Cryptology ePrint Archive: Report 2013/046

Fast and Maliciously Secure Two-Party Computation Using the GPU

Tore Kasper Frederiksen and Jesper Buus Nielsen

Abstract: We describe, and implement, a maliciously secure protocol for secure two-party computation, based on Yao's garbled circuit and an efficient OT extension, in a parallel computational model. The implementation is done using CUDA and yields the fastest results for maliciously secure two-party computation in a realistic and practical setting by using a simple consumer grade CPU and GPU. Our protocol further introduces some novel constructions in order to combine garbled circuits and an OT extension in a parallel and maliciously secure setting.

Category / Keywords: cryptographic protocols / implementation, two-party computation

Date: received 29 Jan 2013, last revised 15 Feb 2013

Contact author: jot2re at cs au dk