Cryptology ePrint Archive: Report 2013/155

MiniLEGO: Efficient Secure Two-Party Computation From General Assumptions

Tore Kasper Frederiksen and Thomas Pelle Jakobsen and Jesper Buus Nielsen and Peter Sebastian Nordholt and Claudio Orlandi

Abstract: One of the main tools to construct secure two-party computation protocols are Yao garbled circuits. Using the cut-and-choose technique, one can get reasonably efficient Yao-based protocols with security against malicious adversaries. At TCC 2009, Nielsen and Orlandi suggested to apply cut-and-choose at the gate level, while previously cut-and-choose was applied on the circuit as a whole. This appealing idea allows for a speed up with practical significance (in the order of the logarithm of the size of the circuit) and has become known as the ``LEGO'' construction. Unfortunately the construction by Nielsen and Orlandi is based on a specific number-theoretic assumption and requires public-key operations per gate of the circuit.

The main technical contribution of this work is a new XOR-homomorphic commitment scheme based on oblivious transfer, that we use to cope with the problem of connecting the gates in the LEGO construction. Our new protocol has the following advantages: \begin{enumerate}

\item It maintains the efficiency of the LEGO cut-and-choose.

\item After a number of seed oblivious transfers linear in the security parameter, the construction uses only primitives from Minicrypt (i.e., private-key cryptography) per gate in the circuit (hence the name MiniLEGO).

\item On the contrary of original LEGO, MiniLEGO is compatible with all known optimization for Yao garbled gates (row reduction, free-XORs, point-and-permute).

\end{enumerate}

Category / Keywords: cryptographic protocols / Garbled circuits, cut-and-choose, error correcting codes

Publication Info: Extended abstract version has been accepted at EUROCRYPT 2013

Date: received 14 Mar 2013, last revised 18 Mar 2013

Contact author: jot2re at cs au dk

Available formats: PDF | BibTeX Citation

Note: A bug from [BHR12] cascaded into this paper. It is not significant and has now been fixed.

Version: 20130318:102453 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]