- Scribes?
- lecture recording

- final exam
- last class today!

Function secret sharing (FSS)

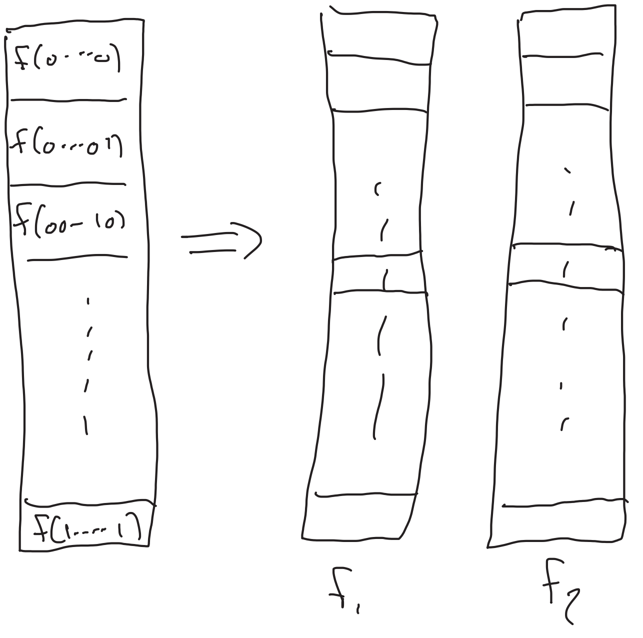
Given a function $f: \{0,1\}^K \to \{0,1\}$

distribute n shares $f_1, \dots, f_n$

- no collection of t shares $f_{i_1}, \dots, f_{i_t}$ gets information about f
- for any t+1 parties holding $f_{i_1}, \dots, f_{i_{t+1}}$, given an input x, then $f_{i_1}(x), \dots, f_{i_{t+1}}(x)$ should be a secret sharing of $f(x)$

E.g., if $n=2$, then for all x

$$f_1(x) \oplus f_2(x) = f(x)$$

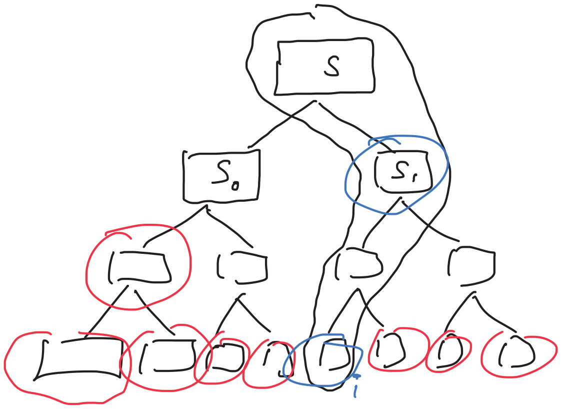


Point Function $f_i: \{1, \dots, N\} \to \{0,1\}$

$$f_i(x) = \begin{cases} 1 & \text{if } x = i \\ 0 & \text{o/w} \end{cases}$$

GGM tree

Assume $G: \{0,1\}^k \to \{0,1\}^{2k}$ is a pseudorandom generator



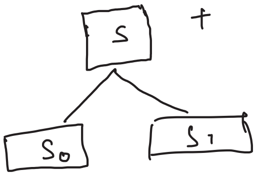
$s_0 / s_1 = G(s)$

FSS for point functions, 2-party case

Want to share f_i

set up information for each party to compute a tree satisfying the following:

- each node of the tree will have a seed & a control bit
- each level of the tree will have a correction word CW



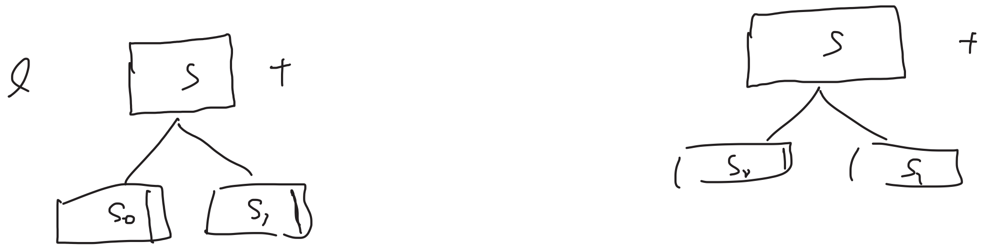
$s_0 / s_1 = G(s) \oplus t \cdot CW$

(1) On the special path, control bits of the parties XOR to 1, seeds should be independent

