ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Solution to Exercise 13

13.1 General Adversary Structures

a) The adversary structure $\mathcal{Z}$ induced by the condition $t < \frac{n}{3}$ is $\{Z \subseteq P : |Z| \leq t\}$. The number of maximal sets is $\binom{n}{t}$.

b) Assume there is a protocol π actively secure against an adversary structure $\mathcal{Z}$ that is not Q^3. This means that there exists $Z_1, Z_2, Z_3 \in \mathcal{Z}$ that are pairwise disjoint and satisfy $Z_1 \cup Z_2 \cup Z_3 = P$.

Now consider protocol π' in the threshold setting with $n = 3$ and $t = 1$, where each party P_i executes the programs of parties in Z_i. Protocol π' is actively secure against one malicious party P_i, because π is actively secure against the parties in Z_i cheating. However, we know that there is no protocol secure against active adversaries for $n = 3$ and $t = 1$.

c) A possible adversary structure would be:

$$\mathcal{Z} = \{\{\}, \{P_1\}, \{P_2\}, \{P_3\}, \{P_1, P_2\}, \{P_2, P_3\}, \{P_1, P_3\}, \{P_1, P_2, P_3\}, \{P_4\}, \{P_5\}, \{P_6\}\}.$$

13.2 Weak Consensus for GA

Consider the following protocol:

Protocol $\mathsf{WeakConsensusGA}(x_1, \ldots, x_n) \rightarrow (y_1, \ldots, y_n)$**:**

1. $\forall P_i$: send x_i to each P_j. Let x_{ij} be the value received by P_j.
2. $\forall P_j$: $y_j = \begin{cases} 0 & \text{if } \{P_i : x_{ij} \neq 0\} \in \mathcal{Z} \\ 1 & \text{if } \{P_i : x_{ij} \neq 1\} \in \mathcal{Z} \\ \bot & \text{otherwise} \end{cases}$
3. $\forall P_j$: return y_j

First observe that the conditions $\{P_i : x_{ij} \neq 0\} \in \mathcal{Z}$ and $\{P_i : x_{ij} \neq 1\} \in \mathcal{Z}$ are mutually exclusive (due to Q^3).

Persistency: If all honest players input the same value x, each honest player can only receive $\overline{x}$ from corrupted players. Since $\mathcal{Z}$ is monotone, $\{P_i : x_{ij} \neq x\} \in \mathcal{Z}$.

Weak Consistency: Assume for the sake of contradiction that two honest players P_i and P_j decide on y_i and $y_j := \overline{y_i}$ respectively. Hence, P_i received $\overline{y_i}$ only from players in $Z_p \in \mathcal{Z}$, and P_i received y_i only from players in $Z_q \in \mathcal{Z}$.

This implies that the players in $Z := \overline{Z_p} \cap \overline{Z_q}$ are dishonest, since those players sent y_i to P_i and $\overline{y_i}$ to P_j. This contradicts Q^3, as $Z \cup Z_p \cup Z_q = P$.

Termination: Obvious.

13.3 Active Multiplication Protocol

PRIVACY: If there is no corrupted party $P_k \in \overline{Z_p} \cap \overline{Z_q}$, then no information on a_p and b_q is leaked (all opened differences are 0). On the other hand, if there is at least a corrupted party $P_k \in \overline{Z_p} \cap \overline{Z_q}$, the adversary already knew a_p and b_q.

CORRECTNESS: First observe that since $\mathcal{Z}$ is Q^3, there is an honest player $P_k \in \overline{Z_p} \cap \overline{Z_q}$ (because $\overline{Z_p} \cap \overline{Z_q} \in \mathcal{Z}$ would imply $Z_p \cup Z_q \cup (\overline{Z_p} \cap \overline{Z_q}) = P$). This P_k computes and shares the correct product $a_p b_q$. Hence, if some malicious party $P_j \in \overline{Z_p} \cap \overline{Z_q}$ shares a incorrect product, an inconsistency is observed (i.e., one of the opened differences is non-zero), and the shares are reconstructed.