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

Title: Fast Garbling of Circuits under Standard Assumptions

Author: Ariel Nof, Bar Ilan University, Israel

Protocols for secure computation enable mutually distrustful parties to jointly compute on their private inputs without revealing anything but the result. Over recent years, secure computation has become practical and considerable effort has been made to make it more and more efficient. A highly important tool in the design of two-party protocols is Yao's garbled circuit construction (Yao 1986), and multiple optimizations on this primitive have led to performance improvements of orders of magnitude over the last years.

However, many of these improvements come at the price of making very strong assumptions on the underlying cryptographic primitives being used (e.g., that AES is secure for related keys, that it is circular secure, and even that it behaves like a random permutation when keyed with a public fixed key). The justification behind making these strong assumptions has been that otherwise it is not possible to achieve fast garbling and thus fast secure computation. In this paper, we take a step back and examine whether it is really the case that such strong assumptions are needed.

We provide new methods for garbling that are secure solely under the assumption that the primitive used (e.g., AES) is a pseudorandom function. Our results show that in many cases, the penalty incurred is not significant, and so a more conservative approach to the assumptions being used can be adopted.