# On Broadcast in Generalized Network and Adversarial Models

Varun Maram

7th December 2020

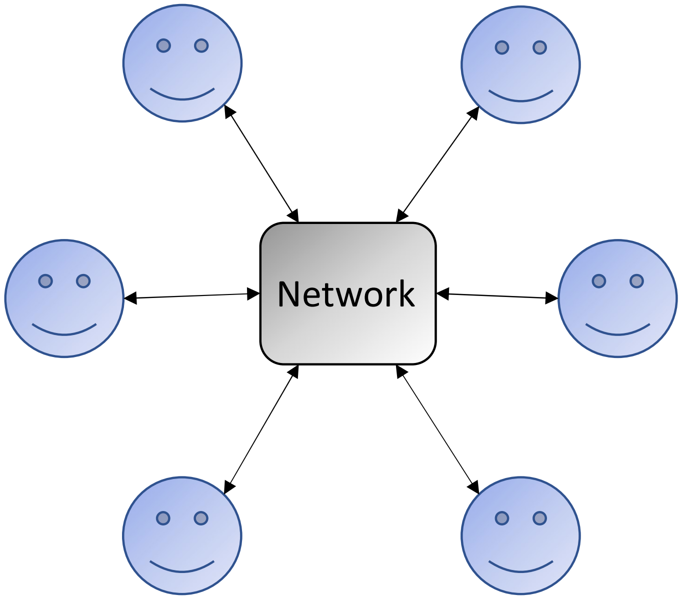
Joint work with Chen-Da Liu-Zhang and Ueli Maurer

Department of Computer Science, ETH Zurich

# Broadcast

## Setting

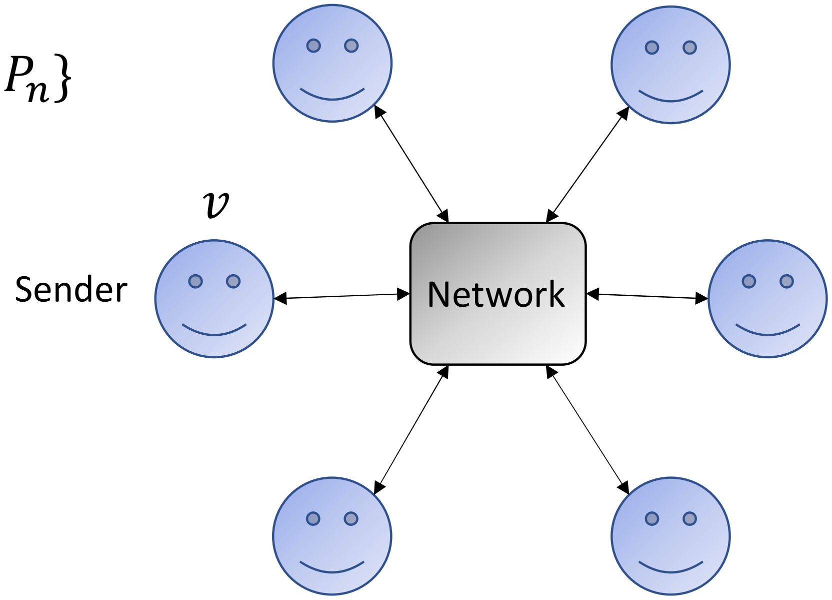
- Parties: $P = \{P_1, P_2, .., P_n\}$
- Synchronous
- No PKI setup



# Broadcast

## Setting

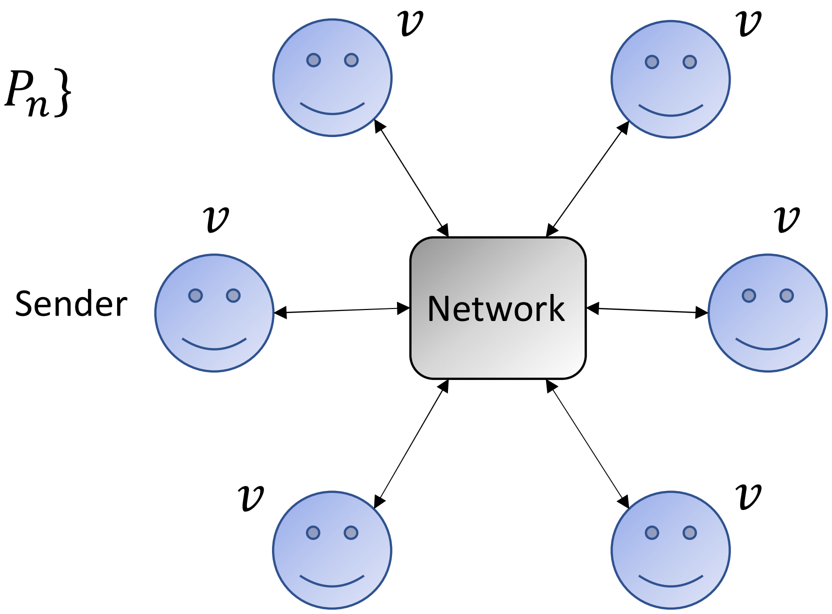
- Parties: $P = \{P_1, P_2, .., P_n\}$
- Synchronous
- No PKI setup



# Broadcast

## Setting

- Parties: $P = \{P_1, P_2, .., P_n\}$
- Synchronous
- No PKI setup



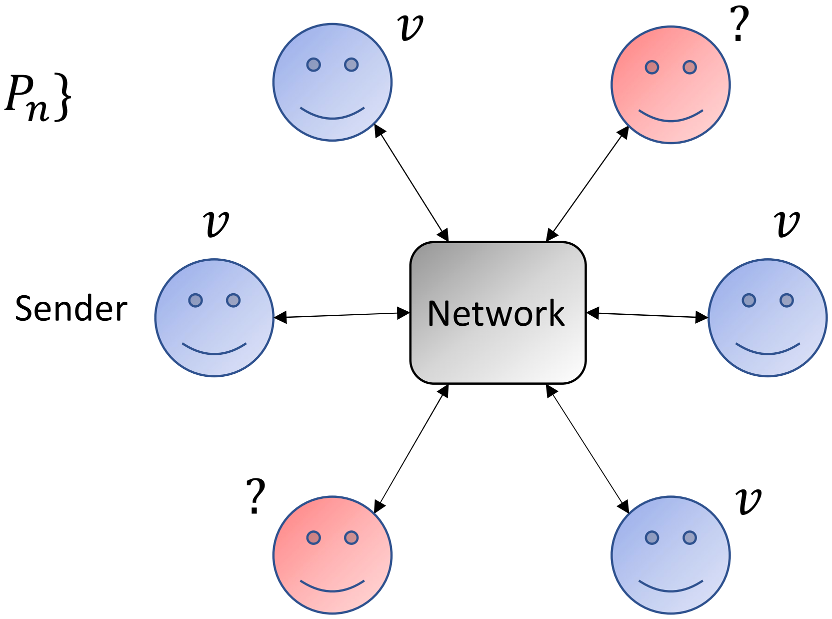
# Broadcast

## Setting

- Parties: $P = \{P_1, P_2, .., P_n\}$
- Synchronous
- No PKI setup

## Adversary

- Static
- Active (Byzantine)
- Unbounded



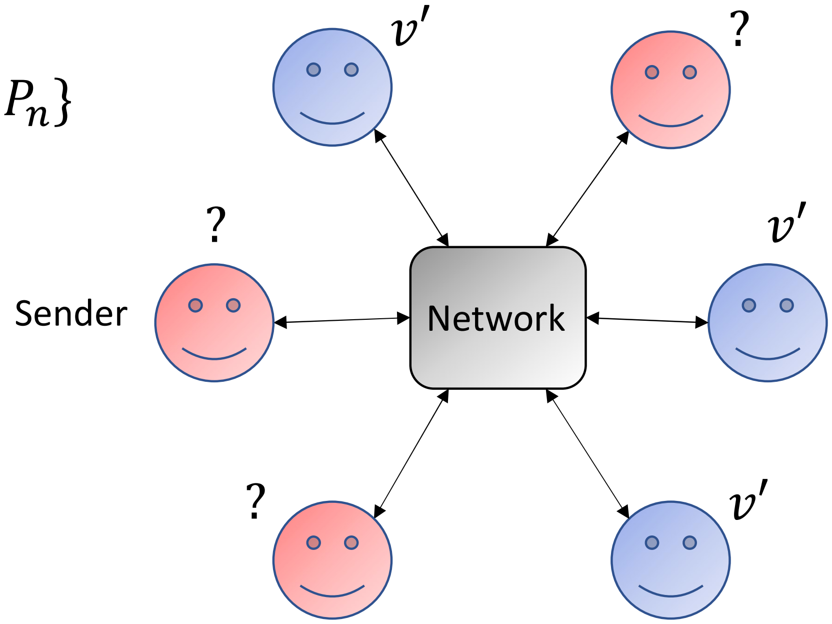
# Broadcast

## Setting

- Parties: $P = \{P_1, P_2, .., P_n\}$
- Synchronous
- No PKI setup

## Adversary

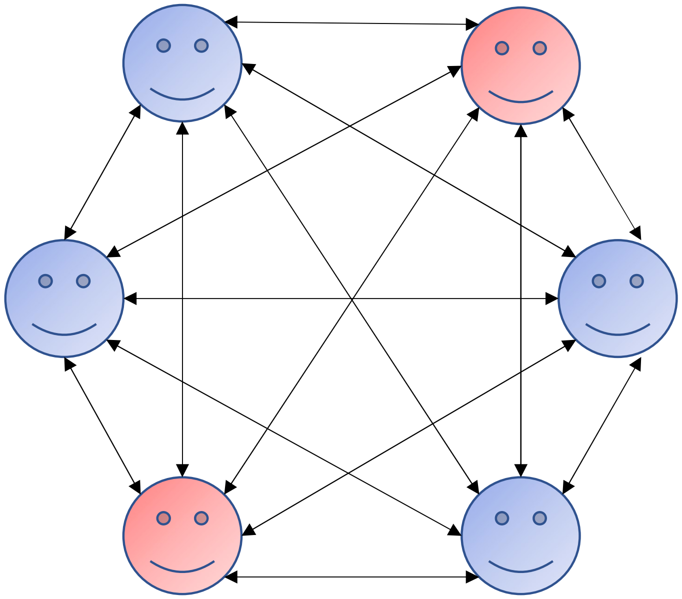
- Static
- Active (Byzantine)
- Unbounded



# Classical model

[PSL80]:

“Broadcast possible if and only if $t < n/3$”

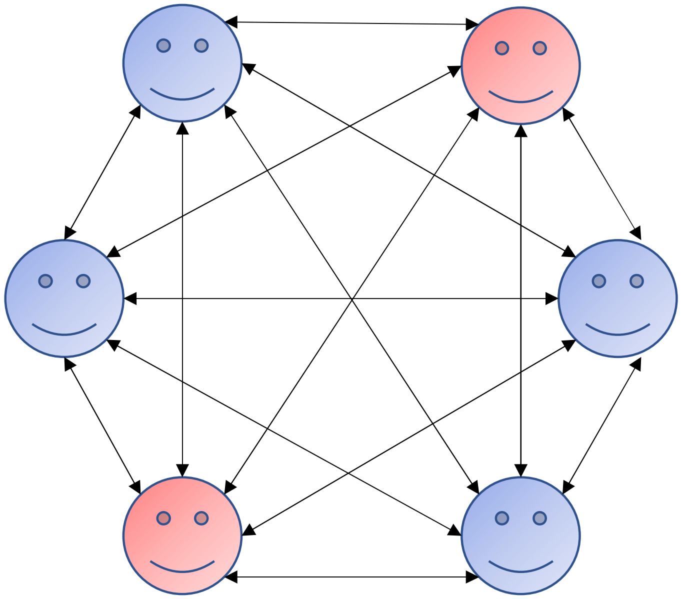


# Classical model

[PSL80]:

