Generalized Secret Sharing.

Secret $s \in \mathbb{F}$

$s_1 \; \text{- - - -} \; s_n \longrightarrow$ shares

Any t or less shares will have no info on s

Any $t+1$ or more shares will have full info on s

$\hookrightarrow$ polynomial time algo to reconstruct s.

Generalized version. $\Longrightarrow$ only some subset of shares can reconstruct s

General Access Structure $\mathbb{A}$

$\mathbb{A} \subseteq 2^{[1,\dots,n]}$

$\mathbb{A}$ is monotone

Shamir Secret Sharing $\longrightarrow$ All shares of size $>t$ can reconstruct

$S \subseteq [1,\dots,n]$ if $|S| > t$ then YES

$|S| \le t$ then NO

$\therefore \mathbb{A}$ for Shamir Secret Sharing

$$\mathbb{A} = \{ S \mid |S| > t \}$$

for Generalized version, only a few select subsets can reconstruct s

$f : \{0,1\}^n \longrightarrow \{0,1\}$

if $f(S) = 0$ then secret cannot be reconstructed

if $f(S) = 1$ then secret can be reconstructed

what does "monotone" mean?

if S is authorized to reconstruct the secret then any superset of this S can also reconstruct the secret

$\boxed{Q}$ Given access structure $\mathbb{A}$, design secret sharing scheme s.t. (open problem: finding optimum scheme)

$S \in \mathbb{A}$, subset S is authorized

$S \notin \mathbb{A}$, subset S is not authorized

for Shamir Secret Sharing if secret size $= k$ bits. (share size $= nk$.) bits.

Scheme.

For a subset $S \in \mathbb{A}$ & secret $\boxed{s}$

Choose $|S|-1$ random elements $\in \mathbb{F}$

say $\rho_1, \rho_2, \dots \rho_{|S|-1}$

Let $S = \{ i_1, i_2 \dots i_{|S|} \}$

Give to $i_j \longrightarrow \rho_j \quad j < |S|$

Give to $i_{|S|} \longrightarrow \left(s - \sum_{j=1}^{|S|-1} \rho_j \right)$

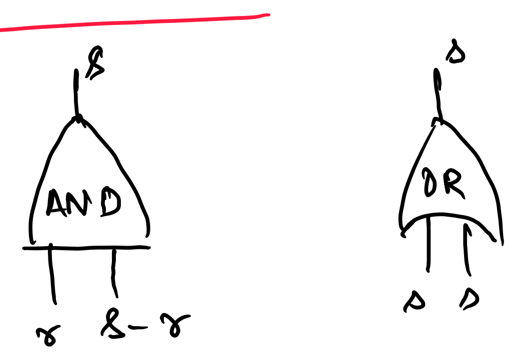
Total share size $= \sum_{S \in \mathbb{A}} |S|$

(for shamir: share size $= (t+1)\, {}^{n}C_{t+1}$

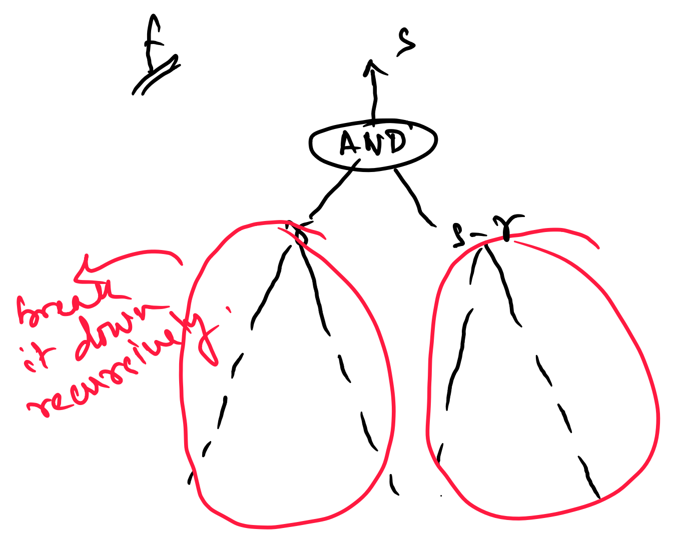
shamir had share size $= n$)

Thm: if f is monotone then it can be implemented using $\underbrace{\text{AND/OR Gate only}}_{\text{no need for NOT Gate}}$.

for 2 shares,



for a general f, break into circuit of branching (2)



This is still not optimum. since even though monotone f^ns can be implemented using AND, OR but circuit size if we use AND, OR, NOT is much smaller

AND, OR $\longrightarrow$ super polynomial circuit size.

AND, OR, NOT $\rightarrow$ polynomial " "

Assuming one-way f^ns exist, can we increase optimality of Shamir secret. Sharing

Secret s.

Choose Key k

$C = Enc_k(s)$ $\longrightarrow$ shamir secret sharing on k

$\hookrightarrow$ store in public

Original SSS :- nx bits.
$\hookrightarrow$ size of s.

New SSS :- $x + ny$. $\longrightarrow$ size of k. $\boxed{(y \ll x)}$

Open problem:- Give an example of $\mathbb{A}$ s.t it does not have an efficient secret sharing scheme

Inputs : secret s, No: of shares n, Access structure

Input size :- still not defined yet (right now, it is $|s| + n$)

$\hookrightarrow$ cannot explain complexity of Access structure

Open problem

Does every $\mathbb{A}$ have efficient (poly. in n & complexity of $\mathbb{A}$) sharing scheme?