Multi-level / Hierarchical Secret Sharing

Disjunctive Multi-level Secret Sharing Protocol (DJS)

Def: DJS has a hierarchical construction, where a certain number of players from at least one level must collaborate to reconstruct the secret.

The secret (α) is shared among the players with monotonically increasing thresholds: $t_1 < t_2 < \ldots < t_L$

Let P be the set of n players, where P is composed of L disjoint sets, or levels.

$$P = \bigcup_{i=1}^{L} P_i \text{ , where } P_i \cap P_j = \phi \text{ for all } 1 \le i < j \le L$$

$$\text{and } |P_i| \geq t_i$$

Then, the secret can be recovered by an authorized subset of players A, iff the members satisfy at least one threshold at level 1 to j.

$$\left| A \cap \left(\bigcup_{i=1}^{j} P_i \right) \right| \geq t_j \quad \text{for at least one } j \text{, where } 1 \le j \le L$$

DJS) $\boxed{\text{Sharing Phase}}$

① Each player is assigned to a level Γ_j, where each level Γ is a disjoint subset of the set of all players P.
There are L disjoint levels, where each level Γ_j is assigned a threshold value t_j such that: $t_1 < t_2 < \cdots < t_L$

Players at the lowest levels have the lowest threshold values and highest authority in secret recovery.

$$|P| = n \quad \text{and} \quad \bigcap_{i=0}^{L} \Gamma_i = \phi \quad \text{and} \quad \bigcup_{i=0}^{L} \Gamma_i = P$$

② The dealer selects a polynomial of degree $t-1$, $f(x) \in \mathbb{Z}_q(x)$
The leading coefficient is the secret (α), and t is the publicly known maximum threshold:

$$f(x) = \sum_{i=0}^{t-1} a_i x^i \quad \text{where } a_{t-1} = \alpha$$

Example: $f(x) = 2 + 3x + x^2 + 5x^3 + 6x^4 + \underline{\underline{13}}x^5$ $\boxed{\mathbb{Z}_{19},\ t=6}$ $\alpha = 13$

14 15 $\rightarrow L_0 \rightarrow t_0 = 2$
11 12 13 $\rightarrow L_1 \rightarrow t_1 = 3$
7 8 9 10 $\rightarrow L_2 \rightarrow t_2 = 4$
1 2 3 4 5 6 $\rightarrow L_3 \rightarrow t_3 = 6$

③ For each level Γ_j with threshold t_j, the dealer takes the d^{th} derivative of the original polynomial, where $d = t - t_j$, and computes the share (α_i) for each level's player p_i: $f^d(i) = \alpha_i$ so that player p_i recieves (i, α_i) for each player $p_i \in \Gamma_j$

$L_0 \rightarrow f^4(x) = 11 + 2x \longrightarrow$ (players 14-15)
$L_1 \rightarrow f^3(x) = 11 + 11x + x^2 \longrightarrow$ (players 11-13)
$L_2 \rightarrow f^2(x) = 2 + 11x + 15x^2 + 13x^3 \longrightarrow$ (players 7-10)
$L_3 \rightarrow f^0(x) = 2 + 3x + x^2 + 5x^3 + 6x^4 + 13x^5 \longrightarrow$ (players 1-6)

(DJS) $\boxed{\text{Recovery Phase}}$

① A group of players can form an authorized subset A to recover the secret if there are at least t_j players at levels less than or equal to Γ_j:

$$|A| \geq t_j \quad \text{where } A \in \sum_{i=0}^{j} \Gamma_j \qquad A \in \bigcup_{i=0}^{j} \Gamma_j$$

② Each player starts with a parametric polynomial $g(x)$, of degree $t-1$, where t is maximum threshold. Each player will take the d^{th} derivative of the polynomial, where $d = t - t_j$, and t_j is the threshold for the player's corresponding level Γ_j.

$$g(x) = \sum_{i=0}^{t-1} a_i x^i \quad \text{where } a_{t-1} = \alpha$$

<u>Example</u>:

$$f^0(x) = a + bx + cx^2 + dx^3 + ex^4 + gx^5 \longrightarrow L_3$$
$$f'(x) = b + 2cx + 3dx^2 + 4ex^3 + 5gx^4$$
$$f^2(x) = 2c + 6dx + 12ex^2 + gx^3 \longrightarrow L_2$$
$$f^3(x) = 6d + 5ex + 3gx^2 \longrightarrow L_1$$
$$f^4(x) = 5e + 6gx \longrightarrow L_0$$

③ Each player then substitutes their ID for x, and their share for their $g(x)$ solution. By combining each of the players' parametric equations, (in subset A), the leading coefficient (original secret α) can be recovered.

