ABSTRACT

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

Speaker: Ivan Bjerre Damgård, Aarhus University

Title: Multiparty Computation in the preprocessing model

Abstract: Multiparty Computation secure against a dishonest majority is not possible without using public-key machinery which is typically quite expensive. Recently, Bendlin et.al. showed that most of the hard work can be pushed into a preprocessing phase, such that the actual computation, the "on-line phase" - only requires cheap information theoretically secure primitives. We describe recent work where we construct on-line phase protocols for any number of players that are essentially optimal w.r.t. the amount of data one needs to get from the preprocessing, and w.r.t. the computational work needed. We also show how the preprocessing can be efficiently implemented based on somewhat homomorphic encryption.

Joint work with Valerio Pastro, Nigel Smart and Sarah Zakarias