Secrect Sharing Progress

Joan Ngure

August 2019

Report

We have a dealer who wishes to share the secret s with n persons $P_1, \cdots, P_n$. Each person gets a share of the secret and only a subset of authorized persons can unlock the secret. We have a threshold t where only t participants can unlock the secret but t-1 persons learn nothing about the secret. Share is a randomized algorithm where any input m $\in$ M outputs n-tuple of shares $(s_1 \cdots s_n)$. Reconstruct is a deterministic algorithm give t-tuple of shares, outputs a message in M. A correctness requirement is satisfied that the probability that the authorized subset give m is 1.
For any possible secrets m and m$'$ definitions (secret sharing security via identical distributions and secret sharing security with adversaries) requires that shares should look exactly the same.Hence we say that secret sharing t out of n is perfectly secure.
For 2 out of n, our secret m $\in \{0,1\}^n$, we randomly choose a string say $s_1 \in \{0,1\}^n$ then $s_2 = s_1 \oplus m$.