“Broadcast possible if and only if $t < n/3$”

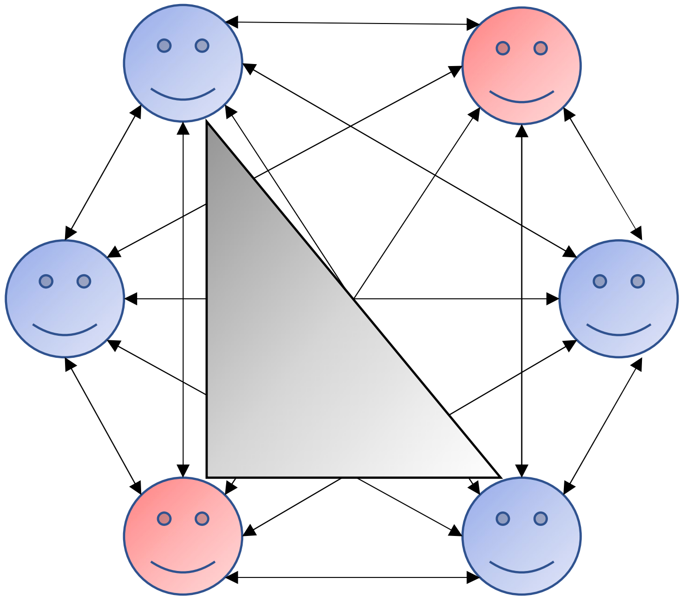
*Can we tolerate more?*



# 3-minicast model

[FM00]:

“Broadcast possible if and only if $t < n/2$”

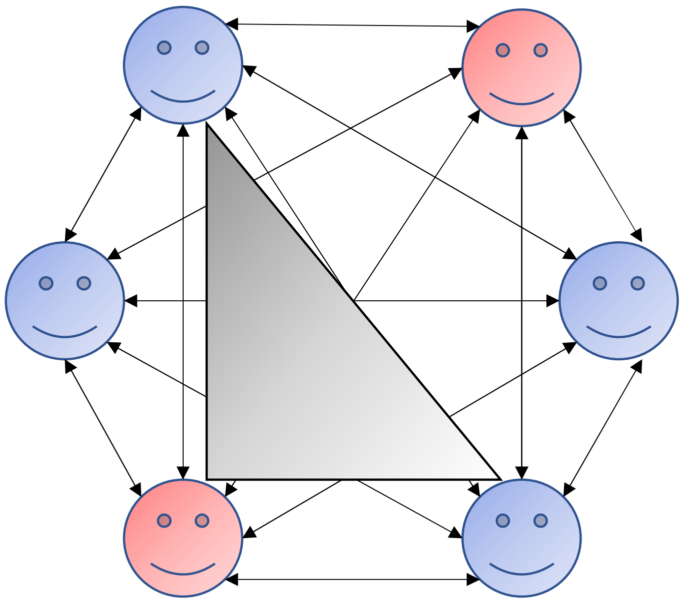


# 3-minicast model

[FM00]:

“Broadcast possible if and only if $t < n/2$”

*Trade-off b/w power of network and power of adversary?*



# Current literature

| Adversary structure | Network structure | Reference |
|---|---|---|
| $t < n/3$ | Bilateral channels | [PSL80] |
| $t < n/2$ | 3-minicast channels | [FM00] |

# Current literature

| Adversary structure | Network structure | Reference |
|---|---|---|
| $t < n/3$ | Bilateral channels | [PSL80] |
| $t < n/2$ | 3-minicast channels | [FM00] |
| $t < \frac{b-1}{b+1}n$ | *b*-minicast channels | [CFF$^+$05] |

# Current literature

Threshold:
$t < T$

| Adversary structure | Network structure | Reference |
|---|---|---|
| $t < \ n/3$ | Bilateral channels | [PSL80] |
| $t < n/2$ | 3-minicast channels | [FM00] |
| $t < \frac{b-1}{b+1}n$ | *b*-minicast channels | [CFF+05] |

# Current literature

| Adversary structure | Network structure | Reference |
|---|---|---|
| $t < n/3$ | Bilateral channels | [PSL80] |
| $t < n/2$ | 3-minicast channels | [FM00] |
| $t < \frac{b-1}{b+1}n$ | *b*-minicast channels | [CFF+05] |
| | | |
| $Q^{(3)}$ | Bilateral channels | [FM98] |

Threshold:
$t < T$

General:
$A = \{A_1, A_2, .., A_k\}$
$A_i \subseteq P$

# Current literature

| | Adversary structure | Network structure | Reference |
|---|---|---|---|
| Threshold:<br>$t < T$ | $t < n/3$ | Bilateral channels | [PSL80] |
| | $t < n/2$ | 3-minicast channels | [FM00] |
| | $t < \frac{b-1}{b+1}n$ | *b*-minicast channels | [CFF+05] |
| | | | |
| General:<br>$A = \{A_1, A_2, .., A_k\}$<br>$A_i \subseteq P$ | $Q^{(3)}$ | Bilateral channels | [FM98] |
| | $(b+1)$-chain free | *b*-minicast channels | [Ray15] |

# Current literature

| | Adversary structure | Network structure | Reference |
|---|---|---|---|
| Threshold:<br>$t < T$ | $t < n/3$ | Bilateral channels | [PSL80] |
| | $t < n/2$ | 3-minicast channels | [FM00] |
| | $t < \frac{b-1}{b+1} n$ | *b*-minicast channels | [CFF$^{+}$05] |
| | | | |
| General:<br>$A = \{A_1, A_2, .., A_k\}$<br>$A_i \subseteq P$ | $Q^{(3)}$ | Bilateral channels | [FM98] |
| | $(b+1)$-chain free | *b*-minicast channels | [Ray15] |

*What's left to be done?*

# Current literature

Complete!

| | Adversary structure | Network structure | Reference |
|---|---|---|---|
| Threshold:<br>$t < T$ | $t < n/3$ | Bilateral channels | [PSL80] |
| | $t < n/2$ | 3-minicast channels | [FM00] |
| | $t < \frac{b-1}{b+1} n$ | *b*-minicast channels | [CFF⁺05] |
| | | | |
| General:<br>$A = \{A_1, A_2, .., A_k\}$<br>$A_i \subseteq P$ | $Q^{(3)}$ | Bilateral channels | [FM98] |
| | $(b+1)$-chain free | *b*-minicast channels | [Ray15] |

*What's left to be done?*

# General networks

Threshold:
$t < T$

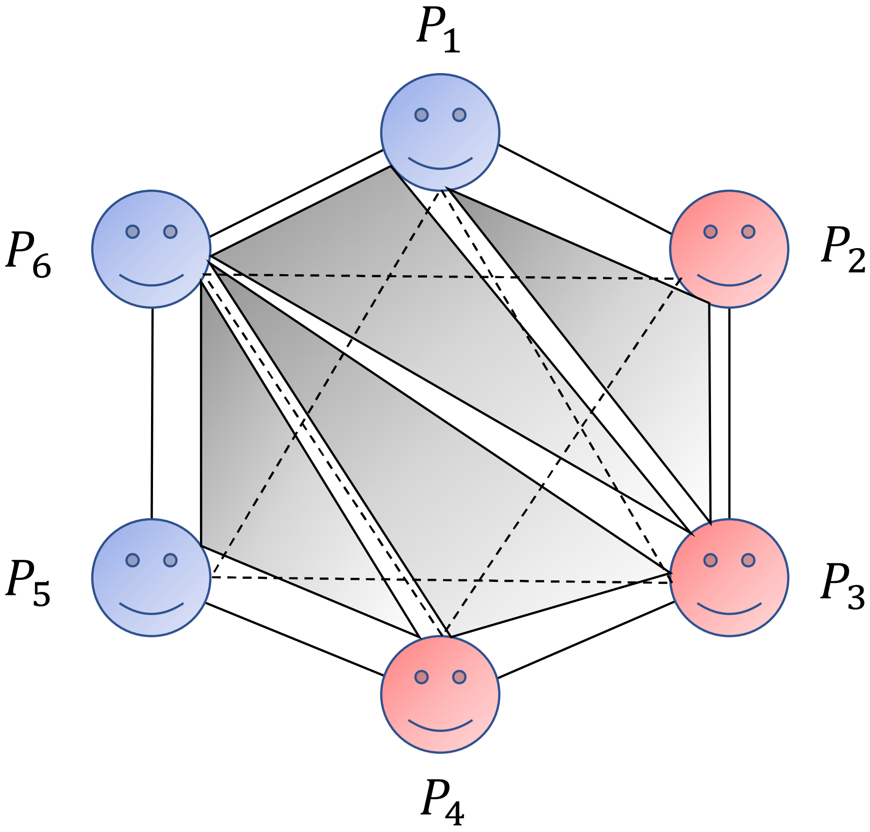
| Adversary structure | Network structure | Reference |
|---|---|---|
| $n/3 \leq t < n/2$ | Some 3-minicast channels | [RVS+04], [JMS12] |

# General networks

| | Adversary structure | Network structure | Reference |
|---|---|---|---|
| Threshold:<br>$t < T$ | $n/3 \leq t < n/2$ | Some 3-minicast channels | [RVS$^{+}$04], [JMS12] |
| | | | |
| General:<br>$A = \{A_1, A_2, .., A_k\}$<br>$A_i \subseteq P$ | $A$ contains $b$-chain(s) and $A$ is $(b + 1)$-chain free $\left(A \in \mathfrak{A}^{(b)}\right)$ | Some $b$-minicast channels | [LMM20] |

# Example

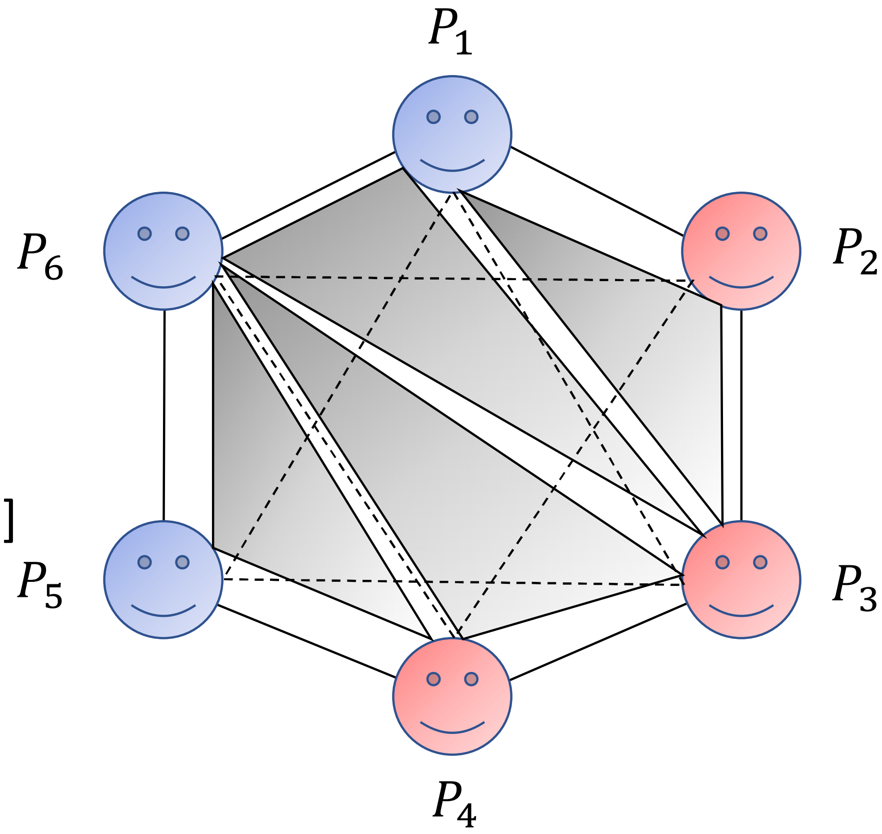
- 3-minicast model
- Six parties
- $t \leq 3$



