Fair Multi-Party Computation

Juan Garay

Bell Labs - Lucent Technologies

<garay@research.bell-labs.com>

Abstract

We consider the problem of constructing secure multi-party computation (MPC) protocols that are *completely fair* — meaning that either all the parties learn the output of the function, or nobody does — even when a majority of the parties are corrupted. We first propose a framework for fair multi-party computation (FMPC), within which we formulate a definition of secure and fair protocols. The definition follows the standard simulation paradigm, but is modified to allow the protocol to depend on the runing time of the adversary. In this way, we avoid a well-known impossibility result for fair MPC with corrupted majority; in particular, our definition admits constructions that tolerate up to $(n-1)$ corruptions, where n is the total number of parties. Next, we define a "commit-prove-fair-open" functionality and construct an efficient protocol that realizes it, using a new variant of a cryptographic primitive known as "time-lines." With this functionality, we show that some of the existing secure MPC protocols can be easily transformed into fair protocols while preserving their security. Furthermore, these protocols remain secure when arbitrarily composed with any protocols, which means, in particular, that they are concurrently composable and non-malleable.

This is joint work with Phil MacKenzie and Ke Yang.