# Cryptology ePrint Archive: Report 2013/073

**Zero-Knowledge Using Garbled Circuits: How To Prove Non-Algebraic Statements Efficiently**

*Marek Jawurek and Florian Kerschbaum and Claudio Orlandi*

**Abstract:** Zero-knowledge protocols are one of the fundamental concepts in modern cryptography and have countless applications. However, after more than 30 years from their introduction, there are only very few languages (essentially those with a group structure) for which we can construct zero-knowledge protocols that are efficient enough to be used in practice.

In this paper we address the problem of how to construct efficient zero-knowledge protocols for generic languages and we propose a protocol based on Yao's garbled circuit technique.

The motivation for our work is that in many cryptographic applications it is useful to be able to prove efficiently statements of the form e.g., ``I know x s.t. y=SHA-256(x)'' for a common input y (or other ``unstructured'' languages), but no efficient protocols for this task are currently known.

It is clear that zero-knowledge is a subset of secure two-party computation (i.e., any protocol for generic secure computation can be used to do zero-knowledge). The main contribution of this paper is to construct an efficient protocol for the special case of secure two-party computation where only one party has input (like in the zero-knowledge case).

The protocol achieves active security and is essentially only twice as slow as Yao's garbled circuit protocol. This is a great improvement with respect to the cut-n-choose technique to make Yao's protocol actively secure, where the complexity grows linearly with the security parameter.

**Category / Keywords:** cryptographic protocols / Zero-knowledge, Garbled Circuits, Secure Two-Party Computation, Active Security

**Date:** received 15 Feb 2013, last revised 20 Feb 2013

**Contact author:** orlandi at cs au dk