Cryptology ePrint Archive: Report 2013/137

How to Hide Circuits in MPC: An Efficient Framework for Private Function Evaluation

Payman Mohassel and Saeed Sadeghian

Abstract: We revisit the problem of general-purpose \emph{private function evaluation} (PFE) wherein a single party P_1 holds a circuit $\C$, while each P_i for $1 \le i \leq n$ holds a private input x_i, and the goal is for a subset (or all) of the parties to learn $\C(x_1, \ldots, x_n)$ but nothing else. We put forth a general framework for designing PFE where the task of hiding the circuit and securely evaluating its gates are addressed independently: First, we reduce the task of hiding the circuit topology to oblivious evaluation of a mapping that encodes the topology of the circuit, which we refer to as \emph{oblivious extended permutation} (OEP) since the mapping is a generalization of the permutation mapping. Second, we design a subprotocol for private evaluation of a single gate (PFE for one gate), which we refer to as \emph{private gate evaluation} (PGE). Finally, we show how to naturally combine the two components to obtain efficient and secure PFE.

We apply our framework to several well-known general-purpose MPC constructions, in each case, obtaining the most efficient PFE construction to date, for the considered setting. Similar to the previous work we only consider semi-honest adversaries in this paper.

\begin{itemize} \item In the \emph{multiparty} case with dishonest majority, we apply our techniques to the seminal GMW protocol~\cite{GMW87} and obtain the first general-purpose PFE with \emph{linear complexity} in the circuit size.

\item In the \emph{two-party} case, we transform Yao's garbled circuit protocol~\cite{yao86} into a constant-round two-party PFE. Depending on the instantiation of the underlying subprotocol, we either obtain a two-party PFE with linear complexity that improves on the only other work with similar asymptotic efficiency (Katz and Malka, ASIACRYPT 2011~\cite{katzpfe}), or a two-party PFE that provides the best concrete efficiency to date despite not being linear.

\item The above two constructions are for boolean circuits. In case of \emph{arithmetic circuits}, we obtain the first PFE with linear complexity based on any additively homomorphic encryption scheme. \end{itemize}

Though each construction uses different techniques, a common feature in all three is that the overhead of hiding the circuit $\C$ is essentially equal to the cost of running the OEP protocol on a vector of size $|\C|$. As a result, to improve efficiency, one can focus on lowering the cost of the underlying OEP protocol. OEP can be instantiated using a singly homomorphic encryption or any general-purpose MPC but we introduce a new construction that we show is significantly more efficient than these alternatives, in practice. The main building block in our OEP construction is an efficient protocol for \emph{oblivious switching network evaluation} (OSN), a generalization of the previously studied oblivious shuffling problem which is of independent interest. Our results noticeably improve efficiency of the previous solutions to oblivious shuffling, yielding a factor of 25 or more gain in computation and communication.

Category / Keywords: secure computation, private function evaluation, oblivious shuffling

Publication Info: Eurocrypt 2013

Date: received 7 Mar 2013, last revised 11 Mar 2013

Contact author: pmohasse at cpsc ucalgary ca

Note: An extended abstract of this paper is to appear in Advances in Cryptology--EUROCRYPT 2013

Version: 20130312:001657 (All versions of this report)