Highly Efficient Secure Two-Party Computation - the Road from Theory to Practice

Yehuda Lindell, Bar Ilan University

Abstract

Secure multiparty computation has a rich theory and has been studied on a foundational level from the mid 1980s until today. This theory has yielded impressive results, and we have a deep understanding of the feasibility of secure computation today. Over the past five years, interest has grown rapidly in the application of the theory of secure computation to practice via designing efficient protocols and implementing them. In this talk, I will give a short survey of the current state-of-the-art of secure two-party computation and what real-world applications can already be solved. I will then present a new protocol for secure two-party computation in the presence of malicious adversaries based on Yao's garbled circuits that is significantly faster than all previous protocols.