FairPlay – A Secure Two-Party Computation System

Dahlia Malkhi

The Hebrew University of Jerusalem and Microsoft Research

Abstract

Advances in modern cryptography coupled with rapid growth in processing and communication speeds make secure two-party computation a realistic paradigm. Yet, thus far, interest in this paradigm has remained mostly theoretical.

The talk introduces and demonstrates Fairplay, a full-fledged system that implements generic secure function evaluation (SFE). Fairplay comprises of a high level procedural definition language called SFDL tailored to the SFE paradigm; a compiler of SFDL into a one-pass Boolean circuit presented in a language called SHDL; and Bob/Alice programs that evaluate the SHDL circuit in the manner suggested by Yao in 1986.

This system enables us to present the first evaluation of an overall SFE in real settings, as well as examining its components and identifying potential bottlenecks. It provides a test-bed of ideas and enhancements concerning SFE, whether by replacing parts of it, or by integrating with it. We exemplify its utility by examining several alternative implementations of oblivious transfer within the system, and reporting on their effect on overall performance.

The Fairplay system and the Usenix Security 2004 paper can be downloaded from `http://www.cs.huji.ac.il/labs/danss/Fairplay/`

Fairplay is a joint work with Noam Nisan, Benny Pinkas and Yaron Sella.