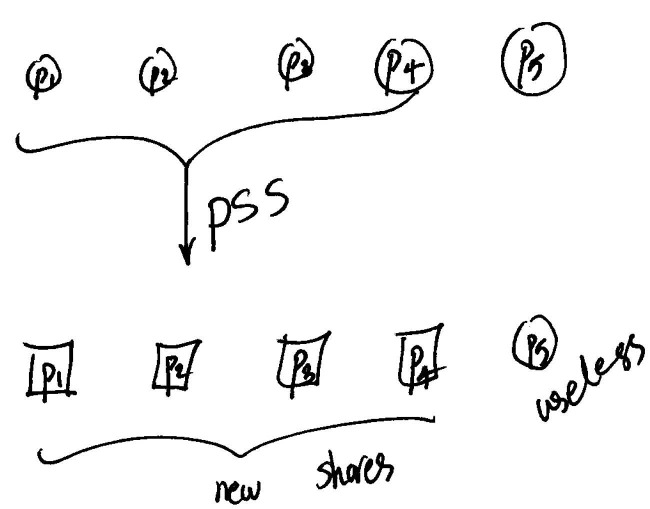
Danamic Secret Sharing (DSS)

players are able to activate a specific access structure out of a given set or recover various secrets in diff time intervals by transmitting a unique broadcast message.

Any secret sharing scheme in which the number of players (by enrollment or disenrollment protocols), the threshold and/or access structure can be changed dynamically.

(t, n) ⟶ must be done in the absence of the dealer: without having access to the original secret sharing poly

1. disenrollment
to decrease "n" ⟶ All you need to do is to execute proactive secret sharing among players excluding the one that you want to disenroll



② $n \nearrow$ **Enrollmet protocol**

① players select an id j such that $j \notin P$. Then, t players P_i are selected (e.g. $1 \leq i \leq t$). They compute Lagrange $\underset{\text{public}}{\underline{\text{constants}}}$ as follows

$$\gamma_i = \prod_{\substack{1 \leq K \leq t \\ i \neq K}} \frac{j-K}{i-K}$$ where i, j, K are players' ids

② Each P_i multiplies his share $f(i)$ by his Lagrange constant. H then randomly splits the result into "t" portions.

$$\underbrace{f(i)}_{\text{share of } P_i} * \gamma_i = \partial_{1i} + \partial_{2i} + \cdots + \partial_{ti} \quad \text{for } \underbrace{1 \leq i \leq t}.$$

③ players enchanges ∂_{Ki}'s through pairwise channels. As a result, each player P_K holds "t" values. He adds these values & reveal $\sigma_K = \sum_{i=1}^{K} \partial_{Ki}$ to the newcomer.

④ The newcomer simply add these values together & the result is a new share on the secret sharing polynomial. $f(j) = \sum_{K=1}^{t} \sigma_K$

Example

Enrollment protocol to increase "n"

$f(x) = 3 + 2x + x^2$ $\qquad \mathbb{Z}_{41} \longrightarrow \boxed{t=3}$

$P_1 \rightarrow 6$
$P_2 \rightarrow 11$
$P_3 \rightarrow 18$

The dealer is gone & we don't have access to $f(x)$.
players don't want to reveal their private shares.
they want to generate $f(4)$ for P_4 as a newcomer.

public values

$$C_1 = \frac{(4-2)(4-3)}{(1-2)(1-3)} = 1 \qquad C_2 = \frac{(4-1)(4-3)}{(2-1)(2-3)} = -3$$

$$C_3 = \frac{(4-1)(4-2)}{(3-1)(3-2)} = 3$$

P_1: $6 * 1 = 6 \rightarrow 1, 2, 3$

P_2: $11 * -3 = -33 \overset{41}{\equiv} 8 \rightarrow 1, 5, 2$

P_3: $18 * 3 = 54 \overset{41}{\equiv} 13 \rightarrow 4, 5, 4$

$$\begin{array}{c} P_1 \rightarrow \\ P_2 \rightarrow \\ P_3 \rightarrow \end{array} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 5 & 2 \\ 4 & 5 & 4 \end{bmatrix}$$

each player generates a row

received: $P_1 \rightarrow 6$, $P_2 \rightarrow 12$, $P_3 \rightarrow 9$

P_4: $6 + 12 + 9 = 27$

check $f(4) = 3 + 2(4) + (4)^2 = 27$ ✓

$\boxed{\text{Threshold Modification in the passive adv setting}}$ $t \nearrow\!\swarrow$

(I) $\boxed{\text{Lagrange Method}}$

$t \longrightarrow t' > t$ or $t' < t$

$f(x) \longrightarrow$ original SS poly of degree $t-1$

(1) Each player P_i selects a random polynomial $g_i(x)$ of degree at most $t'-1$ such that $\underbrace{g_i(0) = f(i)}_{\text{i.e., re-share his share}}$. He then gives $g_i(j)$ to P_j $1 \leq j \leq n$.

