ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 13

13.1 General Adversary Structures

Consider the set of players $P = \{P_1, \ldots, P_n\}$. As seen in the lecture, an adversary structure is a collection $\mathcal{Z} \subseteq 2^P$, that is closed under taking subsets. That is, if $Z \in \mathcal{Z}$ and $Z' \subseteq Z$ then $Z' \in \mathcal{Z}$. An adversary structure $\mathcal{Z}$ is Q^k if no k sets in $\mathcal{Z}$ cover P. The maximal sets of an adversary structure $\mathcal{Z}$ are the elements $Z \in \mathcal{Z}$ such that no $Z' \supset Z$ is in $\mathcal{Z}$.

a) Compute the adversary structure induced by the threshold condition $t < n/3$. What is the number of maximal sets?

b) Show that if there is a protocol π actively secure against an adversary structure that is not Q^3, then there is a protocol π' that is actively secure in the threshold setting for $n = 3$ and $t = 1$.

c) Give a Q^3-adversary structure $\mathcal{Z}$ for $n = 6$ that contains a set of 3 parties.

13.2 Weak Consensus for GA

In the lecture it was mentioned that there are actively secure broadcast protocols against Q^3-adversaries. One can adapt the consensus protocol from the lecture to be secure against general adversaries.

Adjust the protocol for weak consensus from the lecture to be secure against Q^3-adversaries characterized by $\mathcal{Z}$.

13.3 Active Multiplication Protocol

Prove that the active multiplication protocol seen in the lecture is secure. In particular, show that privacy and correctness are satisfied.