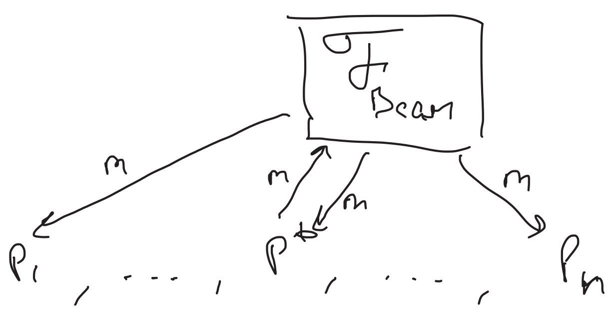
- Scribes?
- lecture recording
- no class next week

Broadcast definition

An n-party protocol run by $P_1, \ldots, P_n$ with a designated party $P^* \in \{P_1, \ldots, P_n\}$ is a broadcast protocol if:

[Validity] If P^* is honest & has input m, then all honest parties output m

[Consistency] All honest parties output the same value



Securely realizing $\mathcal{F}_{Bcast}$ (with full security)

$\Updownarrow$

broadcast

(assuming $t \geq 1$ corrupted parties)

---

last time: w/o setup, broadcast is impossible if $t \geq n/3$

Today:

- broadcast is possible if $t < n/3$ (w/o setup)
- w/ setup, broadcast is possible for $t < n$

Protocol for BA tolerating $t < n/3$ corruptions.

- Construct a phase-King sub-protocol, w/ designated party called "King"
- overall protocol:
  - run phase-King subprotocol $t+1$ times w/ $P_1, \dots, P_{t+1}$ as the successive Kings

Phase-King sub-protocol w/ King P_K :

(round 1) every P_i sends its input v_i to everyone else

each P_i sets $C_i^b = 1$ iff $\geq n-t$ parties sent it the bit b

(round 2) each P_i sends C_i^0, C_i^1 to everyone else $\quad C_i^v = 1 \quad C_i^{\bar{v}} = 0$

each P_i sets $D_i^b = \{\#$ of parties who sent $C^b = 1\}$ $\quad D_i^v \geq n-t \quad D_i^{\bar{v}} \leq t$

if $D_i^1 > t$, set $v_i = 1$; else $v_i = 0$ $\quad > t$

$\Rightarrow v_i = v$

(round 3) P_K sends v_K to all parties

each P_i does: if $D_i^{v_i} < n-t$, then output v_K

else output v_i $\quad \Rightarrow$ output v

Lemma If $t < n/2$ and all honest parties begin holding input v, then they all output v.

Lemma If $t < n/3$ and the King is honest, then all honest parties agree on their output.

Proof

P_K sends the same v_K to everyone.

The only possible way agreement can fail is if some honest P_i does not adopt the King's value.

I.e., if $D_i^{v_i} \geq n-t$.

Claim: if $D_i^{v_i} \geq n-t$, then $v_i = v_k$

Case 1 $v_i = 1$. Becase $D_i^1 \geq n-t$

$\Rightarrow$ any other honest party P_j has $D_j^1 \geq n-t-t$
$> t$

$\Rightarrow D_k^1 > t \Rightarrow v_k = 1$

Case 2 $v_i = 0$, $D_i^0 \geq n-t \Rightarrow D_k^0 \geq n-2t > t$.

$\Rightarrow$ at least one honest party sent $C^0 = 1$ in round 1

$\Rightarrow$ at least one honest party received 0 from $\geq n-t$ parties in round 1, & received 1 from $\leq t$ parties in round 1

$\Rightarrow$ every honest party received 1 from $\leq 2t$ parties in round 1, $2t < n-t$

$\Rightarrow$ every honest party sends $C^1 = 0$ in round 1

$\Rightarrow$ every honest party has $D_i^1 \leq t$

$\Rightarrow v_k = 0$

PKI = public-key infrastructure

every party P_i has (sk_i, pk_i) for signature scheme

every party has the same vector $(pk_1, pk_2, \ldots, pk_n)$

Dolev-Strong protocol

Assume P_1 is the sender

(m,i)-valid message is received in round i & has the form:

$m, \sigma_1, \underline{\sigma_2, \ldots, \sigma_i}$ by parties distinct from the receiver

m-valid message $\iff$ (m,i)-valid for some i

(round 1) P_1 signs m and sends m, σ_1 to everyone

(round 2, ..., n-1) If P_i received an m-valid message in the previous round, it appends its signature and sends an m-valid message in the current round

(Conclusion) Let S_i denote the set of m for which P_i received an m-valid message.

If $|S_i| = 0$ or $|S_i| > 1$ output 1

If $|S_i| = 1$, then output the value in S_i

Validity is immediate.

Consistency: Claim All honest parties agree on the set of m-valid messages

Efficiency?

The protocol as described is not necessarily efficient, but can be modified so that it is