# Example

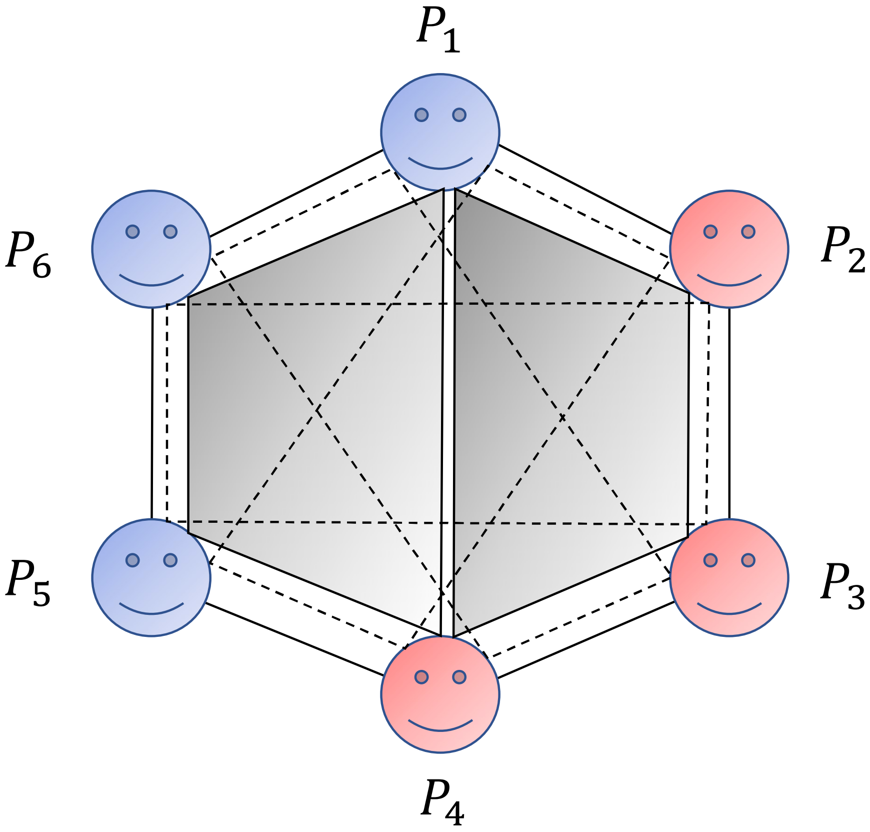
- 3-minicast model
- Six parties
- $t \leq 3$

- Broadcast is impossible [CFF+05]



# Example

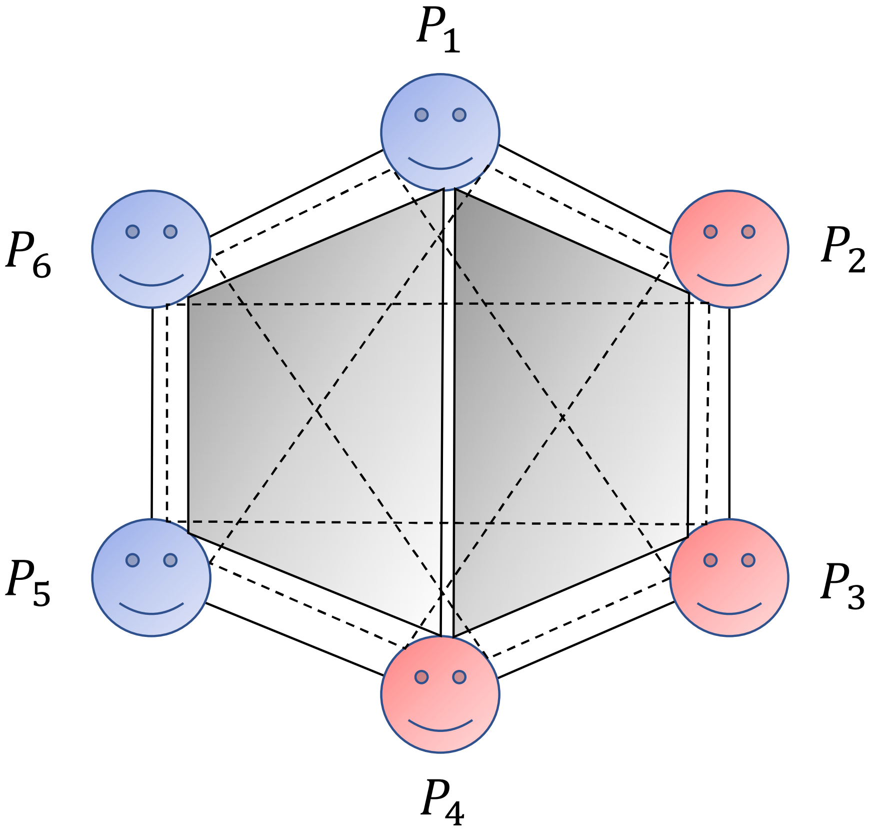
- 4-minicast model
- Six parties
- $t \leq 3$



# Example

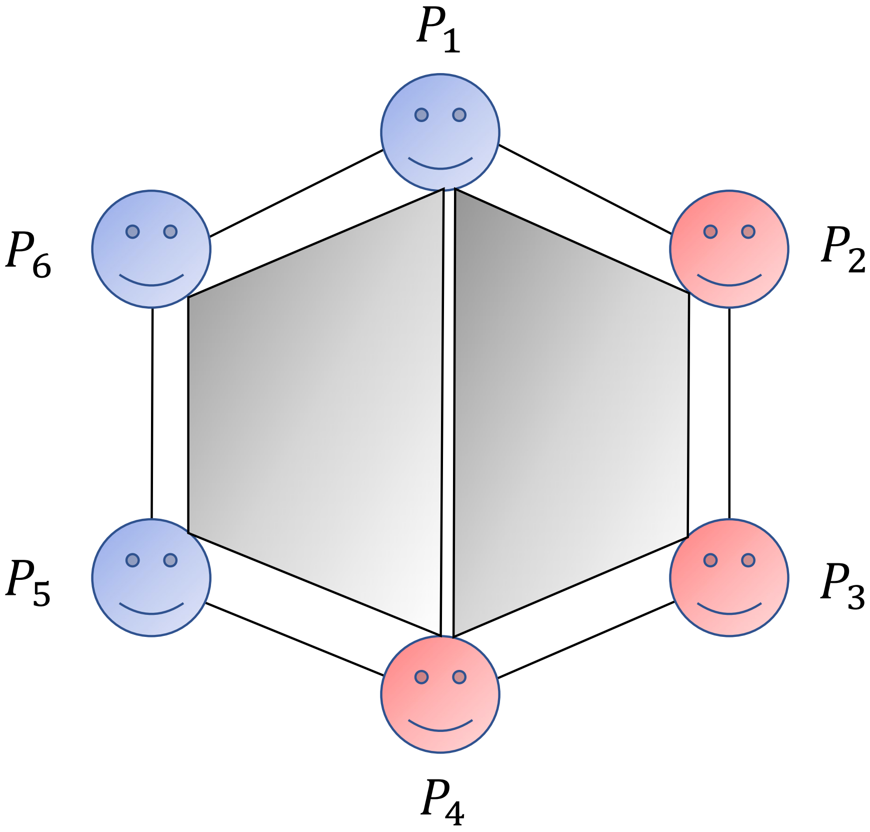
- 4-minicast model
- Six parties
- $t \leq 3$

- Broadcast is possible [CFF+05]