<u>Example</u>: $L_0 : t_0 = 2$ $(14, 1)$ and $(15, 3)$

$$\left.\begin{aligned} 5e + 6g(14) &= 1 \\ 5e + 6g(15) &= 3 \end{aligned}\right\} \longrightarrow e = 6,\ g = 13$$

$13 = \alpha$ ✓

CJS: Conjunctive Hierarchical Secret Sharing

DEF: In a conjunctive secret sharing scheme, a secret α is shared among the players with monotonically increasing thresholds $t_1 < t_2 < \dots < t_L$. Let P be a set of "n" players and assume P is composed of L disjoint levels.

$$P = \bigcup_{i=1}^{L} P_i, \text{ where } P_i \cap P_j = \underset{\text{EMPTY}}{\emptyset} \text{ for all } 1 \le i \le j \le L$$

AND $|P_i| \ge t_i$ for all i

↳ SET OF PLAYERS AT LEVEL i

P, P_i, P_j are sets

In this model, the secret α can be then recovered by an authorized subset of players A only if:

$$|A \cap (\bigcup_{i=1}^{j} P_i)| \ge t_j \text{ for all } j \text{ where } 1 \le j \le L$$

Sharing Phase

① Each player is assigned to a level T_j, where each level T is a disjoint subset the set of all players P. There are L disjoint levels, where each level T_j is assigned a threshold value t_j such that $t_1 < t_2 < \dots < t_L$.

② THE Dealer assigns the player ids in increasing order or random.

(3) The dealer selects a polynomial of degree $t-1$, $f(x) \in \mathbb{Z}_q[x]$ Where the secret (α) is the constant term.

Example: $f(x) = \underbrace{\boxed{13}}_{\text{SECRET}} + 3x + x^2 + 5x^3 + 6x^4 + 2x^5 \qquad \mathbb{Z}_{19}$

$L_0 \to t_0 = 2$ 1 2

$L_1 \to t_1 = 3$ 3 4 5

$L_2 \to t_2 = 4$ 6 7 8 9

$L_3 \to t_3 = 6$ 10 11 12 13 14 15

(4) For each level Γ_j with threshold t_j, the dealer takes the h^{th} derivative of the original polynomial, Where h is the threshold of the previous level (Γ_{j-1}). The dealer computes the shares (α_i) for each player P_i in the level $f^h(i) = \alpha_i$, so that the player P_i recieves (i, α_i) for each $P_i \in \Gamma_j$

$f^{(0)}(x) = 13 + 3x + x^2 + 5x^3 + 6x^4 + 2x^5 \longrightarrow$ FOR PLAYERS 1-2

$f^{(2)}(x) = 2 + 11x + 15x^2 + 2x^3 \longrightarrow$ FOR PLAYERS 3-5

$f^{(3)}(x) = 11 + 11x + 6x^2 \longrightarrow$ FOR PLAYERS 6-9

$f^{(4)}(x) = 11 + 12x \longrightarrow$ FOR PLAYERS 10-15

Recovery Phase

1) A group of authorized players A can recover the secret iff A is a subset of players from all levels, such that $|A| \geq t_j$

2) Each player creates a parametric polynomial $g(x)$ of degree $t-1$, where t is the maximum threshold. Each player will take the h^{th} derivative of the polynomial where h is the threshold of the previous level.

$$g(x) = \sum_{i=0}^{t-1} a_i x^i \quad \text{Where } a_0 = \alpha \rightarrow \text{SECRET}$$

3) Each player collaborates to construct j equations with at most j unknowns.

FOR EXAMPLE:

$$f^{(0)}(x) = a + bx + cx^2 + dx^3 + ex^4 + gx^5 \longrightarrow \begin{cases} a + b + c + d + e + g = 11 \\ a + 2b + 4c + 8d + 16e + 13g = 1 \end{cases}$$

$$f^{(2)}(x) = 2c + 6dx + 12ex^2 + gx^3 \longrightarrow \{ 2c + 13d + 13e + 8g = 15$$

$$f^{(3)}(x) = 6d + 5ex + 3gx^2 \longrightarrow \{ 6d + 11e + 13g = 6$$

$$f^{(4)}(x) = 5e + 6gx \rightarrow \begin{cases} 5e + 3g = 17 \\ 5e + 9g = 10 \end{cases}$$

4) Each player uses his id and share to solve the system of linear equations to recover the secret.

$\boxed{a = 13}$ $\quad b = 3 \quad c = 1 \quad d = 5 \quad e = 6 \quad g = 2$

$\hookrightarrow$ secret α

NOTE: YOU CAN USE CRAIMER'S RULE TO SOLVE THE SYSTEM OF LINEAR EQUATIONS.