Universally Composable Computation Without Honest Majority

Ran Canetti
Cryptography Research Group
IBM T.J. Watson Research Center
Hawthorne Building, P.O. Box 704
Yorktown Heights, NY 10598
U.S.A.

Abstract

We show how to securely realize any two-party and multi-party functionality in a *universally composable way, regardless of the number of corrupted participants. That is, we consider an asynchronous multi-party network with open communication and an adversary that can adaptively corrupt as many parties as it wishes. In this setting, our protocols allow any subset of the parties (with pairs of parties being a special case) to securely realize any desired functionality of their local inputs, and be guaranteed that security is preserved regardless of the activity in the rest of the network. This implies that security is preserved under concurrent composition of an unbounded number of protocol executions, as well as non-malleability with respect to arbitrary protocols. Our constructions are in the common reference string model and rely on standard intractability assumptions.*

The construction roughly follows the Goldreich-Micali-Wigderson paradigm, where the basic primitives (OT, ZK, Commitment) are replaced with universally composable counterparts. In fact, Given ideal instantiations of these primitives, the construction becomes unconditionally secure. This feature may be condusive to developing quantum versions of the construction.

Joint work with Yehuda Lindell, Rafi Ostrovsky, and Amit Sahai.