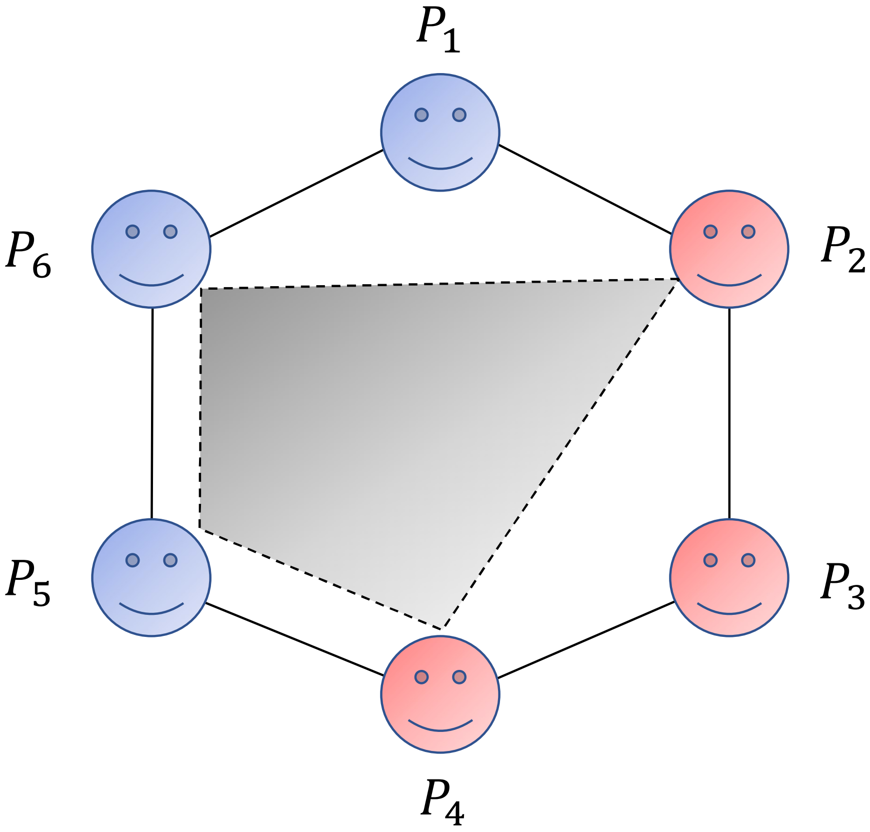
# Example

- Some 4-minicast channels
- Six parties
- $t \leq 3$



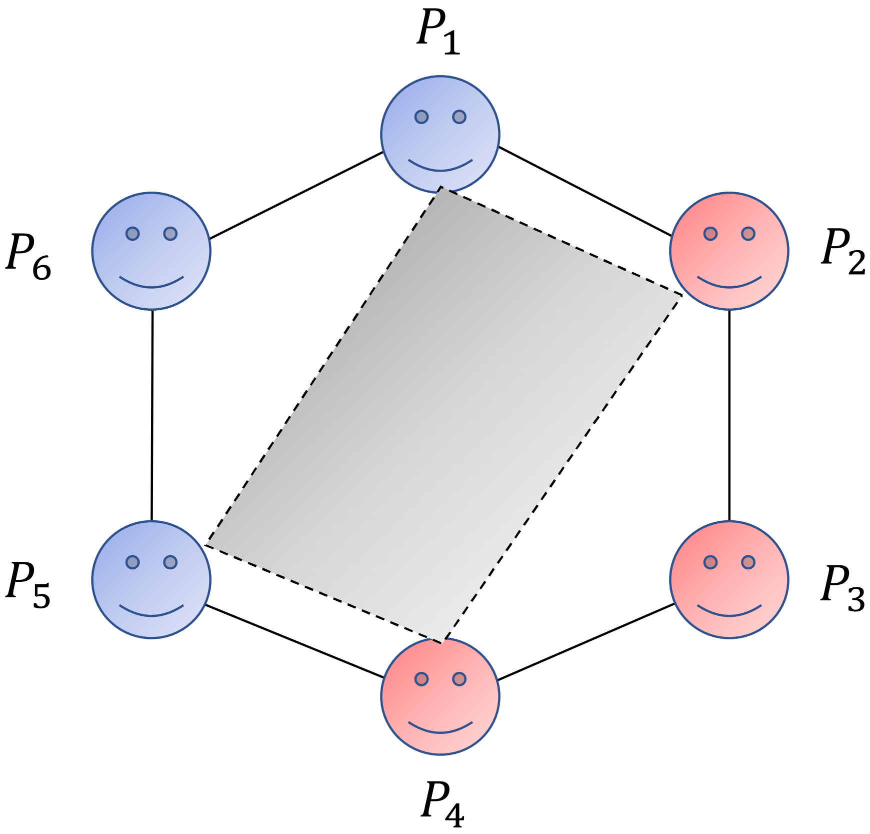
# Example

- Some 4-minicast channels
- Six parties
- $t \leq 3$



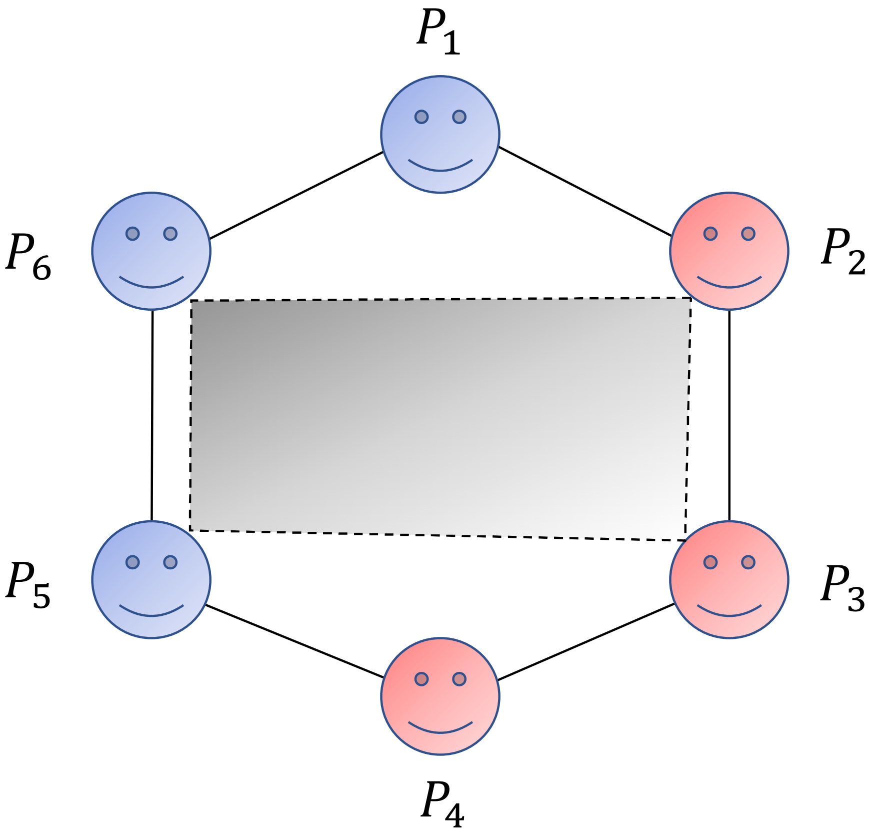
# Example

- Some 4-minicast channels
- Six parties
- $t \leq 3$



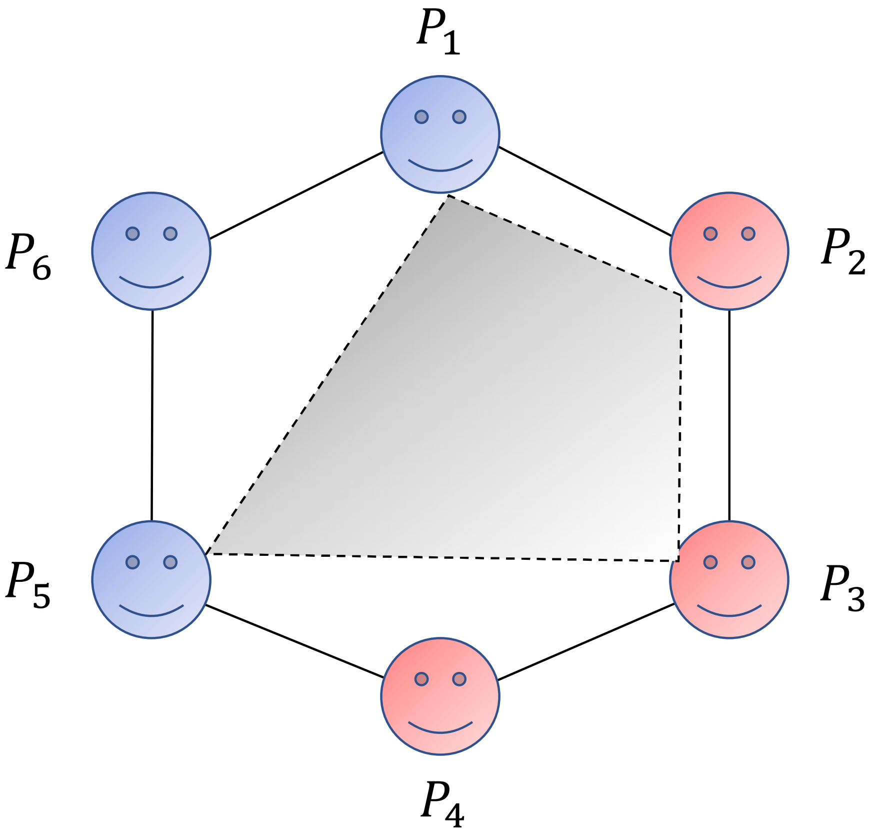
# Example

- Some 4-minicast channels
- Six parties
- $t \leq 3$



# Example

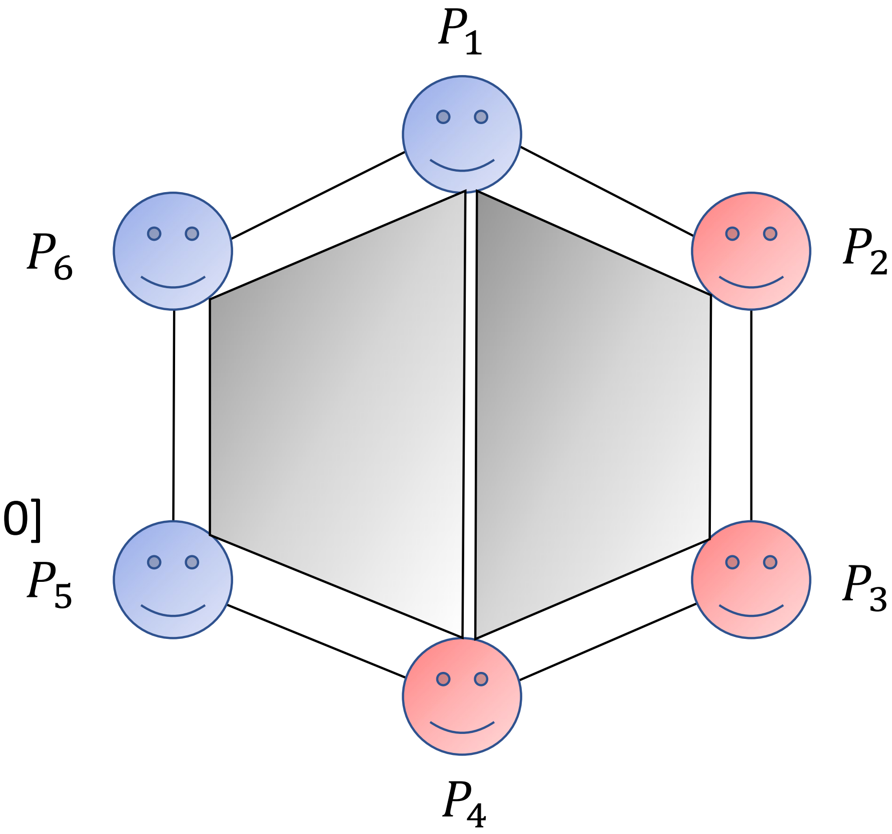
- Some 4-minicast channels
- Six parties
- $t \leq 3$



# Example

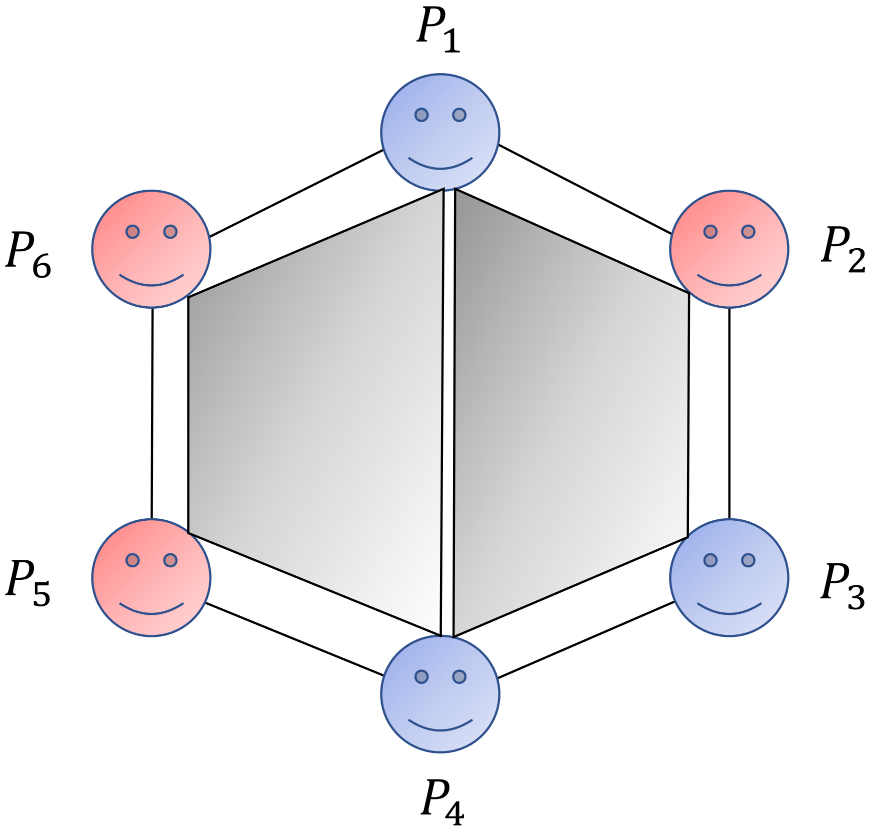
- Some 4-minicast channels
- Six parties
- $t \leq 3$

