Ideal Broadcast
Real Broadcast
Real Broadcast
Standard Model

- **$n$ players:** \[ P = \{P_1, \ldots, P_n\} \]
- **Network:**
  - Complete
  - Synchronous
  - Pairwise
  - Authenticated
- **Adversary:**
  - Threshold $t$
  - Active (Byzantine)
  - Unlimited (unconditional 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.

<table>
<thead>
<tr>
<th>Sender correct:</th>
<th>Always:</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Diagram of sender correctness" /></td>
<td><img src="image" alt="Diagram of always" /></td>
</tr>
</tbody>
</table>
## 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.

<table>
<thead>
<tr>
<th>Pre-agreement:</th>
<th>Always:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b$</td>
<td>$b$</td>
</tr>
<tr>
<td>$\bullet$?</td>
<td>$\bullet$?</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
</tr>
<tr>
<td>$\bullet$?</td>
<td>$\bullet$?</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
</tr>
<tr>
<td>$\bullet$?</td>
<td>$\bullet$?</td>
</tr>
<tr>
<td>Setting</td>
<td>Condition</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>information-theoretic</td>
<td>$t &lt; n/3$</td>
</tr>
</tbody>
</table>
| cryptographic   | BC: $t < n$
                Cons: $t < n/2$ | [DS82]           |
| i.t., PKI       | BC: $t < n$
                Cons: $t < n/2$ | [PW92]           |
**Definition: Weak Consensus**

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

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

<table>
<thead>
<tr>
<th>Pre-agreement:</th>
<th>Always:</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Pre-agreement Diagram" /></td>
<td><img src="image" alt="Always Diagram" /></td>
</tr>
</tbody>
</table>
Protocol Weak Consensus

WeakConsensus\((x_1, \ldots, x_n) \rightarrow (y_1, \ldots, y_n)\)

1. \(\forall P_i\): send \(x_i\) to every \(P_j\)

2. \(\forall P_j\): \(y_j = \begin{cases} 
0 & \text{if } \#\text{Zeros} \geq n - t \\
1 & \text{if } \#\text{Ones} \geq n - t \\
\bot & \text{else}
\end{cases}\)

3. \(\forall P_j\): return \(y_j\)
**Definition: Graded Consensus**

**Definition**  \((\text{Inputs } x_1, \ldots, x_n, \text{ Outputs } (y_1, g_1), \ldots, (y_n, g_n))\)

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

<table>
<thead>
<tr>
<th>Pre-agreement:</th>
<th>Always:</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Pre-agreement Diagram" /></td>
<td><img src="image" alt="Always Diagram" /></td>
</tr>
</tbody>
</table>
Protocol Graded Consensus

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

1. \((z_1, \ldots, z_n) = \text{WeakConsensus}(x_1, \ldots, x_n)\)

2. \(\forall P_i: \) send \(z_i\) to every \(P_j\).

3. \(\forall P_j: \)

\[
\begin{align*}
y_j &= \begin{cases} 
0 & \text{if } \#\text{Zeros} \geq \#\text{Ones} \\
1 & \text{if } \#\text{Zeros} < \#\text{Ones}
\end{cases} \\
g_j &= \begin{cases} 
1 & \text{if } \#y_j's \geq n - t \\
0 & \text{else}
\end{cases}
\end{align*}
\]

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

<table>
<thead>
<tr>
<th>Pre-agreement:</th>
<th>King correct:</th>
<th>Else:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$b$</td>
</tr>
<tr>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$b$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$b$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$b$</td>
</tr>
</tbody>
</table>

- $b$ represents a correct input.
- $\bar{b}$ represents a correct output.
- ? represents an uncertain status.
- $\bullet$ indicates a player.
- $\odot$ indicates the King.

"?" is used to indicate an uncertain status, often used in the context of consensus problems to denote a player's uncertainty about the input or output, especially in the context of the King Consensus definition.
Protocol King Consensus (King $P_k$)

$\text{KingConsensus}_{k}(x_1, \ldots, x_n) \rightarrow (y_1, \ldots, y_n)$

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

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 $y_j$
Protocol Consensus / Broadcast

Consensus \((x_1, \ldots, x_n) \rightarrow (y_1, \ldots, y_n)\)

1. for \(k = 1\) to \(t + 1\) do
   \[(x_1, \ldots, x_n) = \text{KingConsensus}_k(x_1, \ldots, x_n)\]
   od

2. \(\forall P_j: \text{ return } x_j\)

Broadcast \((x, \bot, \ldots, \bot) \rightarrow (y_1, \ldots, y_n)\)

1. \(P_1: \text{ send } x \text{ to every } P_j, P_j \text{ receives } x_j\)

2. \((y_1, \ldots, y_n) = \text{Consensus}(x_1, \ldots, x_n)\)

3. \(\forall P_j: \text{ return } y_j\)
Impossibility for 3 players, 1 corrupted