ANDRE SCEDROV, University of Pennsylvania
Bounded memory Dolev-Yao adversaries

We investigate how much damage can be done by insiders alone, without collusion with an outside adversary. All the players inside our system, including potential adversaries, have similar capabilities. They have bounded storage capacity. We investigate the complexity of the decision problem of whether or not an adversary is able to discover secret data. We show that this problem is PSPACE-complete. Joint work with M. Kanovich, T. Ban Kirigin, and V. Nigam.