- Broadcast is impossible [LMM20]



# Example

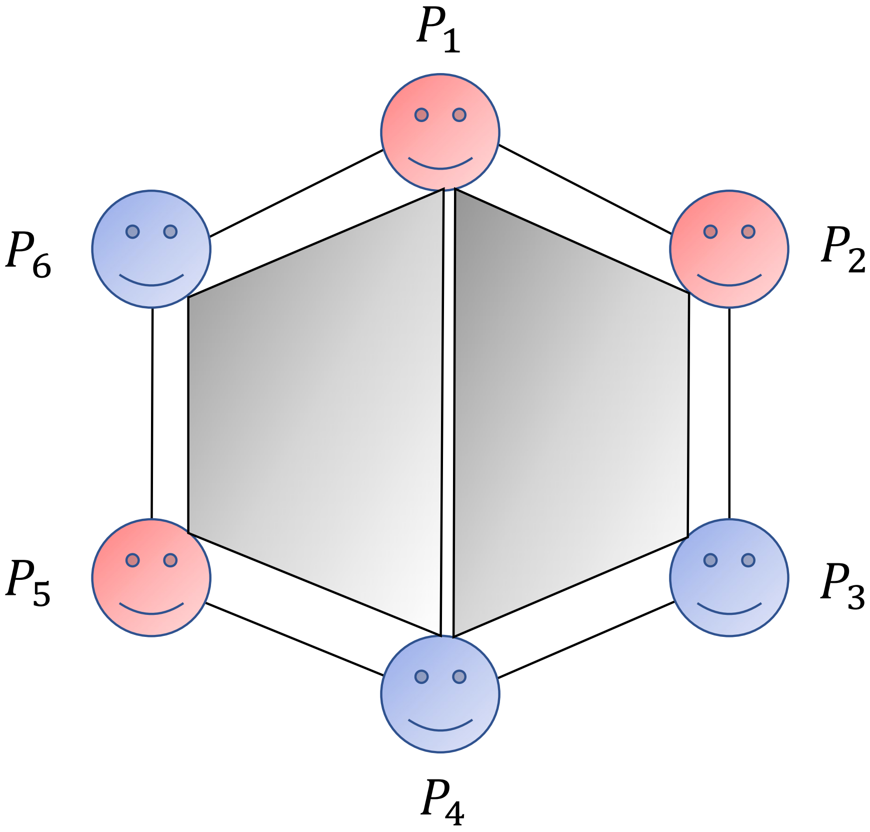
- Some 4-minicast channels
- Six parties
- $A = \{A_1, A_2, .., A_k\}$
  $(|A_i| = 3)$



# Example

- Some 4-minicast channels
- Six parties
- $A = \{A_1, A_2, .., A_k\}$

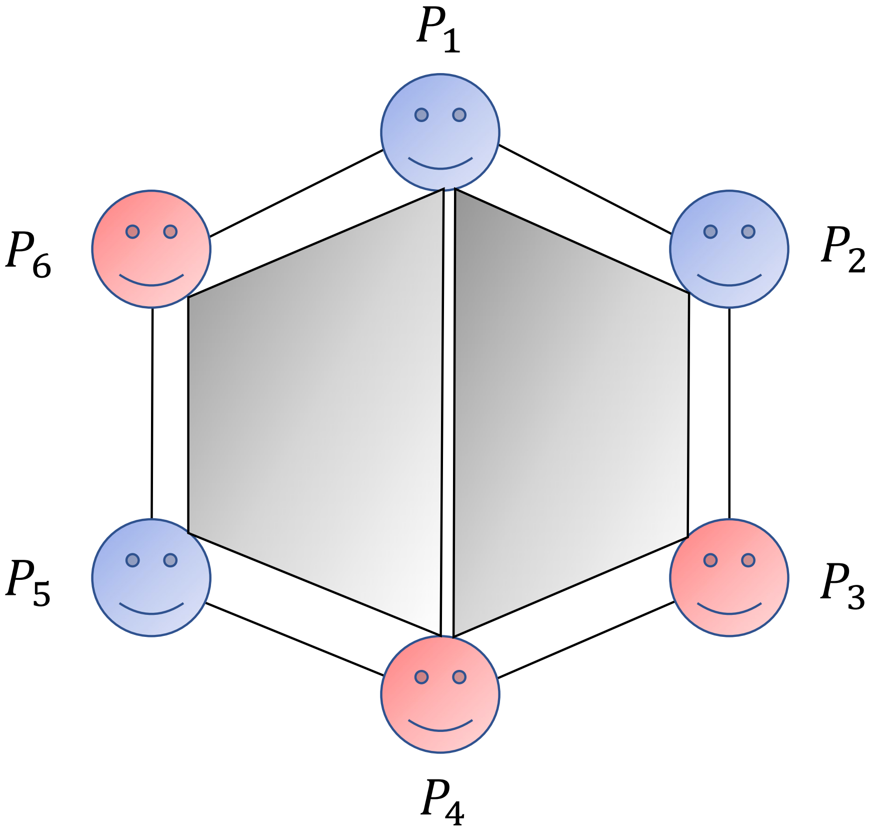
  $(|A_i| = 3)$



# Example

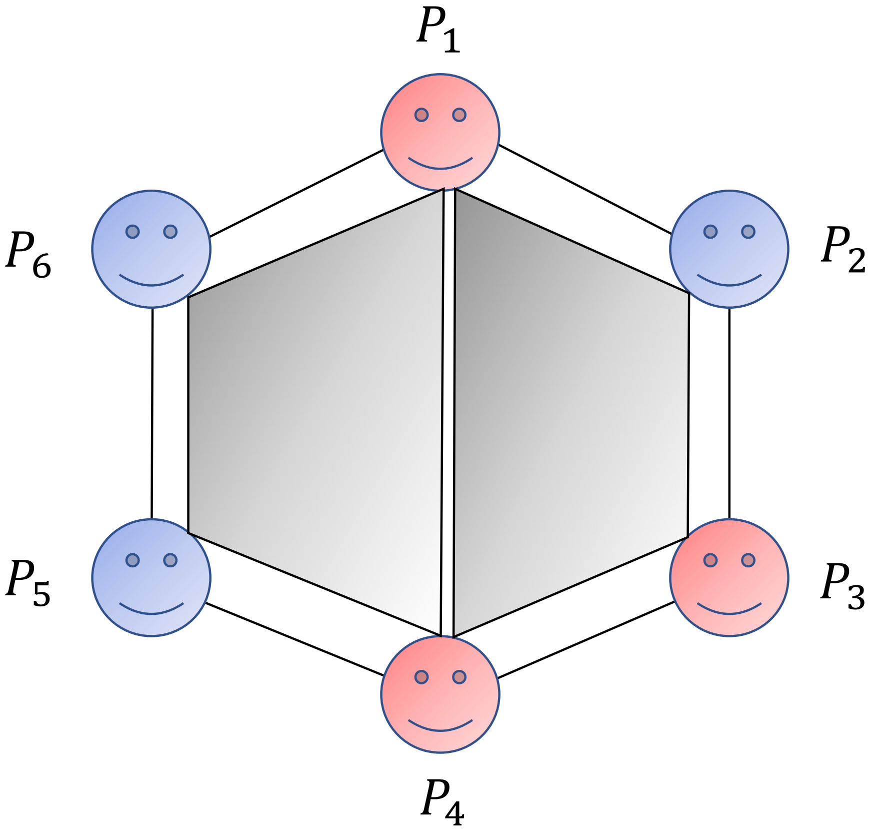
- Some 4-minicast channels
- Six parties
- $A = \{A_1, A_2, .., A_k\}$

  $(|A_i| = 3)$



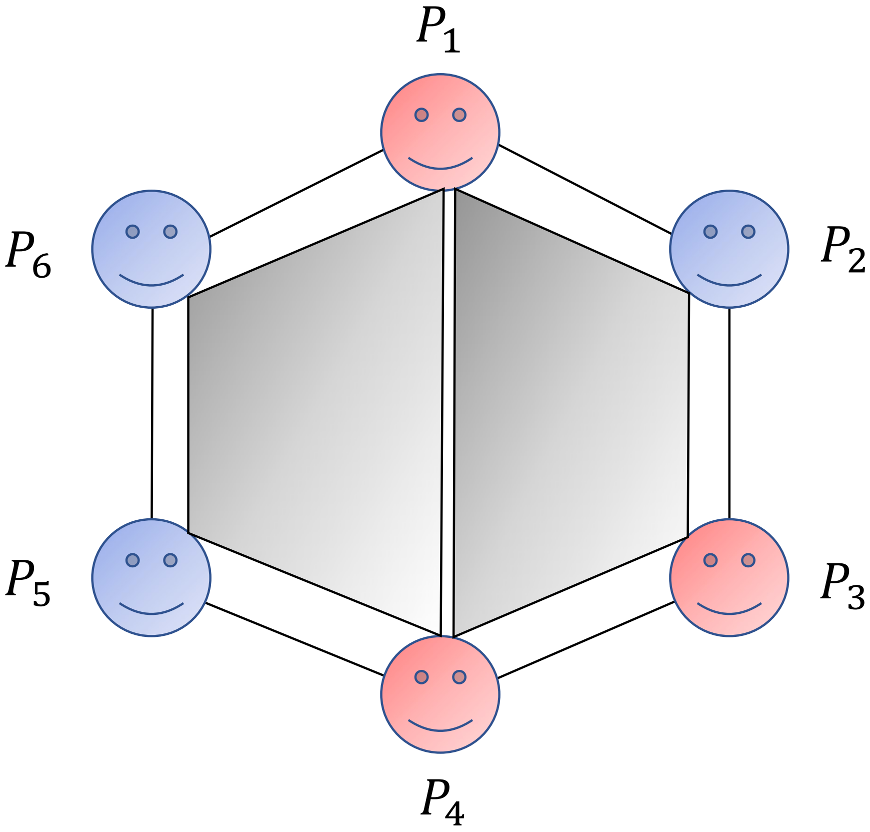
# Example

- Some 4-minicast channels
- Six parties
- $A = \{A_1, A_2, .., A_k\}$
  $(|A_i| = 3)$

