Lecture 06: Secret Sharing Schemes (4)

Aim

- State and Prove the security of Shamir's Secret Sharing Scheme
  - We will begin by recalling the basics of probability
  - We will define security of a secret sharing scheme
  - We will provide the outline of the security proof for Shamir's Secret Sharing Scheme (the full proof will be derived by you in the homework)

Random Variable and Sample Space

- A sample space is a set Ω
- A random variable C over the sample space Ω is a distribution that assigns probability to every element in Ω

For example

- Let $\Omega = \{H, T\}$
- Let C be a random variable over the sample space Ω such that
  - $\mathbb{P}[C = H] = 1/3$, and
  - $\mathbb{P}[C = T] = 2/3$.
- Semantics: We have a coin C. We know that the probability that, when tossed, the outcome is Heads is $1/3$. And, the probability that, when tosses, the outcome is Tails is $2/3$.
- Note: Before tossing the coin, we have probabilities associated with every outcome in the sample space. Once tossed, the outcome is fixed.

Joint Distribution I

- Suppose C_1 is a random variable over the sample space Ω_1
- Suppose C_2 is a random variable over the sample space Ω_2
- There might be correlations between these random variables. So, represent it as a joint variable over the sample space $\Omega_1 \times \Omega_2$

- For example, let $\Omega_1 = \{H, T\}$ and $\Omega_2 = \{H, T\}$
- Let (C_1, C_2) be a joint distribution over $\Omega_1 \times \Omega_2$
  - $\mathbb{P}[C_1 = H, C_2 = H] = 0$
  - $\mathbb{P}[C_1 = H, C_2 = T] = 1/3$
  - $\mathbb{P}[C_1 = T, C_2 = H] = 1/3$
  - $\mathbb{P}[C_1 = T, C_2 = T] = 1/3$

Joint Distribution II

- Note that

$$\mathbb{P}[C_1 = H] = \mathbb{P}[C_1 = H, C_2 = H] + \mathbb{P}[C_1 = H, C_2 = T]$$
$$= 0 + 1/3 = 1/3$$

In general

- Let (A, B) be a joint distribution over the sample space $\Omega_A \times \Omega_B$
- Then, we have:

$$\mathbb{P}[A = a] = \sum_{b \in \Omega_B} \mathbb{P}[A = a, B = b]$$

Joint Distribution III

- Conditional Probability: Suppose we are guaranteed that $C_2 = T$. Conditioned on this event, what is the probability that $C_1 = H$.
- Conditioned on $C_2 = T$, there are two possibilities $(C_1 = H, C_2 = T)$ and $(C_1 = T, C_2 = T)$. The probabilities of these events are $1/3$ and $1/3$, respectively.
- The probability that $C_2 = T$ happens is $1/3 + 1/3 = 2/3$.
- The probability that $(C_1 = H, C_2 = T)$ happens is $1/3$.
- Putting things together: Starting with the total budget of $2/3$, the interesting event happens with probability $1/3$.
- What is the fraction of the interesting probability in the total budget? The answer is $(1/3)\ /\ (2/3) = 1/2$.
- This is the probability of $C_1 = H$ conditioned on $C_2 = T$.
- Conclusion: $\mathbb{P}\left[C_1 = H | C_2 = T\right] = 1/2$

Joint Distribution IV

- In general, the following holds

$$\mathbb{P}\left[A = a \middle| B = b\right] = \frac{\mathbb{P}\left[A = a, B = b\right]}{\mathbb{P}\left[B = b\right]} = \frac{\mathbb{P}\left[A = a, B = b\right]}{\sum_{a \in \Omega_A} \mathbb{P}\left[A = a, B = b\right]}$$

- This is known as the <u>Bayes' Rule</u>

Joint Distribution V

- Chain Rule
- Suppose $(X_1, X_2, \ldots, X_n)$ is a joint distribution over the sample space $\Omega_1 \times \Omega_2 \times \cdots \Omega_n$ item Then the following holds

$$
\begin{aligned}
&\mathbb{P}\left[X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n\right] \\
=&\mathbb{P}\left[X_1 = x_1\right] \times \mathbb{P}\left[X_2 = x_2 | X_1 = x_1\right] \times \mathbb{P}\left[X_3 = x_3 | X_2 = x_2, X_1 = x_1\right] \\
&\qquad \times \cdots \times \mathbb{P}\left[X_n = x_n | X_{n-1} = x_{n-1}, \ldots, X_1 = x_1\right]
\end{aligned}
$$

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

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

Developing Notion of Security VI

The previous manipulation relied on the following two results

Claim

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

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

You will prove this result in the homework.