ABSTRACT

CFEM & CTIC workshop:
Theory and Practice of Secure Multiparty Computation
May 30 to June 3, 2016
Aarhus University, Denmark

Title: Cross&Clean: Amortized Garbled Circuits With Constant Overhead

Authors: Jesper Buus Nielsen; Claudio Orlandi

Garbled circuits (GC) are one of the main tools for secure two-party computation. One of the most promising techniques for efficiently achieving active-security in the context of GCs is the so called cut-and-choose approach, which in the last few years has received many refinements in terms of the number of garbled circuits which need to be constructed, exchanged and evaluated.

In this paper we ask a simple question, namely "how many garbled circuits are needed to achieve active security?" and we propose a novel protocol which achieves active security while using only a constant number of garbled circuits per evaluation in the amortized setting.