$$\mathcal{E}_{n \times n} = \begin{bmatrix} g_1(1) & g_1(2) & \cdots & g_1(n) \\ & & & \\ & & & \\ g_n(1) & g_n(2) & \cdots & g_n(n) \end{bmatrix} \longleftarrow P_1 \text{ generates}$$

where $g_i(0) = f(i)$

$\downarrow$ received by P_1 $\qquad$ $\downarrow$ by P_n

(2) A set Δ is determined such that it consists of the identifiers of at least "t" elected players. Then the following public constants are computed:

$$\gamma_i^{\Delta} = \prod_{\substack{j \in \Delta \\ j \neq i}} \frac{j}{j-i} \quad \text{where } 1 \leq i, j \leq n \text{ represent players' ids}$$

(3) Each player P_j erases his old shares and the combines the auxiliary shares he has received from other players to compute his new share as follows

$$\varphi_j = \sum_{i \in \Delta} \left(\gamma_i^{\Delta} * g_i(j) \right)$$

II $\boxed{\text{Vandermonde Matrix}}$

1. The $\underbrace{\text{re-sharing}}$ phase is similar to the previous protocol. with $g_i(x)$ of degree $t'-1$ where $t'>t$ or $t'<t$

2. players compute the first row of a public matrix $V^{-1}_{n\times n} \pmod p$ to adjust the threshold.

   $V_{n\times n}$ is Vandermond matrix $V_{i,j} = i^{(j-1)}$ for $1 \leqslant i, j \leqslant n$.

   suppose this vector is $V^{-1}_{1\times n} = (v_1, v_2, \dots, v_n)$

   inverse

3. Each player P_j computes his final share by multiplying $V^{-1}_{1\times n}$ by his vector of shares:

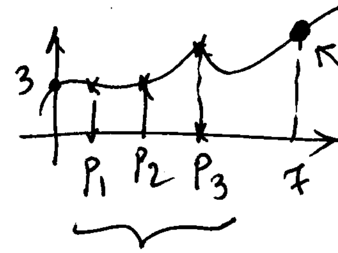
$$\varphi_j = \sum_{i=1}^{n} v_i \, g_i(j) \overset{P_1}{\Longrightarrow} v_1 \, g_1(1) + \dots + v_n \, g_n(1)$$

$$\begin{bmatrix} v_1 & v_2 & \cdots & v_n \end{bmatrix} \begin{bmatrix} g_1(1) \\ \vdots \\ g_n(1) \end{bmatrix}$$

Threshold Decrease from (t) to $(t-1)$ in the passive adv setting

① players select an <u>id</u> (j) such that $j \notin P$.

Then, t players P_i are selected $(1 \leq i \leq t)$



They compute Lagrange constants $\gamma_i = \prod\limits_{\substack{i \neq k \\ 1 \leq k \leq t}} \frac{j-k}{i-k}$

② Each P_i multiplies his original share $f(i)$ by his Lagrange constants

and then splits the result: $f(i) * \gamma_i = \delta_{1i} + \delta_{2i} + \cdots + \delta_{ti}$ (randomly)

③ They enchage these splitted values $\longrightarrow$

$$\begin{bmatrix} \delta_{1i} & \delta_{2i} & \cdots & \delta_{ti} \\ \delta_{1t} & \delta_{2t} & \cdots & \delta_{tt} \end{bmatrix}$$

P_1 receives

$$\sigma_k = \sum_{i=1}^{t} \delta_{ki}$$

④ players add these values together to compute the public $f(j) = \sum\limits_{k=1}^{t} \sigma_k$

⑤ Each player combines his privat share $f(i)$ with public share $f(j)$ as follows:

$$\hat{f}(i) = f(j) - j \left(\frac{f(i) - f(j)}{i - j} \right)$$

public share

location of public share

private share

player's id

⑥ shares $\hat{f}(i)$ are on a new poly $\hat{f}(x) \in \mathbb{Z}_p[x]$ of degree at most $(t-2)$ where $\hat{f}(0) = f(0)$. Therefor, the thereshold decreased by one.

Threshold Increase from t to t' $t' > t$ in the passive adv setting

poly production

① t players P_i are selected at random in order to act as independent dealers.

② Each of t chosen players P_i shares a secret S_i among all the players using TSS. The degree is $t-1$ for all these polynomials. $\longrightarrow S_1 \dots S_t \longrightarrow$ "t" secrets

③ Each player adds his shares of $\underbrace{S_i}$ together. As a result, each P_i has a share on a poly $g(x)$ of degree $t-1$ with the following constant term: $S = \sum_{i=1}^{t} S_i$

Increase the threshold

① players use "poly production" to generate shares of an unknown secret S on a poly $g(x)$ of degree $(t'-2)$

② Each player multiplies his share $g(i)$ by (i). Now, each P_i has a share of $\underset{\text{zero}}{\underline{\phi}}$ on poly $\hat{g}(x) = x * g(x)$ of degree $t'-1$

③ Each player adds his original share $f(i)$ (secret α) to his share $i\,g(i)$ (secret ϕ). As a result, each player has a share of "α" where the threshold now is $t' > t$.