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

Speaker: Benny Pinkas, Bar Ilan University and Google

# Title: Secure Computation on the Web: Computing without Simultaneous Interaction

Secure computation enables mutually suspicious parties to compute a joint function of their private inputs while providing strong security guarantees. However, its use in practice seems limited. We argue that one of the reasons for this is that the model of computation on the web is not suited to the type of communication patterns needed for secure computation. Specifically, in most web scenarios clients independently connect to servers, interact with them and then leave. This rules out the use of secure computation protocols that require that all participants interact simultaneously.

We initiate a study of secure computation in a client-server model where each client connects to the server once and interacts with it, without any other client necessarily being connected at the same time. We point out some inherent limitations in this model and present definitions that capture what can be done. We also present a general feasibility result and several truly practical protocols for a number of functions of interest. All our protocols are based on standard assumptions, and we achieve security both in the semi-honest and malicious adversary models.

Joint work with by Shai Halevi and Yehuda Lindell.