ABSTRACT

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

Speaker: Tal Malkin, Columbia University

Title: Multi-Party Computation for Polynomials and Branching Programs without Simultaneous Interaction

Halevi, Lindell, and Pinkas recently proposed a model for secure computation that captures communication patterns that arise in many practical settings, such as secure computation on the web. In their model, each party interacts only once, with a single centralized server. Parties do not interact with each other; in fact, the parties need not even be online simultaneously.

In this work we present a suite of new, simple and efficient protocols for secure computation in this ``one-pass" model. We give protocols that obtain optimal privacy for the following general tasks:

(1) Evaluating any multivariate polynomial $F(x_1, \ldots, x_n)$ (modulo a large RSA modulus N), where the parties each hold an input x_i.

(2) Evaluating any branching program over the parties' inputs, where each input is read once in the program.

As a special case, these function classes include all previous functions for which an optimally private, one-pass computation was known, as well as many new functions, including variance and other statistical functions, string matching, classification algorithms and some classes of finite automata and decision trees.

Joint work with Dov Gordon, Mike Rosulek, and Hoeteck Wee