Concurrent Security and Non-malleability

Rafael Pass

Cornell University

Abstract. The Internet enables concurrent executions of cryptographic protocols. This concurrent setting, however, also brings forth new types of coordinated attacks in which an adversary controls many parties, interleaving the executions of the various protocol instances, and attempts to "maul" messages from one execution to use in another.
In this talk, we will survey some recent methods for achieving concurrent security without relying on any trusted-set up (such as e.g., Common Reference Strings).