

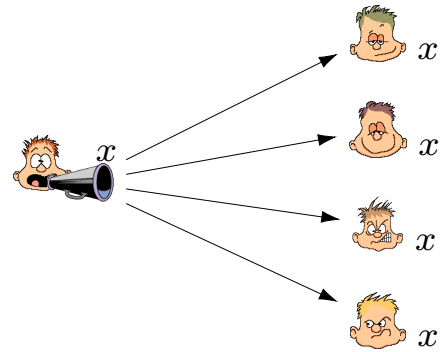
Cryptographic Protocols

Spring 2020

Broadcast

Ideal Broadcast

2



Standard Model

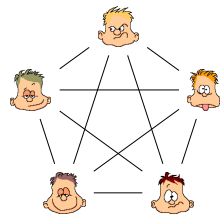
3

Players

- Player set $P = \{P_1, \dots, P_n\}$

Network

- Complete
- Synchronous
- Authenticated



Adversary

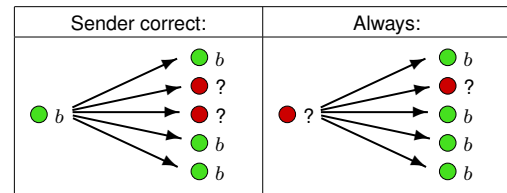
- Threshold $t < n/3$
- Active (Byzantine)
- Unlimited (information-theoretical security)

Definition: Broadcast

4

Definition (Input x_1 , Outputs y_1, \dots, y_n)

- **Consistency:** Every (correct) player receives the same output y .
- **Validity:** Sender correct \Rightarrow every player receives output $y_i = x_1$.
- **Termination:** Every player eventually receives output.

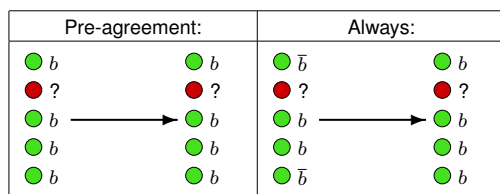


Definition: Consensus

5

Definition (Inputs x_1, \dots, x_n , Outputs y_1, \dots, y_n)

- **Consistency:** Every (correct) player receives the same output y .
- **Persistence:** All correct players have input $x \Rightarrow y_i = x$.
- **Termination:** Every player eventually receives output.



Broadcast vs Consensus

6

Broadcast: $(x, \perp, \dots, \perp) \rightarrow (y_1, \dots, y_n)$

Consensus: $(x_1, \dots, x_n) \rightarrow (y_1, \dots, y_n)$

Consensus \rightarrow Broadcast

1. P_1 : send x to every P_j , P_j receives x_j
2. $(y_1, \dots, y_n) = \text{Consensus}(x_1, \dots, x_n)$
3. $\forall P_j$: return y_j

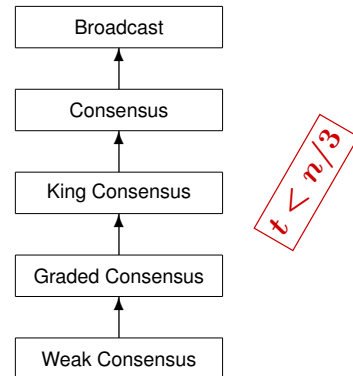
Broadcast \rightarrow Consensus

1. $\forall P_i$: Broadcast(x_i)
2. $\forall P_j$: return $y_j = \text{majority of received } x_i$'s

$t < n/2$

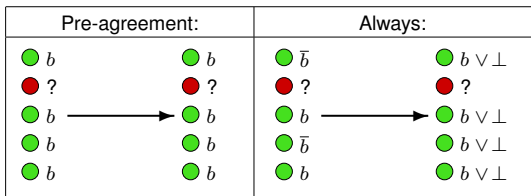
| Setting | Condition | Literature |
|-----------------------|--------------------------------|----------------|
| information-theoretic | $t < n/3$ | [PSL80, BGP89] |
| cryptographic | BC: $t < n$ Cons: $t < n/2$ | [DS82] |
| i.t. | BC: $t < n$ Cons: $t < n/2$ | [PW92] |

w/o setup
with setup



Definition (Inputs x_1, \dots, x_n , Outputs y_1, \dots, y_n)

- **Weak Consistency:** $\exists y \in \{0, 1\}$ such that \forall correct $P_i : y_i \in \{y, \perp\}$.
- **Persistency:** All correct players have input $x \Rightarrow y_i = x$.
- **Termination:** Every player eventually receives output.

