lec 22

Sequential Secret Sharing (SQS)

In a SQS, multiple secrets are shared using a master secret. Although the players in the i^{th} initial level have the required authority to recover the master secret, the cannot do that without the sequential cooperation of the players from all levels.

Example: assume the president & vice president, ministers & senators are in three different authority levels. The president & vice president can recover the master secret only if the have cooperation of ministers & senators. on the other hand, even by having those confirmations, the final secret recovey of the master secret can be done by president & vice president.

Example of the protocal suppose the goal is to creat a 3-level SQS scheme among a set of 13 players. Consider the following subsets:

$$\mathcal{P} = \{P_1 \cdots P_{13}\} \longrightarrow \mathcal{P}_1 = \{P_1, P_2, P_3\}$$

$$\mathcal{P}' = \{P_4 \cdots P_{13}\} \qquad \mathcal{P}_2 = \{P_4, P_5, P_6, P_7\}$$

$$\mathcal{P}_3 = \{P_8, P_9 \cdots, P_{13}\}$$

Sharing phase & the Example

1. The dealer shares a master secret α_1 with the players in $\mathcal{P}$ using a $(2, 13)$-threshold scheme. We denote this sharing by the following notation: $\alpha_1 : \mathcal{P} = \{P_1 \cdots P_{13}\}^{t_0=2}$ (t = 2, n = 13)

2. (a) The players $P_i \in \mathcal{P}$ use poly production protocol to create shares of an unknown secret β_1 having a threshold $t_1 = 3$.

   (b) They add their shares locally to obtain shares of $\alpha_2 = \alpha_1 + \beta_1$ which has a threshold of $t_1 = 3$. All the players erase the shares of α_1.

   (c) players $\{P_1 \cdots P_3\}$ only keep the shares of β_1 & players $\{P_4 \cdots P_{13}\}$ only keep the shares of α_2:

   $$\beta_1 : \mathcal{P}_1 = \{P_1 \cdots P_3\}^{t_1=3} \quad \text{and} \quad \alpha_2 : \mathcal{P}' = \{P_4 \cdots P_{13}\}^{t_1=3}$$

3. (a) The players $P_i \in \mathcal{P}'$ use poly production protocol to create shares of an unknown secret β_2 having a threshold $t_2 = 4$.

   (b) They add their shares locally to obtain shares of $\alpha_3 = \alpha_2 + \beta_2$ which has a threshold of $t_2 = 4$. The players $P_i \in \mathcal{P}'$ erase the shares of α_2.

   (c) players $\{P_4 \cdots P_7\}$ only keep the shares of β_2. Also $\{P_8 \cdots P_{13}\}$ increase threshold $t_2 = 4$ to $t_3 = 6$ & keep the shares of α_3.

   $$\beta_2 : \mathcal{P}_2 \{P_4 \cdots P_7\}^{t_2=4} \quad \text{and} \quad \alpha_3 : \mathcal{P}_3 = \{P_8 \cdots P_{13}\}^{t_3=6}$$

Recovery phase of the Example

1. In the 1st step, six players $P_3 = \{P_8 \cdots P_{13}\}$ recover the secret α_3. These players are in the highest level.

2. Subsequently, players $P_2 = \{P_4 \cdots P_7\}$ recover the secret β_2. As a result, α_2 is uniquely reveal since

$$\alpha_3 = \alpha_2 + \beta_2 \pmod p$$

3. Finally, $P_1 = \{P_1 \cdots P_3\}$ recover the secret β_1. As result, the master secret α_1 is revealed since $\alpha_2 = \alpha_1 + \beta_1 \pmod p$

$\ell = 3 \qquad t_0 = 2, \; t_1 = 3, \; t_2 = 4, \; t_3 = 6$

$\alpha_{i+1} = \alpha_i + \beta_i \longrightarrow \alpha_{i+1} = \alpha_i \beta_i$

Def: Sequential secret sharing is a hierarchical secret sharing scheme where a master secret α_1 along with $\ell - 1$ secrets $\alpha_2 \cdots \alpha_\ell$ are shared among the players with monotonically increasing thresholds $t_0 < t_1 < \cdots < t_\ell$. Let P be a set of "n" players and assume P is composed of ℓ disjoint levels:

$$P = \bigcup_{i=1}^{\ell} P_i \quad \text{where } P_i \cap P_j = \emptyset_{\text{Empty}} \text{ for all } 1 \le i < j \le \ell, \; |P_i| \ge t_i$$

Secret α_k (at level k) can be then recovered only if players in $R_k = \bigcup_{i=k}^{\ell} P_i$ cooperate & recover their secrets sequentially, i.e., from the highest level "ℓ" down to level "k" meaning that α_1 can be only recovered by P_1 only if players in all other levels seq recover their secrets.

Formal protocol SQS

Sharing phase

1. A dealer uses a Shamir scheme to distribute shares of an initial secret α_1 with threshold t_0 among players $\mathcal{P}=\{P_1 \cdots P_n\}$ & then he leaves the scheme.

2. players repeat the following steps for $1 \leq i \leq \ell-1$ to construct an ℓ-level sequential SS scheme.

   (a) players $\mathcal{P}$ use poly production protocol to generate shares of a random secret β_i with threshold t_i where $t_{i-1} < t_i$.

   (b) They compute shares of $\alpha_{i+1} = \alpha_i + \beta_i \pmod p$: the threshold of α_{i+1} is t_i. They then erase their shares of α_i.

   (c) A subset of players, $\mathcal{P}_i \subset \mathcal{P}$ where $|\mathcal{P}_i| \geq t_i$, only keep shares of β_i and the rest of players, $\mathcal{P} - \mathcal{P}_i$, only keep shares of α_{i+1}.

   (d) If $i=\ell-1$, the increase the threshold from $t_{\ell-1}$ to t_ℓ. otherwise ($i<\ell-1$), they set $\mathcal{P} \leftarrow \mathcal{P} \setminus \mathcal{P}_i$.

Recovery phase

1. Appropriate subsets of the players first cooperate to recover α_ℓ as well as $\underbrace{\beta_{\ell-1} \cdots \beta_1}$ unknown secrets

2. They solve the following system of linear congruences:

$$\alpha_{i+1} \equiv \alpha_i + \beta_i \pmod p \longrightarrow \text{given } \alpha_{i+1} \& \beta_i \rightarrow \text{unique } \alpha_i$$

for $i=\ell-1$ down to $i=1$. Therefore $\alpha_i \ldots \alpha_1$ are recovered.