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

Speaker: Jonathan Katz, Maryland University

Title: Recent results on game theory and secure computation

We survey some recent results at the intersection of game theory and secure computation. First, we consider the problem of fair computation where all parties are assumed to be rational. We show that fair computation in this setting is possible (for arbitrary functions and utilities) as long as the parties have a strict incentive to compute the function in an ideal-world formulation of the game.

Next, we turn to the classical problem of Byzantine agreement, where the corrupted parties are assumed to have some preference on the outcomes of the honest players. Both of these settings provide new examples of where game theory can be used to circumvent impossibility results in cryptography.