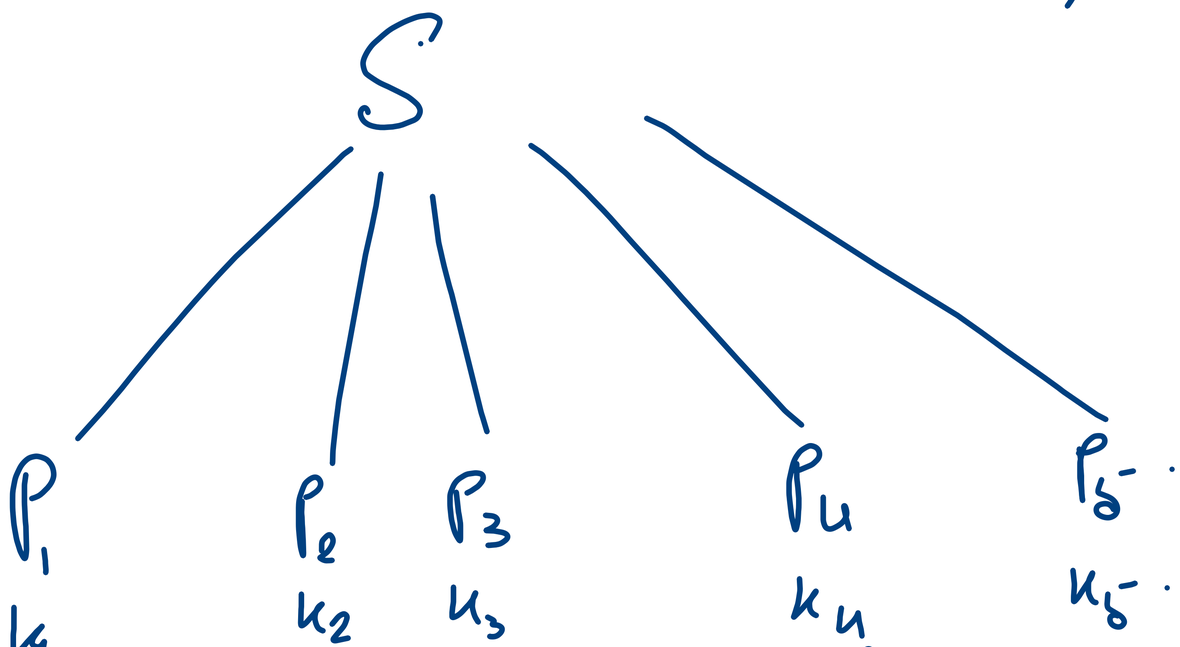
Secret-Sharing / Information Splitting.



3 out of 5 Secret Sharing Scheme.

2-out-of-3.

3 out of 4.

Shamir's threshold scheme.

t out of n scheme (t, n)-scheme.

$S \in \mathbb{Z}_p$.

(1) generate $t-1$ random coefficients from $\mathbb{Z}_p$.
$a_1, a_2, \ldots, a_{t-1}$.

(2) $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$.

where $a_0 = S$.

assume the participants $1, 2, 3, \ldots, n$.

(3) evaluate $p(1), p(2), \ldots, p(n)$ $\quad p(i) \to i$.

Example :- 3 out of 4 scheme., $S \in \mathbb{Z}_7$.

$S = 3$.

$p(x) = 2x^2 + 5x + 3$. t out of n scheme.

$p(0) = 3 = S$.

$S_1 = p(1) = 3$.

$S_2 = p(2) = 0$

$S_4 = p(4) = \underline{6}$.

$$p(x) = 3 \cdot \frac{(x-2)(x-4)}{(1-2)(1-4)} + 0 \cdot \frac{\quad}{\quad} + 6 \frac{(x-1)(x-2)}{(4-1)(4-2)}.$$

$$= 2x^2 + 5x + \underline{3}.$$

who does the reconstruction?

S → Dealer. (Global information.

→ communication Channels.

P_1 P_2 P_3 - - - - P_n. (Participants)

(local information.)

Verifiable Secret Sharing.

