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 $n \leqslant p - 1$
- 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 $\leqslant (t-1)$ 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

Developing Notion of Security II

- 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

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

Developing Notion of Security III

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

$$\mathbb{P}[S = 0] = 0.9$$
$$\mathbb{P}[S = 1] = 0.1$$
$$\mathbb{P}[S = 2] = 0$$
$$\mathbb{P}[S = 3] = 0$$
$$\mathbb{P}[S = 4] = 0$$

- The security of a secret-sharing scheme insists that even after seeing the secret-shares, the conditional distribution of secrets should remain the same

Developing Notion of Security IV

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

$$
\begin{aligned}
&\mathbb{P}\left[S = s \middle| S_{i_1} = s_{i_1}, \ldots, S_{i_k} = s_{i_k}\right] \\
&= \frac{\mathbb{P}\left[S = s, S_{i_1} = s_{i_1}, \ldots, S_{i_k} = s_{i_k}\right]}{\mathbb{P}\left[S_{i_1} = s_{i_1}, \ldots, S_{i_k} = s_{i_k}\right]} \\
&= \frac{\mathbb{P}\left[p[X = 0] = s, p[X = i_1] = s_{i_1}, \ldots, p[X = i_k] = s_{i_k}\right]}{\mathbb{P}\left[p[X = i_1] = s_{i_1}, \ldots, p[X = i_k] = s_{i_k}\right]} \\
&= \frac{\mathbb{P}\left[S = s\right] \cdot \overbrace{\frac{1}{p} \cdot \frac{1}{p} \ldots \frac{1}{p}}^{k\text{-times}}}{\overbrace{\frac{1}{p} \cdot \frac{1}{p} \ldots \frac{1}{p}}^{k\text{-times}}} = \mathbb{P}\left[S = s\right]
\end{aligned}
$$

Developing Notion of Security VI

The previous manipulation relied on the following two results

Claim

$$\mathbb{P}\left[p[X=0]=s, p[X=i_1]=s_{i_1}, \dots, p[X=i_k]=s_{i_k}\right] = \mathbb{P}[S=s] \cdot \frac{1}{p^k}$$

$$\mathbb{P}\left[p[X=i_1]=s_{i_1}, \dots, p[X=i_k]=s_{i_k}\right] = \frac{1}{p^k}$$

You will prove this result in the homework.