Speaker: Muthuramakrishnan Venkitasubramaniam, University of Rochester

Title: Adaptive MPC from New Notions of Non-Malleability

We present a unified approach for obtaining general secure computation that achieves adaptive-Universally Composable (UC)-security. Conceptually, our approach can be viewed as an adaptive analogue to the recent work of Lin, Pass and Venkitasubramaniam [STOC '09], who considered only static (i.e. non-adaptive) adversaries. Their main insight was that the non-malleability requirement could be decoupled from the simulation requirement to achieve UC-security. A main conceptual contribution of this work is, quite surprisingly, that it is still the case even when considering adaptive security. Using our approach we essentially obtain all previous results on adaptive concurrent secure computation, both in relaxed models (e.g., quasi-polynomial time simulation), as well as trusted setup models (e.g., the CRS model, the imperfect CRS model). As a corollary we also obtain the first adaptively secure multiparty computation protocol in the plain model that is secure under bounded-concurrency.

A key element in our construction is a commitment scheme that satisfies a strong definition of non-malleability. Our new primitive of concurrent equivocal non-malleable commitments, intuitively, guarantees that even when a man-in-the-middle adversary observes concurrent equivocal commitments and decommitments, the binding property of the commitments continues to hold for commitments made by the adversary. This definition is stronger than previous ones, and may be of independent interest. Previous constructions that satisfy our definition have been constructed in setup models, but either re- quire existence of stronger encryption schemes such as CCA-secure encryption or require independent "trapdoors" provided by the setup for every pair of parties to ensure non-malleability. A main technical contribution of this work is to provide a construction that eliminates these requirements and requires only a single trapdoor..