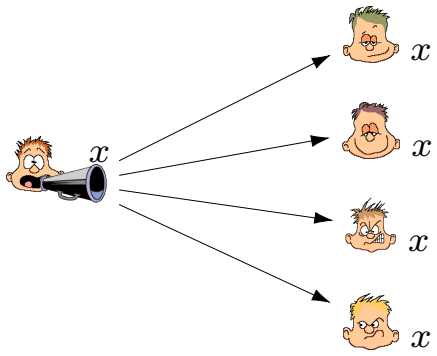
Cryptographic Protocols

Spring 2019

Broadcast

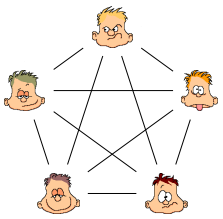
Ideal Broadcast



Standard Model

Players

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



Network

- Complete
- Synchronous
- Authenticated

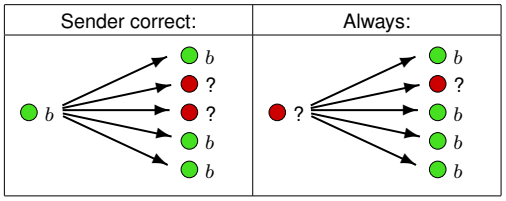
Adversary

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

Definition: Broadcast

Definition (Input x_1, Outputs $y_1, \ldots, y_n$)

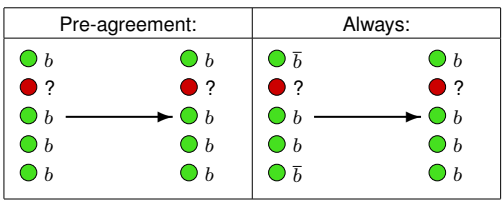
- **Consistency**: Every (correct) player receives the same output y.
- **Validity**: Sender correct $\Rightarrow$ every player receives output $y_i = x_1$.
- **Termination**: Every player eventually receives output.



Definition: Consensus

Definition (Inputs $x_1, \ldots, x_n$, Outputs $y_1, \ldots, y_n$)

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



Broadcast vs Consensus

Broadcast: $(x, \perp, \ldots, \perp) \to (y_1, \ldots, y_n)$

Consensus: $(x_1, \ldots, x_n) \to (y_1, \ldots, y_n)$

Consensus ⟶ Broadcast

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

Broadcast ⟶ Consensus

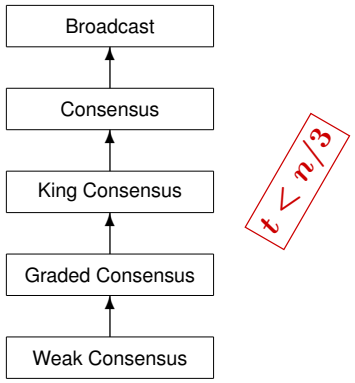
1. $\forall P_i$: Broadcast(x_i)
2. $\forall P_j$: return $y_j =$ majority of received x_i's

$t < n/2$

Known Results (Broadcast/Consensus)

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

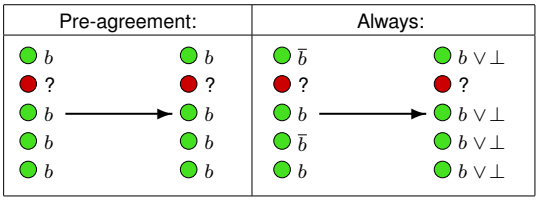
Road Map (w/o setup)



Definition: Weak Consensus

Definition (Inputs $x_1, \ldots, x_n$, Outputs $y_1, \ldots, y_n$)

- **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.



Protocol Weak Consensus

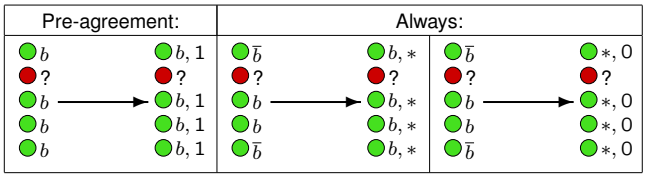
WeakConsensus$(x_1, \ldots, x_n) \to (y_1, \ldots, y_n)$

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: Graded Consensus

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

- **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.



Protocol Graded Consensus

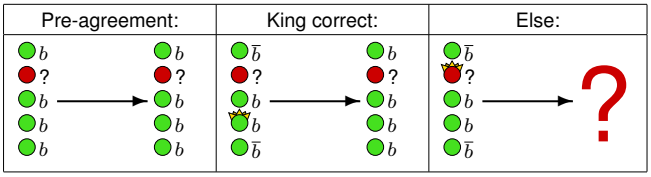
GradedConsensus$(x_1, \ldots, x_n) \to ((y_1, g_1), \ldots, (y_n, g_n))$

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

Definition: King Consensus

Definition (Inputs $x_1, \ldots, x_n$, Outputs $y_1, \ldots, y_n$)

- **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.



Protocols King Consensus (King P_k) and Consensus

KingConsensus$_k(x_1, \ldots, x_n) \to (y_1, \ldots, y_n)$

1. $((z_1, g_1), \ldots, (z_n, g_n)) =$ GradedConsensus$(x_1, \ldots, x_n)$
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

Consensus$(x_1, \ldots, x_n) \to (y_1, \ldots, y_n)$

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

Impossibility for 3 players, 1 corrupted