(2) Off the special path, control bits XOR to 0, seeds should be equal

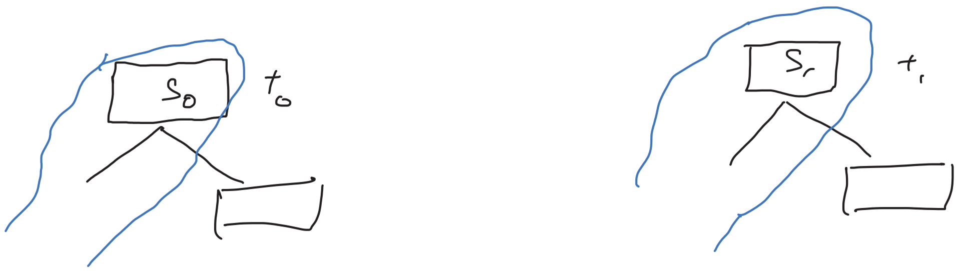
Construction:

- easy to set up the invariant at the root
- give to each party the same CW_ℓ for each level ℓ in tree
- Once (2) holds at some node, it holds for descendants



$s_0 | s_1 = G(s) \oplus t \cdot CW_\ell$

$t_0 \oplus t_1 = 1$



$G(s_0) \oplus t_0 \cdot CW$

$G(s_0) \oplus t_0 \cdot \boxed{(\underline{s_{CW}} | \underline{\gamma^L} | \underline{s_{CW}} | \underline{\gamma^R})}$ $\quad$ $G(s_1) \oplus t_1 \cdot \underline{(s_{CW} | \gamma^L | s_{CW} | \gamma^R)}$

$G_0(s_0) | t_0(s_0) | \boxed{G_1(s_0)} | t_1(s_0) \oplus t_0 \cdot (s_{CW} | \gamma^L | \boxed{s_{CW}} | \gamma^R)$

$\Longrightarrow \quad G_1(s_0) \oplus t_0 \cdot s_{CW} = G_1(s_1) \oplus t_1 \cdot s_{CW}$

$\Longrightarrow \quad s_{CW} = G_1(s_0) \oplus G_1(s_1)$

$\gamma^R = t_1(s_0) \oplus t_1(s_1)$

$\gamma^L = t_0(s_0) \oplus t_0(s_1) \oplus 1$

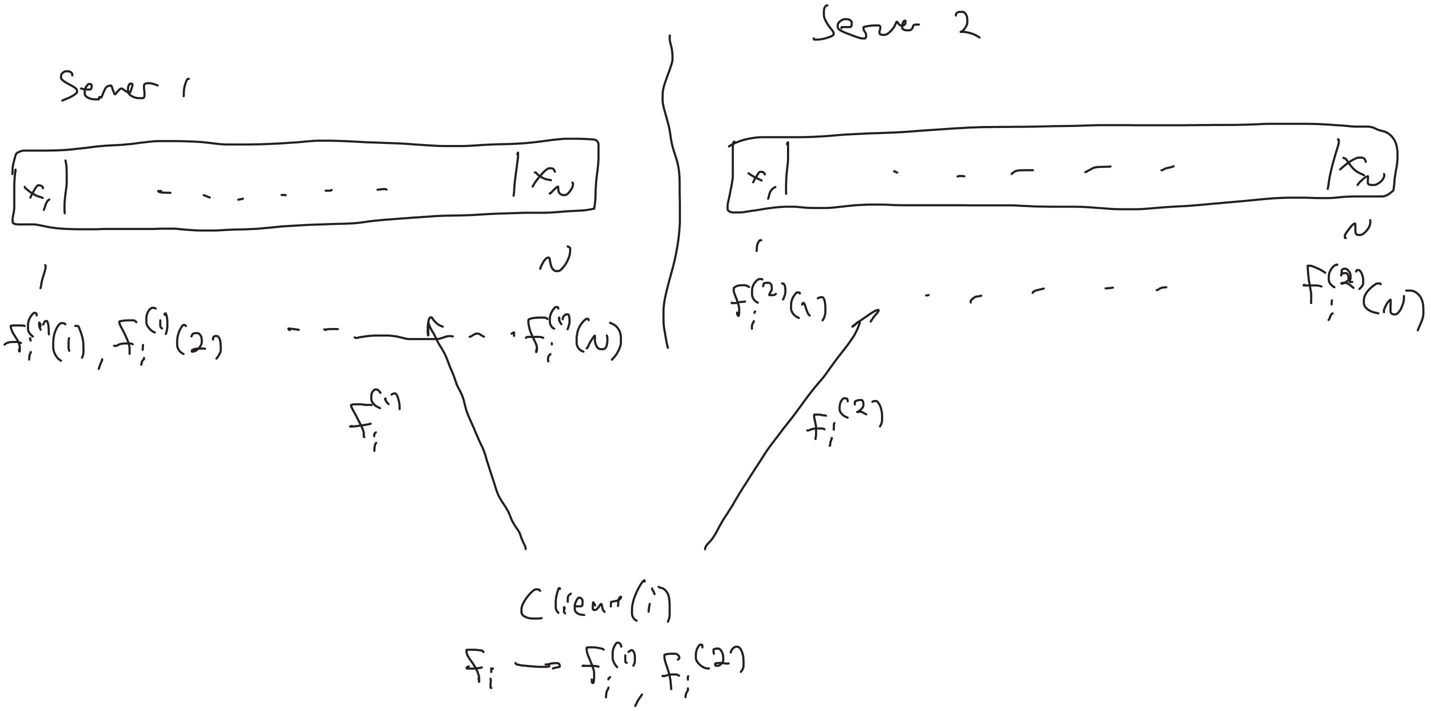
$s_0, t_0, CW_1, CW_2, \ldots, CW_\ell$ $\quad$ $s_1, t_1, CW_1, \ldots, CW_\ell$

