- At any point, Z can communicate with adversary A or access $\mathsf{extract}(chain_i)$ where $chain_i$ is the local state of player i.

- At any point, Z can *corrupt* an honest party j which means that A gets access to its local state and subsequently, A controls party j. (In particular, this means we consider a model with "erasures"; random coin tosses that are no longer stored in the local state of j are not visible to A.)[11]

- At any point, Z can *uncorrupt* a corrupted player j, which means that A no longer controls j and instead player j starts executing $\Pi(1^\kappa)$ with a fresh state $chain_j$. (This is also how we model Z spawning a "new" honest player.) A gets informed of all such uncorrupt messages and is required to deliver all messages previously sent by (currently alive) honest players.[12]