ABSTRACT

CFEM workshop:
Theory and Practice of Secure Multiparty Computation
May 5 to 9, 2014
Aarhus University, Denmark

Speaker: Melissa Chase, Microsoft

Title: Size-Hiding Secure Computation: Revisiting the Ideal Model

We consider secure two party computation with malicious adversaries in the setting where the size of one party's input is private. Our goal is to construct schemes for general functionalities that are secure under standard assumptions. We begin by showing that under previous definitions, size hiding computation (against malicious adversaries) implies a form of "proof of work", thus it seems impossible to construct from standard assumptions. We then revisit the traditional definition of secure computation in terms of real and ideal world games, and present a new ideal model which captures most of the spirit and advantages of the original. Finally, we give a proof of concept construction showing that under this new definition size hiding secure computation is indeed achievable under standard assumptions.

Joint work with Rafail Ostrovsky and Ivan Visconti.