Cryptology ePrint Archive: Report 2013/196

Fast Two-Party Secure Computation with Minimal Assumptions

abhi shelat and Chih-hao Shen

Abstract: All recent implementations of two-party secure computation protocols require specific complexity assumptions for their correctness and/or efficiency (e.g., DDH, homomorphic encryption, Sigma protocols for specific languages). We propose and implement a Yao-based protocol for secure two-party computation against malicious adver- saries that enjoys the following benefits: (1) it assumes the minimal hardness assumption, that is, oblivious transfers; (2) it has constant round complexity; (3) its overhead is O(k) times of the Yao protocol's, which is the best one could hope for by using the circuit-level cut-and-choose technique to achieve malicious security; and (4) it is embarrassingly parallelizable in that its depth complexity is roughly the same as the honest-but-curious Yao protocol. To achieve these properties, we use the cut-and-choose paradigm, but solve the main three problems for achiev- ing malicious security (input consistency, selective failure, and output authentication) in a novel and efficient manner. In particular, we propose an efficient witness-indistinguishable proof for output authentication; we suggest the use of an auxiliary 2-universal circuit to ensure the generator's input consistency; and we advance the performance of the state-of-the-art approach defending the selective failure attack. Not only does our protocol require weaker complexity assumptions, but our implementation of this protocol also demonstrates a several factor improvement over the best prior two-party secure computation protocol which rely on specific number theoretic assumptions.

Category / Keywords: cryptographic protocols /

Date: received 4 Apr 2013, last revised 9 Apr 2013

Contact author: shench at virginia edu