ABSTRACT

CFEM & CTIC workshop:
Theory and Practice of Secure Multiparty Computation
May 30 to June 3, 2016
Aarhus University, Denmark

Title: Probabilistic Termination and Composability of Cryptographic Protocols

Juan Garay, Yahoo Research, USA

When analyzing the round complexity of multi-party cryptographic protocols, one often overlooks the fact that underlying resources, such as a broadcast channel, can be by themselves expensive to implement. For example, it is well known that it is impossible to implement a broadcast channel by a (deterministic) protocol in a sub-linear (in the number of corrupted parties) number of rounds.

The seminal works of Rabin and Ben-Or from the early 80's demonstrated that limitations as the above can be overcome by using randomization and allowing parties to terminate at different rounds, igniting the study of protocols over point-to-point channels with probabilistic termination and expected *constant* round complexity. However, absent a rigorous simulation-based definition, the suggested protocols are proven secure in a property-based manner or via *ad hoc* simulation-based frameworks, therefore guaranteeing limited, if any, composability.

In this work, we put forth the first simulation-based treatment of multi-party cryptographic protocols with probabilistic termination. We define secure multi-party computation (MPC) with probabilistic termination in the UC framework, and prove a universal composition theorem for probabilistic-termination protocols. Our theorem allows to compile a protocol using deterministic-termination hybrids into a protocol that uses expected constant-round protocols for emulating these hybrids, preserving the expected round complexity of the calling protocol.

We showcase our definitions and compiler by providing simulation-based (therefore composable) protocols and security proofs for the following primitives relying on point-to-point channels: (1) Expected-constant-round perfect Byzantine agreement, (2) expected-constant-round perfect parallel broadcast, and (3) perfectly secure MPC with round complexity independent of the number of parties.

This is joint work with Ran Cohen, Sandro Coretti and Vassilis Zikas.