Cryptology ePrint Archive: Report 2013/143

An architecture for practical actively secure MPC with dishonest majority

Marcel Keller and Peter Scholl and Nigel P. Smart

Abstract: We present a runtime environment for executing secure programs via a multi-party computation protocol in the preprocessing model. The runtime environment is general and allows arbitrary reactive computations to be performed. A particularly novel aspect is that it automatically determines the minimum number of rounds needed for a computation, and uses this to minimize the overall cost of the computation. Various experiments are reported on, on various non-trivial functionalities. We show how, by utilizing the ability of modern processors to execute multiple threads at a time, one can obtain various tradeoffs between latency and throughput.

Category / Keywords: implementation /

Original Publication (with minor differences): ACM-CCS 2013
DOI: 10.1145/2508859.2516744

Date: received 9 Mar 2013, last revised 4 Oct 2013

Contact author: nigel at cs bris ac uk,m keller@bristol ac uk,Peter Scholl@bristol ac uk