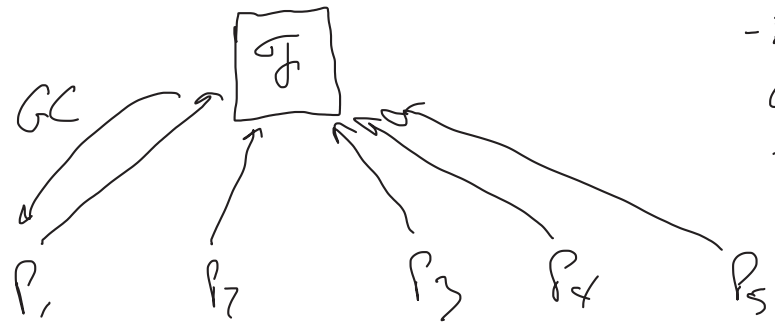
- Scribes?

Outline

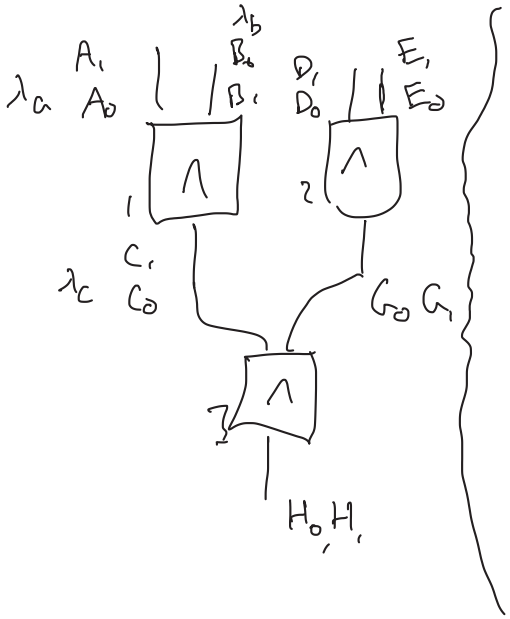
- BMR protocol
- BGW protocol / Beaver triples

- GMW protocol - multiparty setting,
  round complexity linear in depth of circuit
- Yao's protocol - 2-party setting
  constant round complexity
- Beaver-Micali-Rogaway (BMR)
  - multiparty protocol
  - $O(1)$ round complexity

idea: use GMW protocol to compute a garbled circuit



- if $\mathcal{F}$ can be computed by a constant-depth circuit, then we can securely compute $\mathcal{F}$ using the GMW protocol in $O(1)$ rounds