$\ell = O(\log N)$

$|CW_i| = O(\kappa)$

$|\text{share}| = O(\kappa \cdot \log N)$

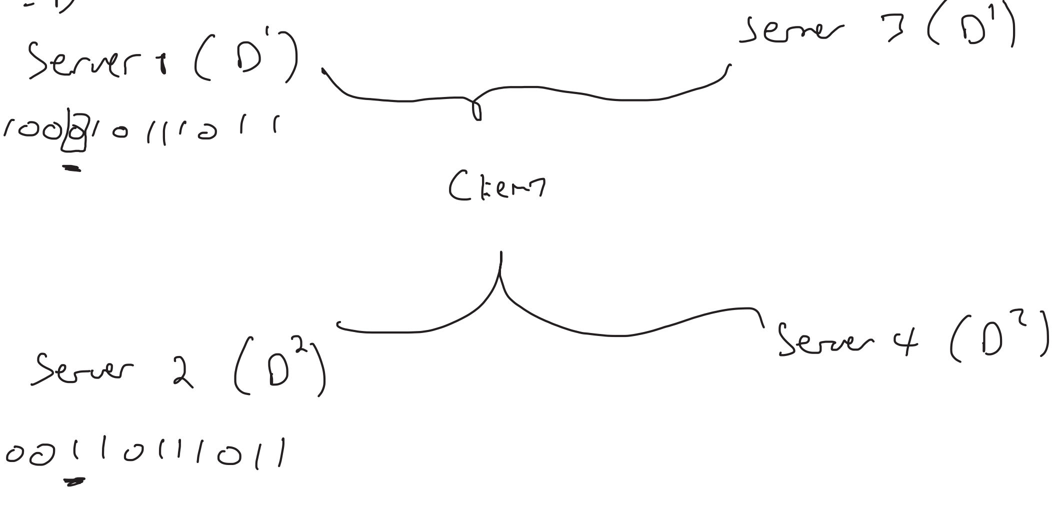
FSS for point functions ⇒ PIR



Server 1
Server 2
x_1
x_N
1
N
$f_i^{(1)}(1), f_i^{(1)}(2) \dots f_i^{(1)}(N)$
$f_i^{(2)}(1) \dots f_i^{(2)}(N)$
$f_i^{(1)}$
$f_i^{(2)}$
Client (i)
$f_i \rightarrow f_i^{(1)}, f_i^{(2)}$

$$\underline{\bigoplus_{j=1}^{N} f_i^{(1)}(j) \cdot x_j} \oplus \underline{\bigoplus_{j=1}^{N} f_i^{(2)}(j) \cdot x_j} = x_i$$

$D^1 \oplus D^2 = D$



Server 1 (D^1)
$1 0 1 0 0 \boxed{0} 1 0 1 1 1 0 1 1$
Server 3 (D^1)
Client
Server 2 (D^2)
$1 0 1 0 0 1 1 0 1 1 1 0 1 1$
Server 4 (D^2)