5.2 View

During an arbitrary multi-party protocol, a player will chose values on his own, see public broadcast values and receive private values. We define his view of the protocol to consist of all these values. Notice that in order to simulate the view for a player one does not have to simulate the values which the player chooses on his own.

In the following, we will analyze the adversary's view during the generation of a random shared secret. In particular, the goal is to build a simulator *SIM* that succeeds in the following game. Let B be the index set of corrupted players. The corrupted players P_i for $i \in B$ first run the protocol with real players such that the public value of the random shared secret outputs a random value Y. Now we run the protocol again, but instead of communicating with the real players, the players P_i for $i \in B$ communicate with the simulator. This simulator will now produce messages exactly as the real players do, such that the public value of the random shared secret is Y, and further, the adversary controlling players P_i for $i \in B$ cannot distinguish this simulated view from the view resulting from the real players.

When generating a distributed random shared secret, as explained in Section 2.4, the view of a player P_i would be the following:

the sharing polynomials	$f_i(\cdot), f'_i(\cdot)$
the temporary shares	$f_j(i), f'_j(i)$ for $j \in H_0$
the public commitments	C_{jm}, A_{jm} for $j \in H_0, k \in \{0, ..., t-1\}$
answers on a valid complaint against P_l	$(f_l(j), f'_l(j))$ for $j \in \{1, ..., n\}$,

and the content of his random tape. If an adversary corrupts P_i and P_j, then the adversary's view is $\{\text{view of } P_i\} \cup \{\text{view of } P_j\}$.

Definition 1 *Suppose that a set H_0 of players compute a random shared secret on input (q, G) and produce output Y. Let $\tilde{A}$ be an adversary that corrupts up to $t-1$ players. Let $view(\tilde{A}, G, q, Y)$ denote the view of the adversary for this protocol. Let $VIEW(\tilde{A}, G, q, Y)$ be the random variable induced by $view(\tilde{A}, G, q, Y)$*[2].

Lemma 1 *For any probabilistic polynomial time adversary $\tilde{A}$ there exists a probabilistic polynomial time simulator* SIM *that can compute a random variable* $\text{SIM}(G, q, Y)$ *which has the same probability distribution as $VIEW(\tilde{A}, G, q, Y)$.*

Proof of Lemma 1 Assume that $\tilde{A}$ corrupts players P_i for $i \in B = \{1, ..., t-1\}$. Further, let B' be the index set that denotes the player who publishes inconsistent values A_{im}. Then, $view(\tilde{A}, G, q, Y)$, when generating a random shared secret, is as follows, assuming $H_0 = \{P_1, ..., P_n\}$:

1. The content of the random tape of $\tilde{A}$
2. $f_i(\cdot), f'_i(\cdot)$ for $i \in B$

[2] view(.) contains random variables and static values. VIEW(.) can be regarded as the interpretation of view(.) as one large bit string, so it is basically a random variable.