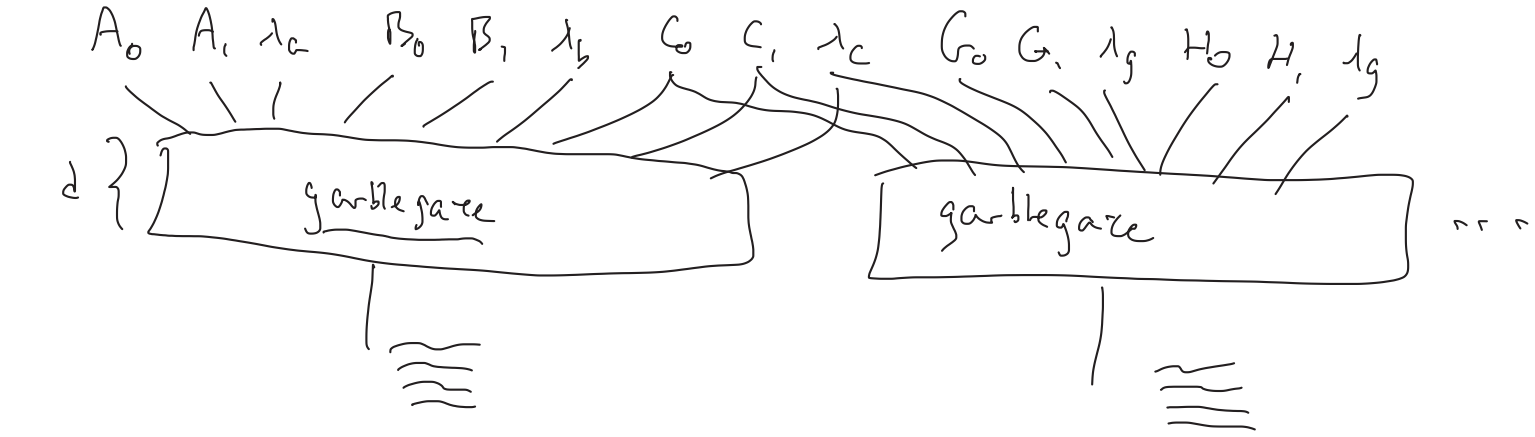


$$F_{A_0}(00,1) \oplus F_{B_0}(00,1) \oplus \left(C_{(\lambda_a \wedge \lambda_b) \oplus \lambda_c},\ (\lambda_a \wedge \lambda_b) \oplus \lambda_c \right)$$

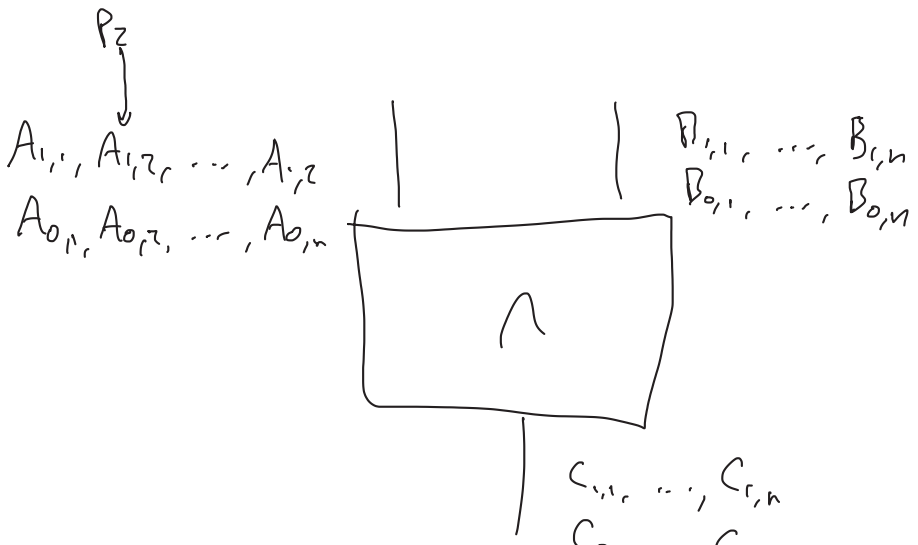
$$\vdots$$

$$F_{A_1}(11,1) \oplus F_{B_1}(11,1) \oplus \left(C_{(\bar{\lambda}_a \wedge \bar{\lambda}_b) \oplus \lambda_c},\ (\bar{\lambda}_a \wedge \bar{\lambda}_b) \oplus \lambda_c \right)$$

$A_0, A_1, \lambda_a, B_0, B_1, \lambda_b, \ldots, H_0, H_1, \lambda_h \xrightarrow{\mathcal{F}} GC$



$F_{A_0}(00,0),\ F_{B_0}(00,0),\ \lambda_a, C_0, C_1, \lambda_c \xrightarrow{O(1)\text{-depth circuit}}$



