Cryptology ePrint Archive: Report 2013/079

Fast Cut-and-Choose Based Protocols for Malicious and Covert Adversaries

Yehuda Lindell

Abstract: In the setting of secure two-party computation, two parties wish to securely compute a joint function of their private inputs, while revealing only the output. One of the primary techniques for achieving efficient secure two-party computation is that of Yao's garbled circuits (FOCS 1986). In the semi-honest model, where just one garbled circuit is constructed and evaluated, Yao's protocol has proven itself to be very efficient. However, a malicious adversary who constructs the garbled circuit may construct a garbling of a different circuit computing a different function, and this cannot be detected (due to the garbling). In order to solve this problem, many circuits are sent and some of them are opened to check that they are correct while the others are evaluated. This methodology, called \emph{cut-and-choose}, introduces significant overhead, both in computation and in communication, and is mainly due to the number of circuits that must be used in order to prevent cheating.

In this paper, we present a cut-and-choose protocol for secure computation based on garbled circuits, with security in the presence of malicious adversaries, that vastly improves on all previous protocols of this type. Concretely, for a cheating probability of at most 2^{-40}, the best previous works send between 125 and 128 circuits. In contrast, in our protocol 40 circuits alone suffice (with some additional overhead). Asymptotically, we achieve a cheating probability of 2^{-s} where s is the number of garbled circuits, in contrast to the previous best of $2^{-0.32s}$. We achieve this by introducing a new cut-and-choose methodology with the property that in order to cheat, \emph{all} of the evaluated circuits must be incorrect, and not just the \emph{majority} as in previous works.

Category / Keywords: cryptographic protocols /

Publication Info: An extended abstract appeared at CRYPTO 2013; this is the full version.

Date: received 16 Feb 2013, last revised 29 May 2013

Contact author: lindell at biu ac il