Cryptology ePrint Archive: Report 2011/533

Two-Output Secure Computation with Malicious Adversaries

abhi shelat and Chih-hao Shen

Abstract: We present a method to compile Yao's two-player garbled circuit protocol into one that is secure against malicious adversaries that relies on witness indistinguishability. Our approach can enjoy lower communication and computation overhead than methods based on cut-and-choose and lower overhead than methods based on zero-knowledge proofs (or sigma-protocols). To do so, we develop and analyze new solutions to issues arising with this transformation:

- How to guarantee the generator’s input consistency

- How to support different outputs for each player without adding extra gates to the circuit of the function f being computed

- How the evaluator can retrieve input keys but avoid selective failure attacks

- Challenging 3/5 of the circuits is near optimal for cut-and-choose (and better than challenging 1/2)

Our protocols require the existence of secure-OT and claw-free functions that have a weak malleability property. We discuss an experimental implementation of our protocol to validate our efficiency claims.

Category / Keywords: applications /

Publication Info: full version of our EUROCRYPT'11 paper

Date: received 30 Sep 2011, last revised 30 Sep 2011

Contact author: shench at virginia edu

Available formats: PDF | BibTeX Citation

Note: remove an redundant table and a repeat section

Version: 20111001:045442 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]