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

Title: Function Secret Sharing, Part II: Succinct Secure Computation from DDH

Elette Boyle, IDC Hertzliya, Israel

The second part of the talk describes a recent construction of 2-party FSS schemes for branching programs (alternatively, log-space functions or NC1 functions) from DDH.

We demonstrate applications of this construction to low-communication secure computation based on DDH. In particular, we obtain secure two-party protocols for NC1 functions in which the communication complexity is linear in the input and output size, protocols for general circuits in which the communication complexity is slightly sublinear in the circuit size, and low-communication 2-server PIR protocols supporting general NC1 searches. Our results provide alternatives to fully homomorphic encryption in several application scenarios.

Joint work with Niv Gilboa and Yuval Ishai