Adversarial models

1. Modify the shares of the participants
2. Destroy local information.
3. Dictator

General expression

$$p(x) = t_0 + t_1 x + \cdots + t_{k-1} x^{k-1}.$$

Shares $s_i = p(a_i) \longrightarrow$ user i

Secret $s = p(0)$.

$$p(x) = \sum_{r=1}^{k} p(a_{i_r}) \frac{(x-a_{i_1}) \cdots \boxed{(x-a_{i_r})} \cdots (x-a_{i_k})}{(a_{i_r}-a_{i_1}) \cdots \boxed{(a_{i_r}-a_{i_r})} \cdots (a_{i_r}-a_{i_k})}.$$

$S \in \mathbb{Z}_p$

Shares $\in \mathbb{Z}_p$.

Information rate of Shamir. S.S $= \dfrac{\text{max size of the shares}}{\text{size of secret}}$

$= \boxed{1}$

Ideal S.S.S → which has information ratio = 1.

Access structure :- $P = \{p_1, p_2, p_3, \ldots, p_n\}$.

$\mathcal{A}$ is a monotone collection of subsets of P.

if $A \in \mathcal{A}$ and $B \supseteq A$, then $B \in \mathcal{A}$.

If $A \in \mathcal{A}$ → authorized sets.

If $B \notin \mathcal{A}$ → unauthorized sets.

n- out of n Scheme

$S \in \mathbb{Z}_p$.

generate $n-1$ random elements.

$$s_1, s_2, \ldots, s_{n-1}.$$

$$s_n = s - (s_1 + s_2 + \cdots + s_{n-1})$$

Access structure is determined by the minimal subsets.

Example: $U = \{1, 2, 3, 4\}$.

$A_{min} = \{\{1,2\}, \{2,3\}, \{3,4\}\}$.

&: 1, 2, 3, 4, 13, 14, 24.

$\{1,2\} \rightarrow a$, &-a.

$\{2,3\} \rightarrow b$, &-b.

$\{3,4\} \rightarrow c$, &-c.

1 → a

2 → &-a, b

3 → &-b, c

4 → &-c.

a, &-b, c.

I.R = 2

↳ not an ideal scheme.

Theorem :- For any access structure $\mathcal{A}$, there is a Secret sharing scheme realizing $\mathcal{A}$.

Ex: $\left(\frac{n}{2}+1\right)$ out of n scheme.

a participant belongs to $\binom{n}{n/2}$ minimal qualified sets.

$$I.R \approx \binom{n}{n/2} \approx \frac{2^n}{\sqrt{n}}.$$

Open problem in S.S.Schem → given a genal access structure give a lower bound on the share size/ Information ratio

Formal Definition of S.S.

$P = \{p_1, p_2, \ldots, p_n\}$.

$\mathcal{A}$ → access structure : monotone collection of subsets of P.

Given: Set of secrets $\mathcal{K}$.

Given: a finite set R with some distribution μ.

Given: Domains of shares for each participant $\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_n$.

$\text{SHARE} : \mathcal{K} \times R \longrightarrow \mathcal{K}_1 \times \mathcal{K}_2 \times \cdots \times \mathcal{K}_n$.

$\text{SHARE}(k, r) = (sh_1, sh_2, \ldots, sh_n)$.

$sh_i \rightarrow p_i$

(1) Correctness/Completeness :- for any $B \in \mathcal{A}$.

$\exists$ a reconstruction function RECON.

$\text{RECON}_B : \mathcal{K}_{i_1} \times \mathcal{K}_{i_2} \times \cdots \times \mathcal{K}_{i_{(B)}} \longrightarrow \mathcal{K}$ s.t

for any secret $k \in \mathcal{K}$,

$$P_r\left[\text{RECON}_B\left(\text{SHARE}(k, r)_B\right) = k\right] = 1.$$

(2) for any unauthorized set $T \notin \mathcal{A}$ and for any two secrets $a, b \in \mathcal{K}$ and for all possible vector of shares $\langle sh_j \rangle_{p_j \in T}$

$$P_r\left[\text{share}(a, r)_T = \langle sh_j \rangle_{p_j \in T}\right]$$

$$= P_r\left[\text{share}(b, r)_T = \langle sh_j \rangle_{p_j \in T}\right]$$