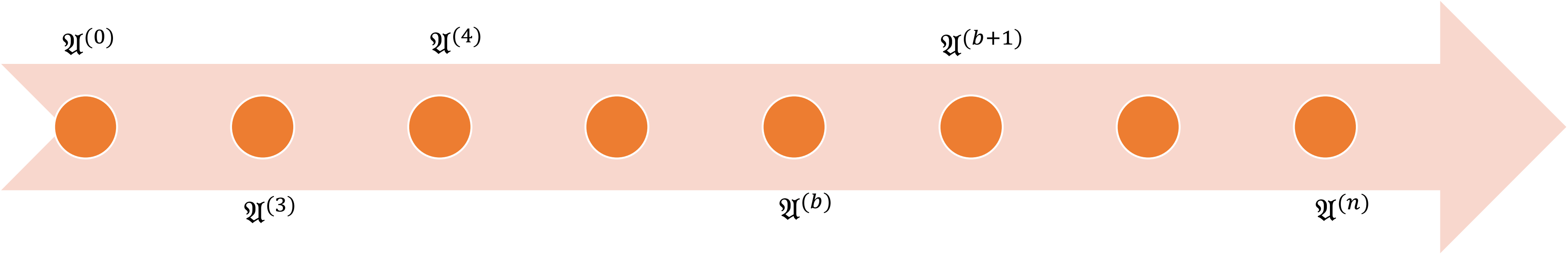


# Example

- Some 4-minicast channels
- Six parties
- $A = \{A_1, A_2, .., A_k\}$
  $(|A_i| = 3)$
- Broadcast is possible [LMM20]



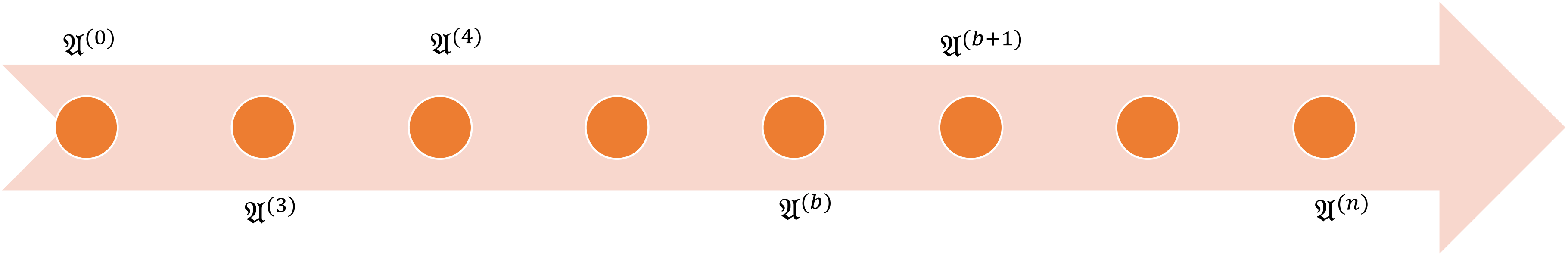
# Overview



$\left(A \in \mathfrak{A}^{(0)}\right)$: $A$ is 3-chain free

$\left(A \in \mathfrak{A}^{(b)}\right)$: $A$ contains $b$-chain(s) and $A$ is $(b+1)$-chain free, for $3 \leq b \leq n$

# Overview

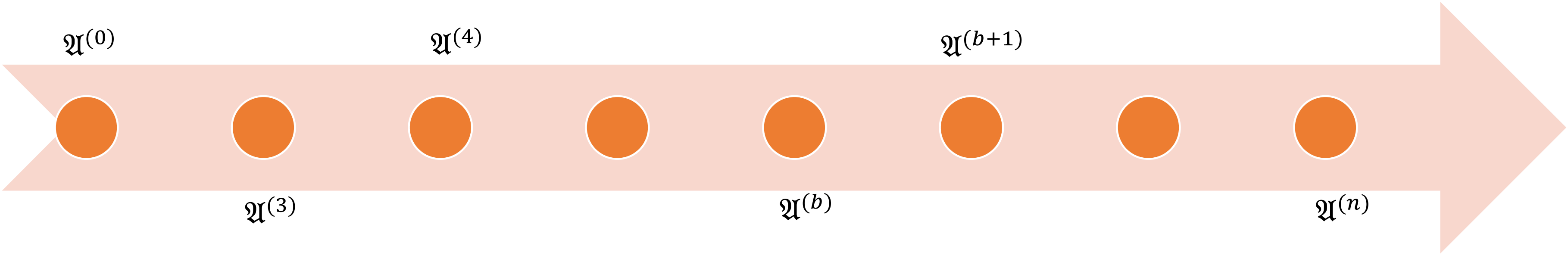


$\left(A \in \mathfrak{A}^{(0)}\right)$: $A$ is 3-chain free

$\left(A \in \mathfrak{A}^{(b)}\right)$: $A$ contains $b$-chain(s) and $A$ is $(b+1)$-chain free, for $3 \leq b \leq n$

