Lecture 08: Shamir Secret Sharing (Security Argument)
Developing Notion of Security I

The Setting

- We shall work over $\mathbb{Z}_p$, where $p$ is a prime number.
- We want to share to $n$ parties and support $t$ reconstruction, where $n \leq p - 1$.
- Let $\mathbb{P}[S = s]$ be the probability that the secret is $s$.
- Recall, that the secret sharing algorithm samples a random polynomial $p[X]$ or degree $\leq (t - 1)$ such that $p[X = 0] = s$.
- The secret shares of parties $\{1, \ldots, n\}$ are defined to be $p[X = 1], \ldots, p[X = n]$.
- For $i \in \{1, \ldots, n\}$, the random variable $S_i$ represents the secret share distribution of the $i$-th party.
Suppose parties $i_1, \ldots, i_k$, where $k < t$, are colluding.

Their respective secrets are $s_{i_1}, \ldots, s_{i_k}$.

We want to say that a secure secret sharing scheme provides no additional information about the secrets.

Mathematically, this is summarized as:

**Definition (Secure Secret-sharing Scheme)**

For all $s \in \mathbb{Z}_p$ we have

$$\mathbb{P}[S = s] = \mathbb{P}[S = s | S_{i_1} = s_{i_1}, S_{i_2} = s_{i_2}, \ldots, S_{i_k} = s_{i_k}]$$
A Clarification

- Suppose we want to share a message \( s \in \{0, 1\} \) among 4 parties such that any two of them can reconstruct it.
- So, we choose \( p = 5 \).
- The probability of the secret is as follows:
  \[
  P [S = 0] = 0.9 \\
  P [S = 1] = 0.1 \\
  P [S = 2] = 0 \\
  P [S = 3] = 0 \\
  P [S = 4] = 0
  \]
- The security of a secret-sharing scheme insists that even after seeing the secret-shares, the conditional distribution of secrets should remain the same.
The outline for the proof of security for Shamir’s Secret Sharing Scheme

- Remember, this is only a proof outline. You will prove the entire result formally in the homework
Consider the following manipulation

\[
\mathbb{P}\left[ S = s \mid S_{i_1} = s_{i_1}, \ldots, S_{i_k} = s_{i_k} \right]
\]

\[
= \frac{\mathbb{P}\left[ S = s, S_{i_1} = s_{i_1}, \ldots, S_{i_k} = s_{i_k} \right]}{\mathbb{P}\left[ S_{i_1} = s_{i_1}, \ldots, S_{i_k} = s_{i_k} \right]}
\]

\[
= \frac{\mathbb{P}\left[ p[X = 0] = s, p[X = i_1] = s_{i_1}, \ldots, p[X = i_k] = s_{i_k} \right]}{\mathbb{P}\left[ p[X = i_1] = s_{i_1}, \ldots, p[X = i_k] = s_{i_k} \right]}
\]

\[
= \mathbb{P}\left[ S = s \right] \cdot \frac{1}{p} \cdot \frac{1}{p} \cdots \frac{1}{p} \underbrace{\cdots}_{k \text{-times}} \frac{1}{p} \cdot \frac{1}{p} \cdots \frac{1}{p} \cdot \frac{1}{p} = \mathbb{P}\left[ S = s \right]
\]
The previous manipulation relied on the following two results

Claim

\[ P[p[X = 0] = s, p[X = i_1] = s_{i_1}, \ldots, p[X = i_k] = s_{i_k}] = P[S = s] \cdot \frac{1}{p^k} \]

\[ P[p[X = i_1] = s_{i_1}, \ldots, p[X = i_k] = s_{i_k}] = \frac{1}{p^k} \]

You will prove this result in the homework.