Completeness in Two Party Computation Revisited

Moni Naor
Department of Computer Science & Applied Mathematics
Weizmann Institute of Science
Rehovot 76100
ISRAEL

Abstract

A Secure Function Evaluation (SFE) of a two-variable function f is a protocol that allows two parties with inputs x and y to evaluate $f(x, y)$ in a manner where neither party learns "more than is necessary". A rich body of work deals with the study of completeness for secure two-party computation. A function f is complete for SFE if a protocol for securely evaluating f allows the secure evaluation of all (efficiently computable) functions. The questions investigated are which functions are complete for SFE, Which functions have "trivial" SFE and whether there are functions that are neither complete nor trivial.

The previous study of these questions was mainly conducted from an Information Theoretic point of view and provided strong answers in the form of combinatorial properties. However, we show that there are major differences between the information theoretic and computational settings. In particular, we show functions that are considered trivial by the combinatorial criteria but are actually complete in the computational setting.

We initiate the fully computational study of these fundamental questions. Somewhat surprisingly, we manage to provide an almost full characterization of the complete functions in this model as well. More precisely, we present a computational criterion (called computational row non-transitivity) for a function f to be complete for the

asymmetric case. Furthermore, if f "disobeys" the new criterion, then f has a simple SFE (based on no additional assumptions).

Joint work with Danny Harnik, Omer Reingold and Alon Rosen.