Cryptology ePrint Archive: Report 2011/257

Secure Multi-Party Computation of Boolean Circuits with Applications to Privacy in On-Line Marketplaces

Seung Geol Choi and Kyung-Wook Hwang and Jonathan Katz and Tal Malkin and Dan Rubenstein

Abstract: Protocols for generic secure multi-party computation (MPC) come in two forms: they either represent the function being computed as a boolean circuit, or as an arithmetic circuit over a large field. Either type of protocol can be used for any function, but the choice of which type of protocol to use can have a significant impact on efficiency. The magnitude of the effect, however, has never been quantified.

With this in mind, we implement the MPC protocol of Goldreich, Micali, and Wigderson, which uses a boolean representation and is secure against a semi-honest adversary corrupting any number of parties. We then consider applications of secure MPC in on-line marketplaces, where customers select resources advertised by providers and it is desired to ensure privacy to the extent possible. Problems here are more naturally formulated in terms of boolean circuits, and we study the performance of our MPC implementation relative to existing ones that use an arithmetic-circuit representation. Our protocol easily handles tens of customers/providers and thousands of resources, and outperforms existing implementations including FairplayMP, VIFF, and SEPIA.

Category / Keywords: implementation /

Date: received 24 May 2011

Contact author: jkatz at cs umd edu