intermediate step, we develop protocols that achieve strong security against so-called non-aborting adversaries that might be of independent interest when considering covert security.

Finally, we show that the simulation-based security guarantees for our three-round protocols are optimal by proving that 1/p-simulation security is impossible to achieve against both parties in three rounds or less when requiring some minimal guarantees on the privacy of their inputs.

This is a joint work with Muthuramakrishnan Venkitasubramaniam.