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

Title: Composable Adaptive Secure Protocols without Setup under Polytime Assumptions

Author: Muthuramakrishnan Venkitasubramaniam, University of Rochester, USA

All previous constructions of general multiparty computation protocols that are secure against adaptive corruptions in the concurrent setting either require some form of setup or non-standard assumptions. In this paper we provide the first general construction of secure multi-party computation protocol without any setup that guarantees composable security in the presence of anadaptive adversary based on standard polynomial-time assumptions. We prove security un- der the notion of “UC with super-polynomial helpers” introduced by Canetti Lin and Pass (FOCS 2010), which is closed under universal composition and implies “superpolynomial-time simulation”. Moreover, our construction relies on the underlying cryptographic primitives in a black-box manner.
Joint work with Carmit Hazay.