$\lambda_{a,1}, \lambda_{a,2}, \dots, \lambda_{a,n}$

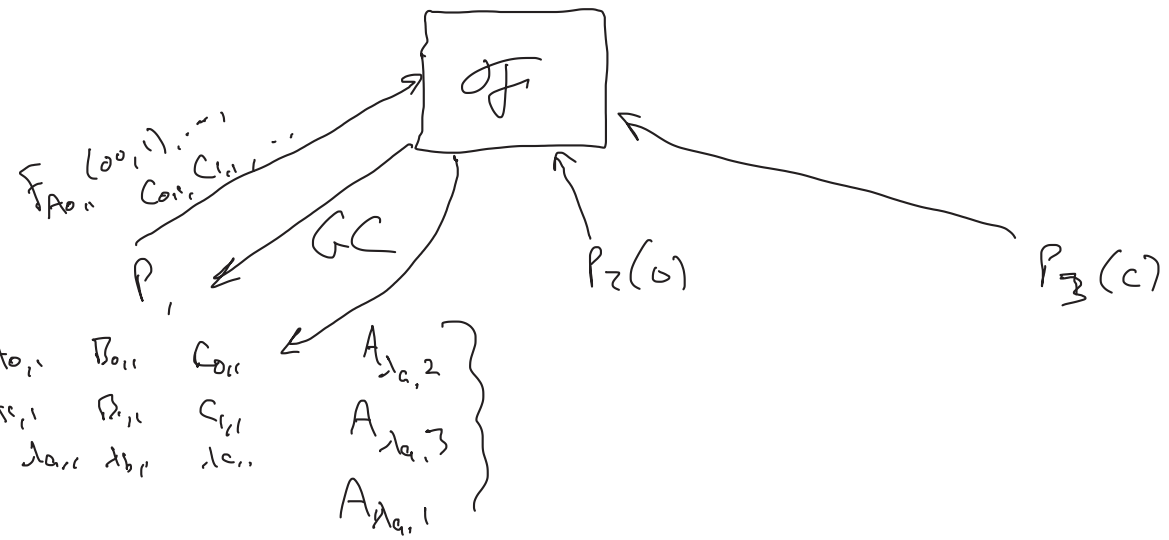
$\lambda_a = \lambda_{a,1} \oplus \dots \oplus \lambda_{a,n}$

00: $F_{A_{0,1}}(00,0) \oplus F_{A_{0,2}}(00,0) \oplus \dots \oplus F_{A_{0,n}}(00,0)$

$\oplus F_{B_{0,1}}(00,0) \oplus \dots \oplus F_{B_{0,n}}(00,0)$

$\oplus \left(C_{\lambda',1}, C_{\lambda',2}, \dots, C_{\lambda',n}, \lambda' \right)$,

where $\lambda' = (\lambda_a \wedge \lambda_b) \oplus \lambda_c$



- BGW protocol
  - multiparty protocol
  - round complexity linear in circuit depth
  - secure if $t < n/2$ parties are corrupted
  - unconditional security
  - arithmetic circuits over $\mathbb{F}_p$
    - wires hold field elements
    - gates are addition/multiplication over $\mathbb{F}_p$

map boolean circuit to arithmetic circuit over $\mathbb{F}_p$:

$0 \rightarrow 0$

$1 \rightarrow 1$

$\wedge \rightarrow$ multiplication

$a \oplus b \rightarrow a + b - 2ab$

For some problems, arithmetic circuits can be smaller than boolean circuits

---

Shamir secret sharing

$x \rightarrow x_1, \ldots, x_n$ s.t. $x_1 \oplus \cdots \oplus x_n = x$

t-out-of-n secret sharing

- any t parties can reconstruct the shared value given their shares
- any set of $t-1$ parties learns no info. about shared value

Use polynomials over $\mathbb{F}_p$

- degree-t polynomial has at most t roots
- Any collection of $t+1$ pairs $\{(x_1, y_1), (x_2, y_2), \ldots, (x_{t+1}, y_{t+1})\}$, where x_i are distinct, define a unique degree-t polynomial f such that $f(x_i) = y_i$ for all i

Shamir scheme:

Given a secret value s, to share in $(t+1)$-out-of-n manner.

- define $f(X) = f_t X^t + f_{t-1} X^{t-1} + \ldots + f_1 X + s$, where $f_t, \ldots, f_1 \leftarrow \mathbb{F}_p$, $p > n$
- give share $f(i)$ to P_i