**Cryptographic Protocols**

*Spring 2020*

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

**Broadcast vs Consensus**

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

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

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

**Broadcast → Consensus**
1. $\forall P_j$: Broadcast($x_i$)
2. $\forall P_j$: return $y_j = \text{majority of received } x_i$’s

$t < n/2$
Known Results (Broadcast/Consensus)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Condition</th>
<th>Literature</th>
</tr>
</thead>
<tbody>
<tr>
<td>information-theoretic</td>
<td>t &lt; n/3</td>
<td>[PSL80, BGP89]</td>
</tr>
<tr>
<td>cryptographic</td>
<td>BC: t &lt; n Cons: t &lt; n/2</td>
<td>[DS82]</td>
</tr>
<tr>
<td>i.t.</td>
<td>BC: t &lt; n Cons: t &lt; n/2</td>
<td>[PW92]</td>
</tr>
</tbody>
</table>

Road Map (w/o setup)

- Broadcast
- Consensus
- King Consensus
- Graded Consensus
- Weak Consensus

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 $P_i : y_i = y$.
- **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>$\top$</td>
</tr>
<tr>
<td>$?$</td>
<td>$?$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
</tr>
<tr>
<td>$b$</td>
<td>$\bot$</td>
</tr>
</tbody>
</table>

Protocol Weak Consensus

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

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 (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.

<table>
<thead>
<tr>
<th>Pre-agreement</th>
<th>Always:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b$</td>
<td>$b, 1$</td>
</tr>
<tr>
<td>$?$</td>
<td>$?$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
</tr>
<tr>
<td>$b$</td>
<td>$\bot$</td>
</tr>
</tbody>
</table>

Protocol Graded Consensus

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

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. $\forall P_j$: $y_j = \begin{cases} 0 & \text{if } \#\text{Zeros} \geq \#\text{Ones} \\ 1 & \text{if } \#\text{Zeros} < \#\text{Ones} \\ \bot & \text{else} \end{cases}$
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.

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

**Protocol King Consensus (King $P_k$)**

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

1. $((z_1, y_1), \ldots, (z_n, y_n)) = \text{GradedConsensus}(x_1, \ldots, x_n)$
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**

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

1. for $k = 1$ to $t + 1$:
   $(x_1, \ldots, x_n) = \text{KingConsensus}_k(x_1, \ldots, x_n)$
2. $\forall P^j$: return $x^j$

**Impossibility for 3 players, 1 corrupted**

\[ \begin{array}{ccc}
\varnothing & (1) & (2) \\
(1) & (1) & (1) \\
(2) & (2) & (2) \\
\end{array} \]