$A$ is $b$-chain free $\Longrightarrow$ $A$ is $(b+1)$-chain free

# Overview



$\mathfrak{A}^{(0)}$

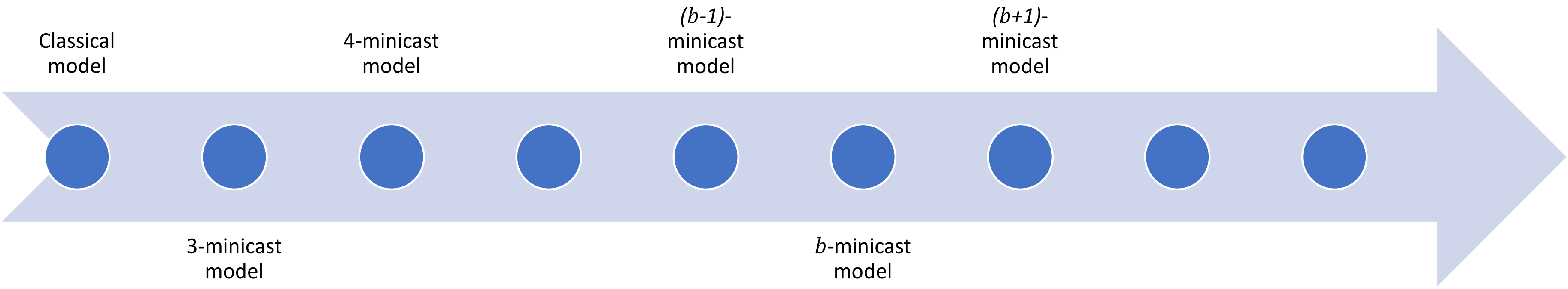
$\mathfrak{A}^{(3)}$

$\mathfrak{A}^{(4)}$

$\mathfrak{A}^{(b)}$

$\mathfrak{A}^{(b+1)}$

$\mathfrak{A}^{(n)}$



Classical model

3-minicast model

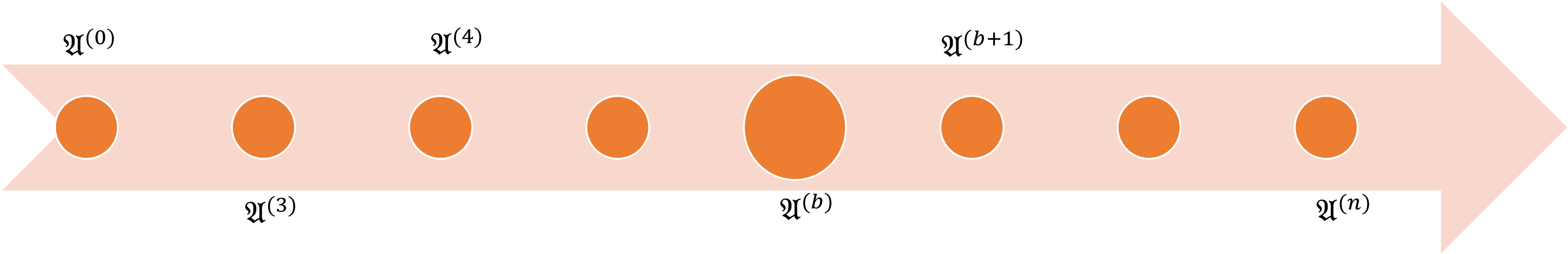
4-minicast model

*(b-1)*-minicast model

*b*-minicast model

*(b+1)*-minicast model

# Overview



$\mathfrak{A}^{(0)}$

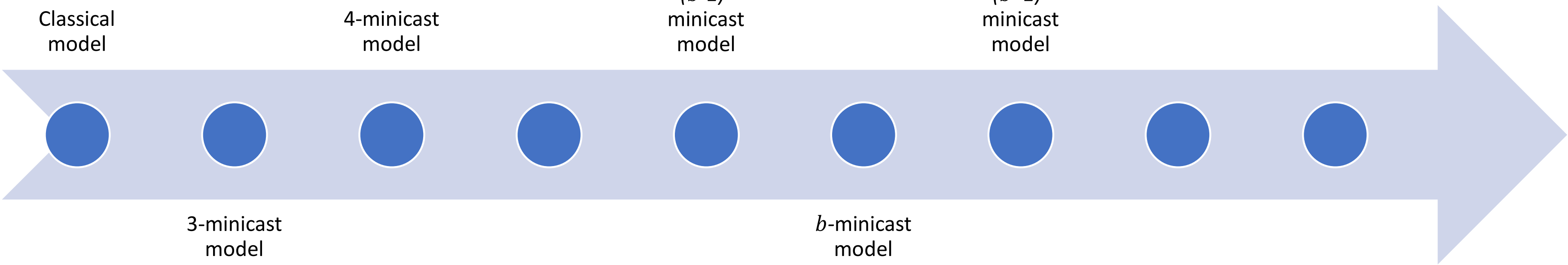
$\mathfrak{A}^{(3)}$

$\mathfrak{A}^{(4)}$

$\mathfrak{A}^{(b)}$

$\mathfrak{A}^{(b+1)}$

$\mathfrak{A}^{(n)}$



Classical model

3-minicast model

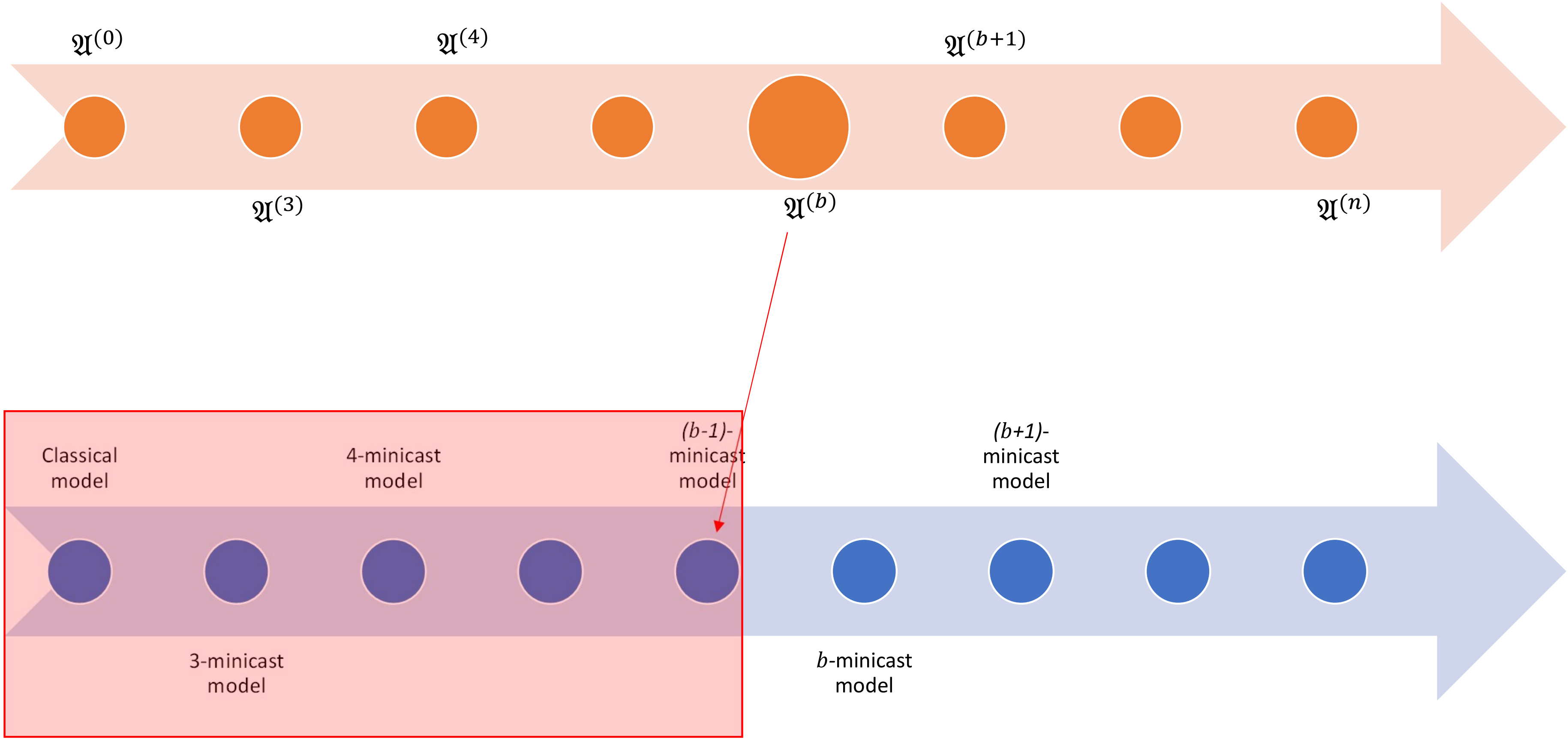
4-minicast model

*(b-1)*-minicast model

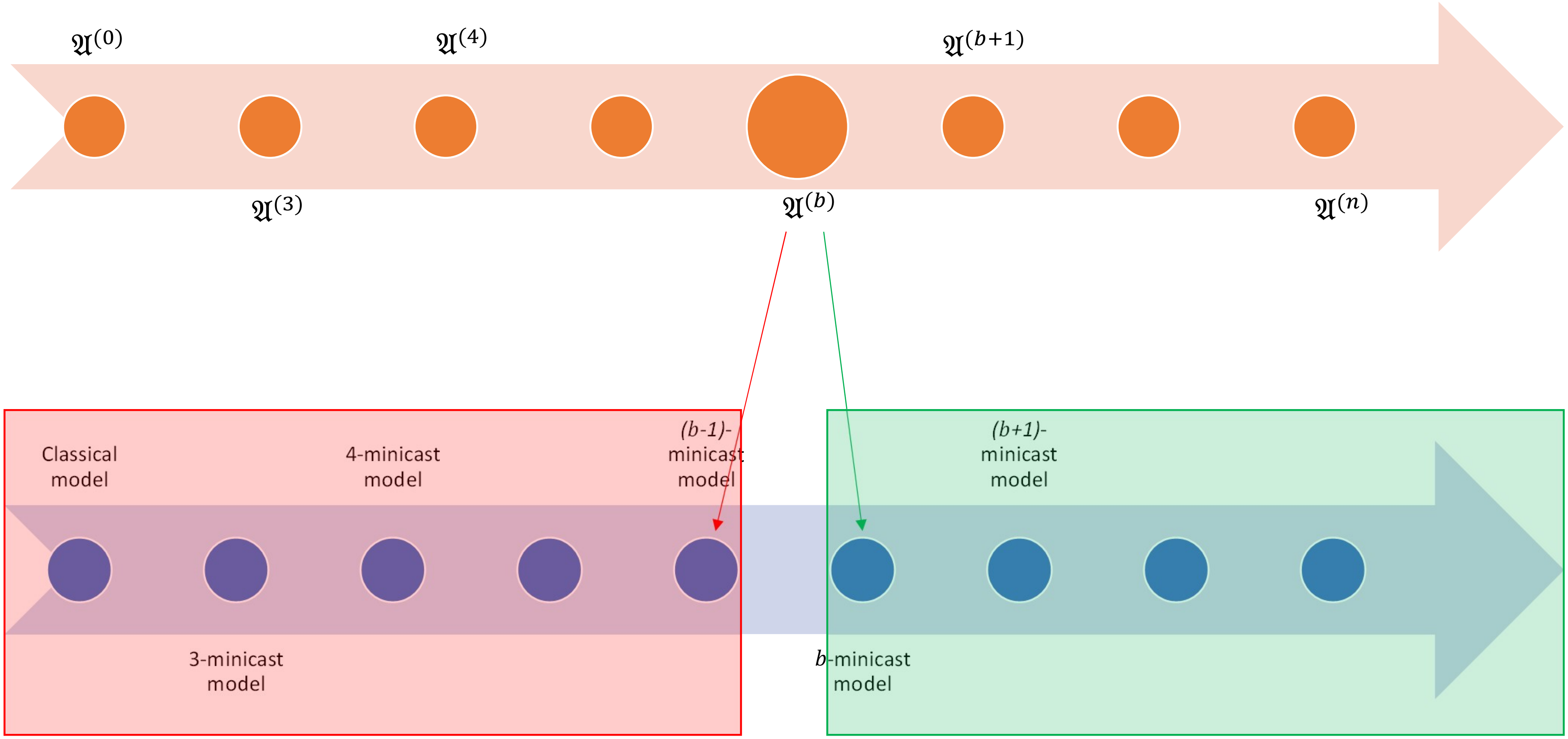
*b*-minicast model

*(b+1)*-minicast model

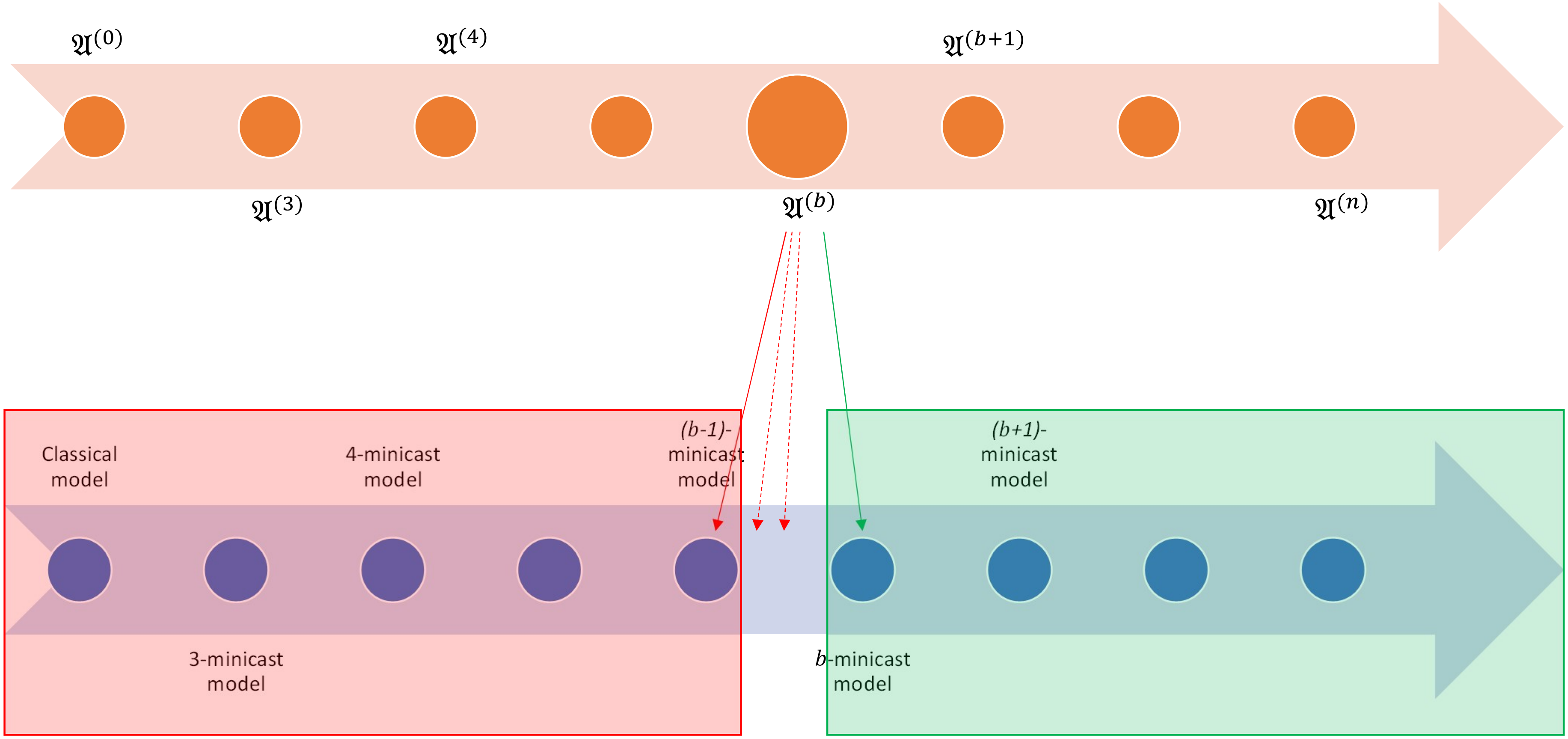
# Overview


$\mathfrak{A}^{(0)}$
$\mathfrak{A}^{(4)}$
$\mathfrak{A}^{(b+1)}$
$\mathfrak{A}^{(3)}$
$\mathfrak{A}^{(b)}$
$\mathfrak{A}^{(n)}$
Classical model
4-minicast model
*(b-1)*-minicast model
*(b+1)*-minicast model
3-minicast model
*b*-minicast model