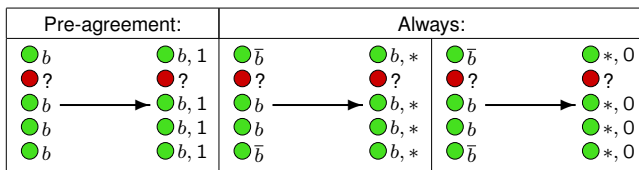


WeakConsensus(x_1, \dots, x_n) $\rightarrow (y_1, \dots, y_n)$

1. $\forall P_i$: send x_i to every P_j
2. $\forall P_j$: $y_j = \begin{cases} 0 & \text{if } \#Zeros \geq n - t \\ 1 & \text{if } \#Ones \geq n - t \\ \perp & \text{else} \end{cases}$
3. $\forall P_j$: return y_j

Definition (Inputs x_1, \dots, x_n , Outputs $(y_1, g_1), \dots, (y_n, g_n)$)

- **Graded Consistency:** Correct P_i has $g_i = 1 \Rightarrow \forall$ corr. $P_j : y_j = y_i$.
- **Graded Persistency:** All corr. players have input $x \Rightarrow (y_i, g_i) = (x, 1)$.
- **Termination:** Every player eventually receives output.



GradedConsensus(x_1, \dots, x_n) $\rightarrow ((y_1, g_1), \dots, (y_n, g_n))$

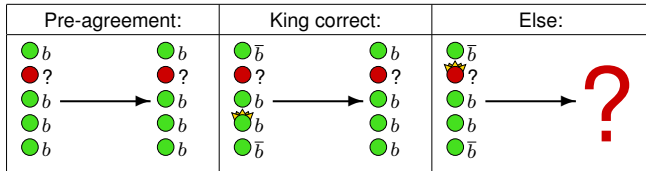
1. $(z_1, \dots, z_n) = \text{WeakConsensus}(x_1, \dots, x_n)$
2. $\forall P_i$: send z_i to every P_j .
3. $\forall P_j$: $y_j = \begin{cases} 0 & \text{if } \#Zeros \geq \#Ones \\ 1 & \text{if } \#Zeros < \#Ones \end{cases}$ $g_j = \begin{cases} 1 & \text{if } \#y_j\text{'s} \geq n - t \\ 0 & \text{else} \end{cases}$
4. $\forall P_j$: return (y_j, g_j)

Definition: King Consensus

13

Definition (Inputs x_1, \dots, x_n , Outputs y_1, \dots, y_n)

- **King Consistency:** King is correct $\Rightarrow \exists y : \forall$ correct $P_i : y_i = y$.
- **Persistency:** All correct players have input $x \Rightarrow y_i = x$.
- **Termination:** Every player eventually receives output.



Protocol King Consensus (King P_k)

14

$\text{KingConsensus}_k(x_1, \dots, x_n) \rightarrow (y_1, \dots, y_n)$

1. $((z_1, g_1), \dots, (z_n, g_n)) = \text{GradedConsensus}(x_1, \dots, x_n)$
2. P_k : send z_k to every P_j .
3. $\forall P_j: y_j = \begin{cases} z_j & \text{if } g_j = 1 \\ z_k & \text{else} \end{cases}$
4. $\forall P_j$: return y_j

Protocol Consensus

15

$\text{Consensus}(x_1, \dots, x_n) \rightarrow (y_1, \dots, y_n)$

1. for $k = 1$ to $t + 1$:
 $(x_1, \dots, x_n) = \text{KingConsensus}_k(x_1, \dots, x_n)$
2. $\forall P_j$: return x_j

Impossibility for 3 players, 1 corrupted

16

