Cryptology ePrint Archive: Report 2011/002

A Zero-One Law for Secure Multi-Party Computation with Ternary Outputs (full version)

Gunnar Kreitz

Abstract: There are protocols to privately evaluate any function in the honest-but-curious setting assuming that the honest nodes are in majority. For some specific functions, protocols are known which remain secure even without an honest majority. The seminal work by Chor and Kushilevitz [CK91] gave a complete characterization of Boolean functions, showing that each Boolean function either requires an honest majority, or is such that it can be privately evaluated regardless of the number of colluding nodes.

The problem of discovering the threshold for secure evaluation of more general functions remains an open problem. Towards a resolution, we provide a complete characterization of the security threshold for functions with three different outputs. Surprisingly, the zero-one law for Boolean functions extends to Z_3, meaning that each function with range Z_3 either requires honest majority or tolerates up to n colluding nodes.

Category / Keywords: foundations /

Publication Info: This is the full version of a paper accepted for publication at TCC 2011

Date: received 1 Jan 2011

Contact author: gkreitz at kth se

Available formats: PDF | BibTeX Citation

Version: 20110105:022712 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]