Cryptology ePrint Archive: Report 2011/577

An Efficient Protocol for the Commit-Prove-Fair-Open functionality

Ou Ruan , Cai Fu and Guohua Cui

Abstract: In TCC 2006, Garay et al. introduced the notion of "commit-prove-fair-open" functionality in order to achieve what they called "resource fairness" of secure multi-party computation(MPC) with corrupted majority. The protocol realizing this notion of fairness follows the gradual release approach and, further, it can be proven secure in the simulation paradigm and enjoys composition properties. In this paper, we show a more efficient resource-fair protocol of FCPFO based on a new variant of Garay et al. time-lines and simplified Camenisch-Shoup(sCS) commitment,whose communication and computation complexity are less than 1/5 of Garay et al. construction. In addition, our new protocol allows commitment to value 0, which is not possible in the plain Garay et al. construction.

Category / Keywords: cryptographic protocols / commit-prove-fair-open functionality, resource fairness, time-lines, secure multi-party computation

Date: received 20 Oct 2011

Contact author: ruanou at 21cn com

Available formats: PDF | BibTeX Citation

Version: 20111102:203546 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]