Recent Advances in Secure Multi-Party Computation

Benny Pinkas

Department of Computer Science

Bar-Ilan University
Israel

Abstract:

Secure multi-party computation enables a set of untrusting parties to jointly compute functions of their private inputs, while revealing no other information about them. Secure computation is relevant for many applications. For example, it enables to compute the outcomes of auctions while hiding the private bids.

Secure multi-party computation is a fast-moving research topic with considerable improvements being presented every year (and even less), with the result that secure computation is now practical for a number of important tasks. We will describe latest progress and results, and present some of the main techniques.