Cryptology ePrint Archive: Report 2011/157

Secure Computation on the Web: Computing without Simultaneous Interaction

Shai Halevi and Yehuda Lindell and Benny Pinkas

Abstract: Secure computation enables mutually suspicious parties to compute a joint function of their private inputs while providing strong security guarantees. Amongst other things, even if some of the participants are corrupted the output is still correctly computed, and parties do not learn anything about each other's inputs except for that output. Despite the power and generality of secure computation, its use in practice seems limited. We argue that one of the reasons for this is that the model of computation on the web is not suited to the type of communication patterns needed for secure computation. Specifically, in most web scenarios clients independently connect to servers, interact with them and then leave. This rules out the use of secure computation protocols that require that \emph{all} participants interact simultaneously.

In this paper, we initiate the study of secure computation in a client-server model where each client connects to the server \emph {once} and interacts with it, without any other client necessarily being connected at the same time. We point out some inherent limitations in this model and present definitions that capture what can be done. We also present a general feasibility result and several truly practical protocols for a number of functions of interest. All our protocols are based on standard assumptions, and we achieve security both in the semi-honest and malicious adversary models.

Category / Keywords: cryptographic protocols / SFE, Web-based computing

Date: received 29 Mar 2011, last revised 26 Apr 2011

Contact author: shaih at alum mit edu