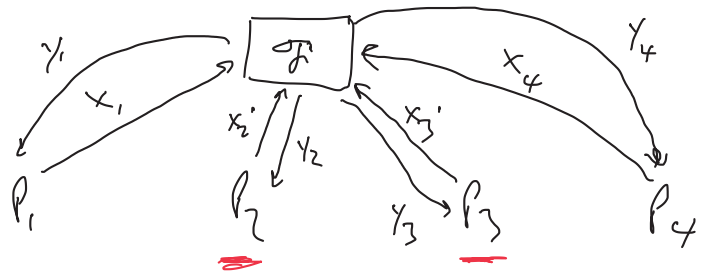
- Scribes?
- lecture recording
- no class next week
- Midterm

- GMW II Compiler
- Broadcast / Byzantine agreement

Security-with-abort



Standard model when $t \geq n/2$ and broadcast available

Can ensure that only one designated party can abort (if they are corrupted)

full security

malicious parties do not have the option of aborting the ideal functionality

Standard model when $t < n/2$ and broadcast available

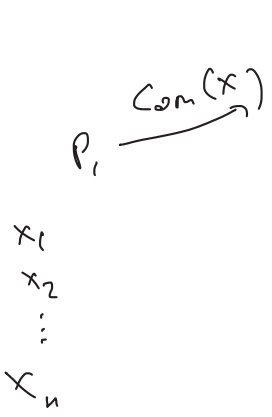
or $t < n/3$

GMW II Compiler

Start with semi-honest protocol Π, secure against $t < n/2$ parties

Shamir's secret sharing $\Rightarrow$ $(t+1)$-out-of-n sharing

Committed Verifiable secret sharing (VSS)



Public information:

$\vec{\text{Com}} = \text{Com}(x_1; r_1), \ldots, \text{Com}(x_n; r_n)$

Each party P_i holds:

- x_i, r_i

P_1 holds:

- $x_1, \ldots, x_n, r_1, \ldots, r_n$

$$\mathcal{F}_{VSS}(x_1, \perp, \ldots, \perp) = \left((\vec{\text{Com}}, \vec{x}, \vec{r}), (\vec{\text{Com}}, x_2, r_2), \ldots, (\vec{\text{Com}}, x_n, r_n)\right)$$

(x_1: $\perp$; $\vec{x}, \vec{r}$: $r_1, \ldots, r_n$; r_2; r_n)

Compiled protocol Π'

1. Parties compute $\mathcal{F}_{VSS}$ using a secure-with-abort protocol, once per party
   - if some P_i misbehaves, kick them out & use a default input for them
2. Parties do the same for a random version of $\mathcal{F}_{VSS}$, once per party
   - if P_i misbehaves, kick it out
3. Run Π using the committed inputs & randomness, giving ZK proof of correctness after each msg.

- if P_i fails when giving some ZK proof,
  - each party broadcasts their share of P_i's input/randomness, plus the corresponding f's
  - parties reconstruct P_i's input/randomness from $t+1$ correct shares
  - parties run Π on behalf of P_i from then on

Broadcast channel

Parties can realize a broadcast channel using a broadcast protocol

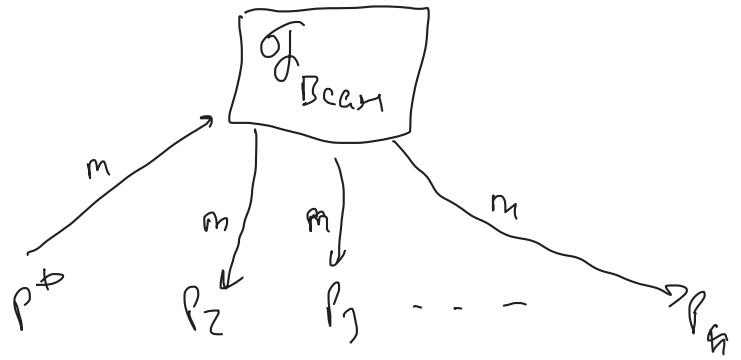
Broadcast protocol

Protocol run by parties $P_1, \dots, P_n$ with designated $P^* \in \{P_1, \dots, P_n\}$ acting as a sender w/ initial input m

[Validity] if P^* is honest, then all honest parties output m

[Consistency] all honest parties should output the same value

---



Broadcast protocol $\equiv$ realizing $\mathcal{F}_{Bcast}$ with full security*

* non-adaptive setting,
$t \geq 1$ corrupted parties (need private broadcast otherwise)

Byzantine agreement protocol

Protocol run by parties $P_1, \ldots, P_n$ where each P_i has initial input m_i

(Consistency) All honest parties output the same value

(Validity) If all honest parties hold the same input value m, then all honest parties output m

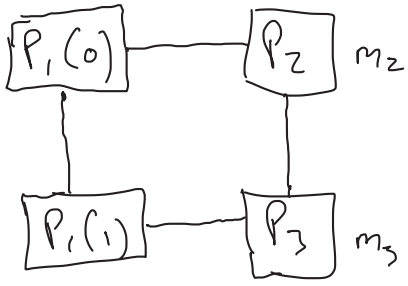
---

For $t < n/2$, BA $\Rightarrow$ broadcast

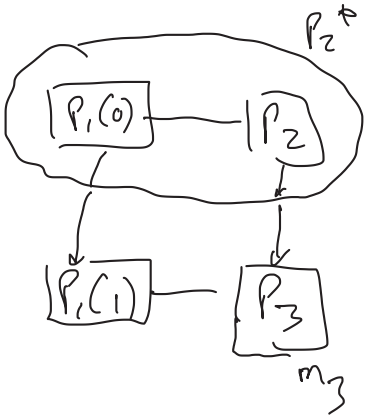
broadcast $\Rightarrow$ BA

BA only makes sense for $t < n/2$, whereas broadcast makes sense even for $t < n$

With no prior setup, BA/broadcast are impossible if $t \geq n/3$



imaginary experiment



real-world execution

Consistency $\Rightarrow$ $m_2 = m_3$

Validity $\Rightarrow$ $m_3 = 1$, $m_2 = 0$

} contradiction