Robust and Private Cloud

Shlomi Dolev

Department of Computer Science

Ben-Gurion University of the Negev
Beer-Sheva, Israel 84105.

Abstract:

The talk summarizes several recent works on robust self-stabilizing cloud and migration of computation to the cloud, where a dealer wants to delegate a computation to processes in the cloud by sending them stream of inputs. The dealer is able to harvest the result by collecting the states of the processes at any given time, while processes have limited or no information concerning the current state of the computation. In particular the following solutions will be described:

- Reactive secret sharing, that changes the secret according to unbounded sequence of common inputs, where no communication among the (dynamic set of) participants is allowed, a fully secure solution for simple functions but somewhat non perfectly secure solution for any function.

- Dynamic online multiparty computation, in which a dynamic group of participants that should not know the sequence of inputs they process nor the program computed. The solution is based on a secret share based implementation of oblivious Turing machine.

- Infinite execution with no communication among the participants where the input is revealed to all participants. We prove that any automaton can be executed without revealing any information concerning the current state of the automaton. The construction is based on Krohn-Rhodes decomposition technique. Using pseudo random sequence, we present a simpler efficient technique for securing the current state of the automaton.

- String matching in which both the inputs and the state are information theoretically secure.