Cryptology ePrint Archive: Report 2013/051

Garbled Circuits Checking Garbled Circuits: More Efficient and Secure Two-Party Computation

Payman Mohassel and Ben Riva

Abstract: Applying cut-and-choose techniques to Yao's garbled circuit protocol has been a promising approach for designing efficient Two-Party Computation (2PC) with malicious and covert security, as is evident from various optimizations and software implementations in the recent years. We revisit the security and efficiency properties of this popular approach and propose alternative constructions and definitions that are more suitable for use in practice.

* We design an efficient fully-secure malicious 2PC protocol for two-output functions that only requires $O(t|C|) $ symmetric-key operations (with small constant factors) where $|C|$ is the circuit size and t is a statistical security parameter. This is essentially the {\em optimal} complexity for protocols based on cut-and-choose, resolving a main question left open by the previous work on the subject.

Our protocol utilizes novel techniques for enforcing \emph{garbler's input consistency} and handling \emph{two-output functions} that are more efficient than all prior solutions.

* Motivated by the goal of eliminating the \emph{all-or-nothing} nature of 2PC with covert security (that privacy and correctness are fully compromised if the adversary is not caught in the challenge phase), we propose a new security definition for 2PC that strengthens the guarantees provided by the standard covert model, and offers a smoother security vs. efficiency tradeoff to protocol designers in choosing the \emph{right deterrence factor}. In our new notion, correctness is always guaranteed, privacy is fully guaranteed with probability ($1-\epsilon$), and with probability ϵ (i.e. the event of undetected cheating), privacy is only ``partially compromised" with at most a {\em single bit} of information leaked, in \emph{case of an abort}.

We present two efficient 2PC constructions achieving our new notion. Both protocols are competitive with the previous 2PC based on cut-and-choose. E.g., the price of strengthening a covert 2PC to satisfy our notion (to obtain full correctness and maximum leakage of a single bit), is only $\frac{1}{\epsilon}$ additional garbled circuits.

A distinct feature of the techniques we use in all our constructions is to check consistency of inputs and outputs using new gadgets that are themselves \emph{garbled circuits}, and to verify validity of these gadgets using \emph{multi-stage} cut-and-choose openings. These techniques may be of an independent interest.

Category / Keywords: Secure Two-Party Computation, Cut-and-choose 2PC

Date: received 1 Feb 2013, last revised 3 Feb 2013