Cryptology ePrint Archive: Report 2011/240

Universal Composability from Essentially Any Trusted Setup

Mike Rosulek

Abstract: It is impossible to securely carry out general multi-party computation in arbitrary network contexts like the Internet, unless protocols have access to some trusted setup. In this work we classify the power of such trusted (2-party) setup functionalities. We show that nearly every setup is either {\bf useless} (ideal access to the setup is equivalent to having no setup at all) or else {\bf complete} (composably secure protocols for {\em all} tasks exist in the presence of the setup). We further argue that those setups which are neither complete nor useless are highly unnatural.

The main technical contribution in this work is an almost-total characterization of completeness for 2-party setups. Our characterization treats setup functionalities as black-boxes, and therefore is the first work to classify completeness of {\em arbitrary setup functionalities} (i.e., randomized, reactive, and having behavior that depends on the global security parameter).

Category / Keywords: foundations / universal composition, multi-party computation

Date: received 14 May 2011

Contact author: mikero at cs umt edu