Cryptology ePrint Archive: Report 2013/081

Efficient Secure Two-Party Computation Using Symmetric Cut-and-Choose

Yan Huang and Jonathan Katz and Dave Evans

Abstract: Beginning with the work of Lindell and Pinkas, researchers have proposed several protocols for secure two-party computation based on the cut-and-choose paradigm. In existing instantiations of this paradigm, one party generates κ garbled circuits; some fraction of those are ``checked" by the other party, and the remaining fraction are evaluated.

We introduce here the idea of symmetric cut-and-choose protocols, in which each party generates κ circuits to be checked by the other party. The main advantage of our technique is that the number κ of garbled circuits can be reduced by a factor of 3 while attaining the same statistical security level as in prior work. Since the number of garbled circuits dominates the costs of the protocol, especially as larger circuits are evaluated, our protocol is expected to run up to 3 times faster than existing schemes. Preliminary experiments validate this claim.

Category / Keywords: cryptographic protocols /

Date: received 16 Feb 2013, last revised 20 Feb 2013

Contact author: jkatz at cs umd edu

Available formats: PDF | BibTeX Citation

Note: Minor fix in Section 4.1.

Version: 20130220:140414 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]