# Overview

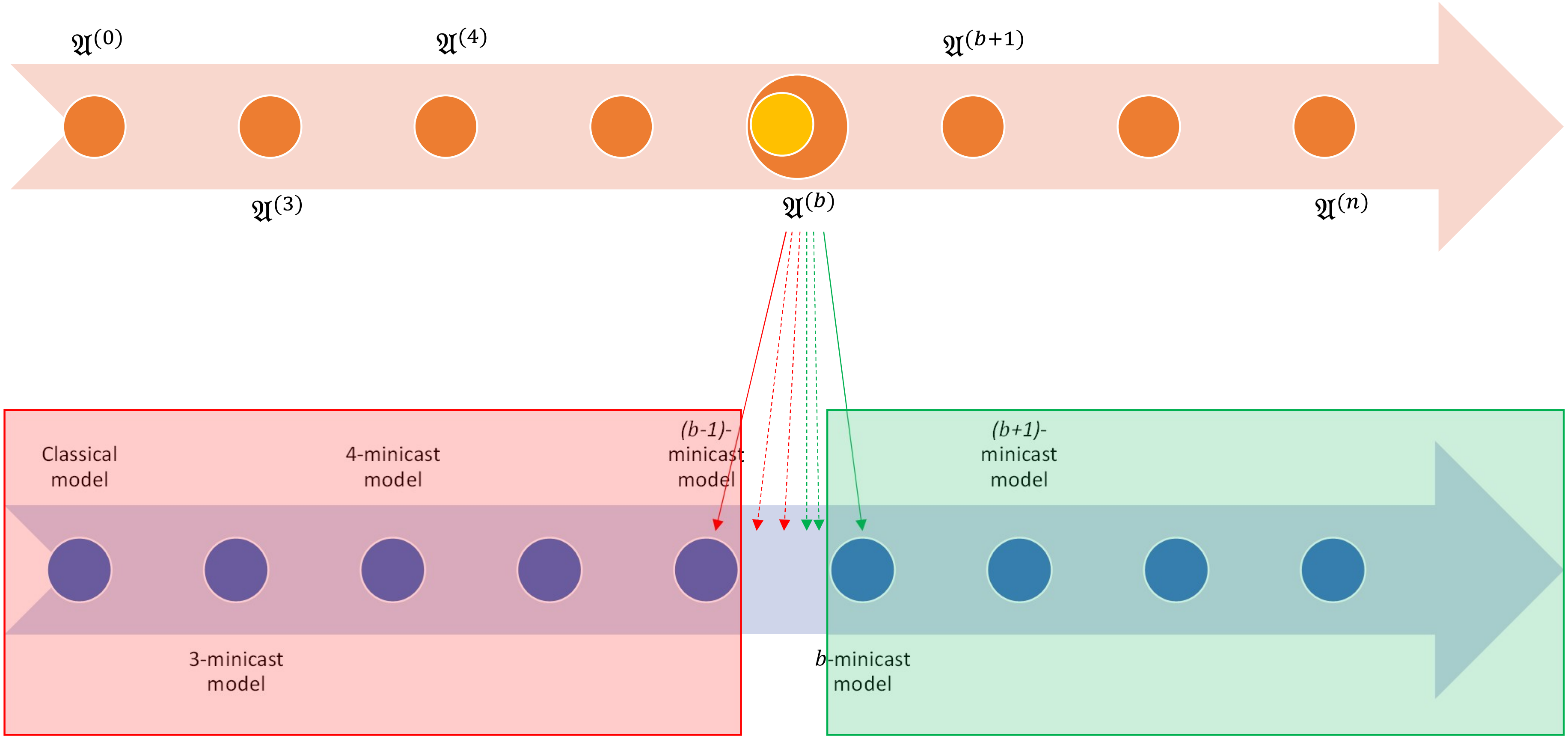

$\mathfrak{A}^{(0)}$
$\mathfrak{A}^{(4)}$
$\mathfrak{A}^{(b+1)}$
$\mathfrak{A}^{(3)}$
$\mathfrak{A}^{(b)}$
$\mathfrak{A}^{(n)}$
Classical model
4-minicast model
*(b-1)*-minicast model
*(b+1)*-minicast model
3-minicast model
$b$-minicast model

# Overview



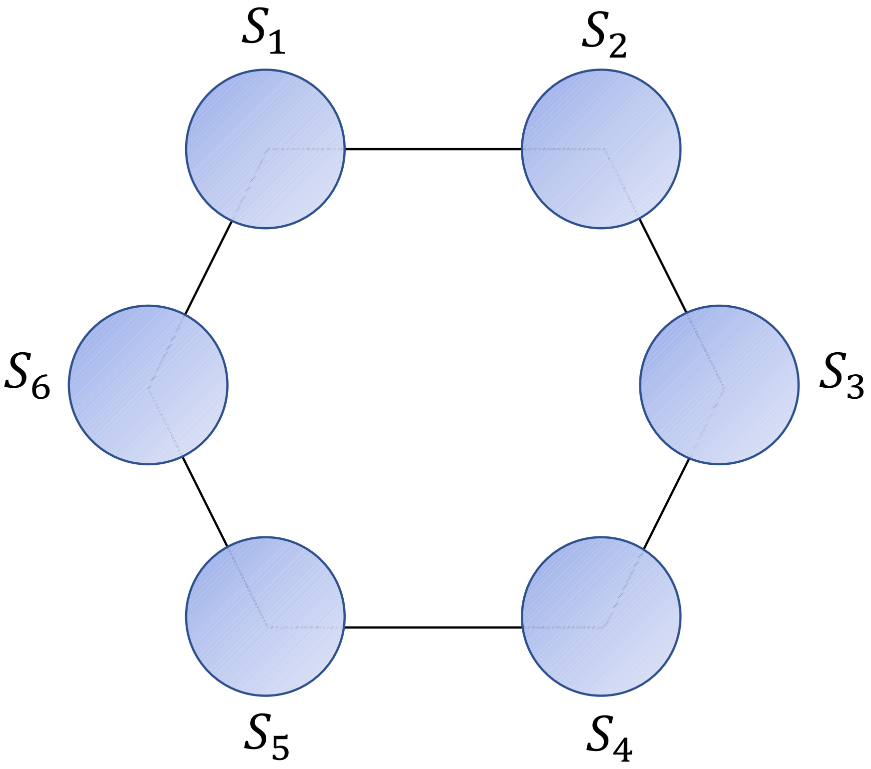
$\mathfrak{A}^{(0)}$
$\mathfrak{A}^{(4)}$
$\mathfrak{A}^{(b+1)}$
$\mathfrak{A}^{(3)}$
$\mathfrak{A}^{(b)}$
$\mathfrak{A}^{(n)}$
Classical model
4-minicast model
*(b-1)*-minicast model
*(b+1)*-minicast model
3-minicast model
$b$-minicast model

# Overview


$\mathfrak{A}^{(0)}$
$\mathfrak{A}^{(4)}$
$\mathfrak{A}^{(b+1)}$
$\mathfrak{A}^{(3)}$
$\mathfrak{A}^{(b)}$
$\mathfrak{A}^{(n)}$
Classical model
4-minicast model
*(b-1)*-minicast model
*(b+1)*-minicast model
3-minicast model
*b*-minicast model

# Chain conditions

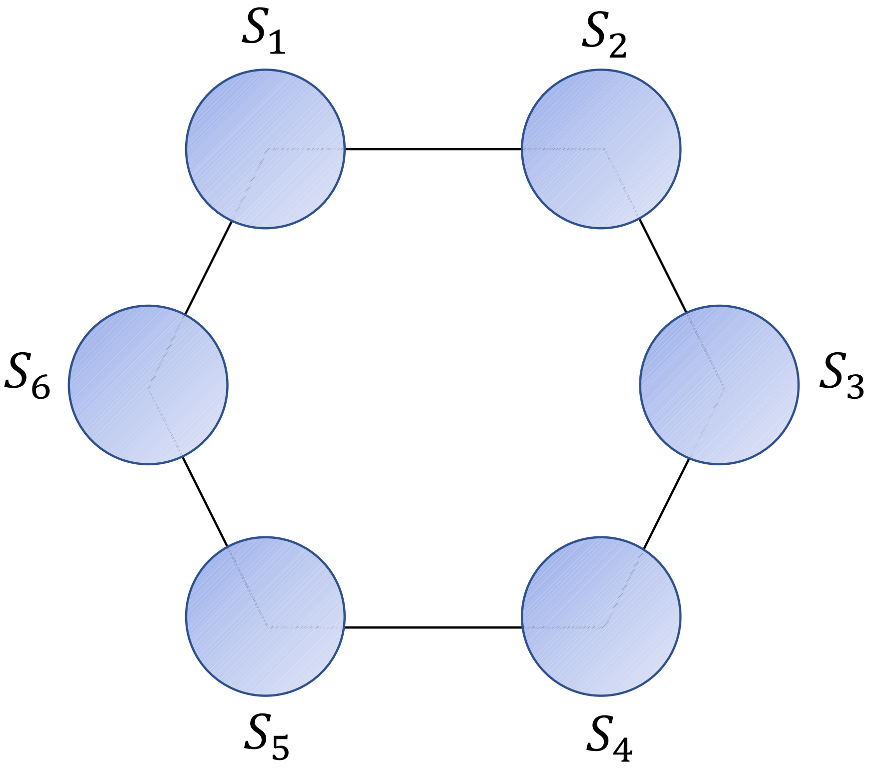
- Parties: $P = \{P_1, P_2, .., P_n\}$
- General: $A = \{A_1, A_2, .., A_k\}$, $A_i \subseteq P$



# Chain conditions

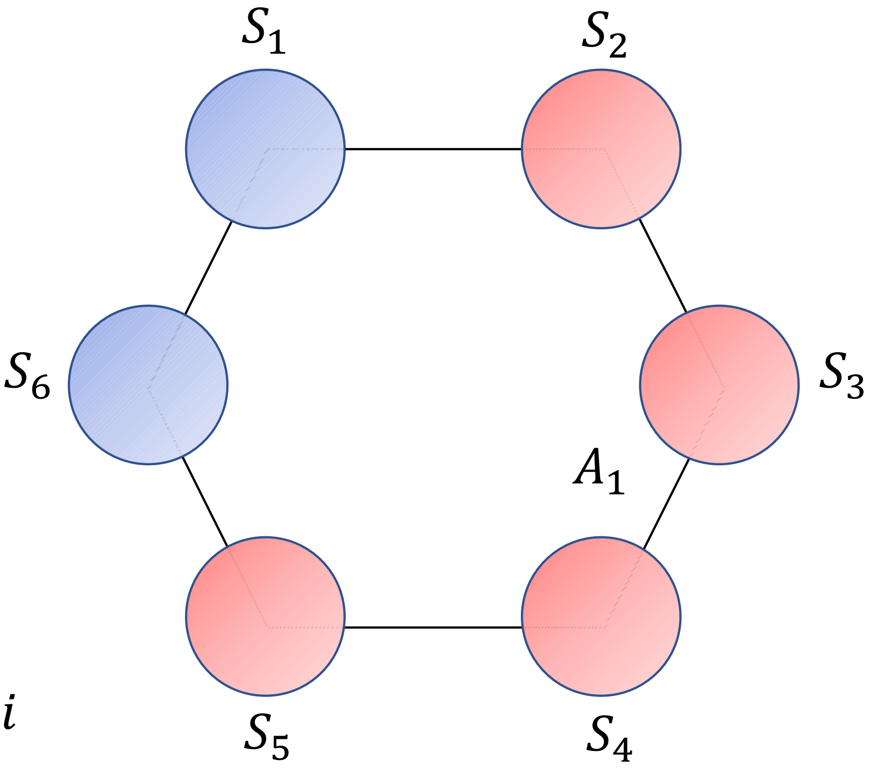
- Parties: $P = \{P_1, P_2, .., P_n\}$
- General: $A = \{A_1, A_2, .., A_k\}$,
  $A_i \subseteq P$

- Partition: $S = (S_1, S_2, .., S_b)$
  - $\cup_{i=1}^{b} S_i = P$
  - $S_i \cap S_j = \emptyset$
  - non-empty $S_i$'s



# Chain conditions

- Parties: $P = \{P_1, P_2, .., P_n\}$
- General: $A = \{A_1, A_2, .., A_k\}$,
  $A_i \subseteq P$
- Partition: $S = (S_1, S_2, .., S_b)$
  - $\bigcup_{i=1}^{b} S_i = P$
  - $S_i \cap S_j = \emptyset$
  - non-empty $S_i$'s
- $P \setminus (S_i \cup S_{i+1}) \in A$, for every $i$

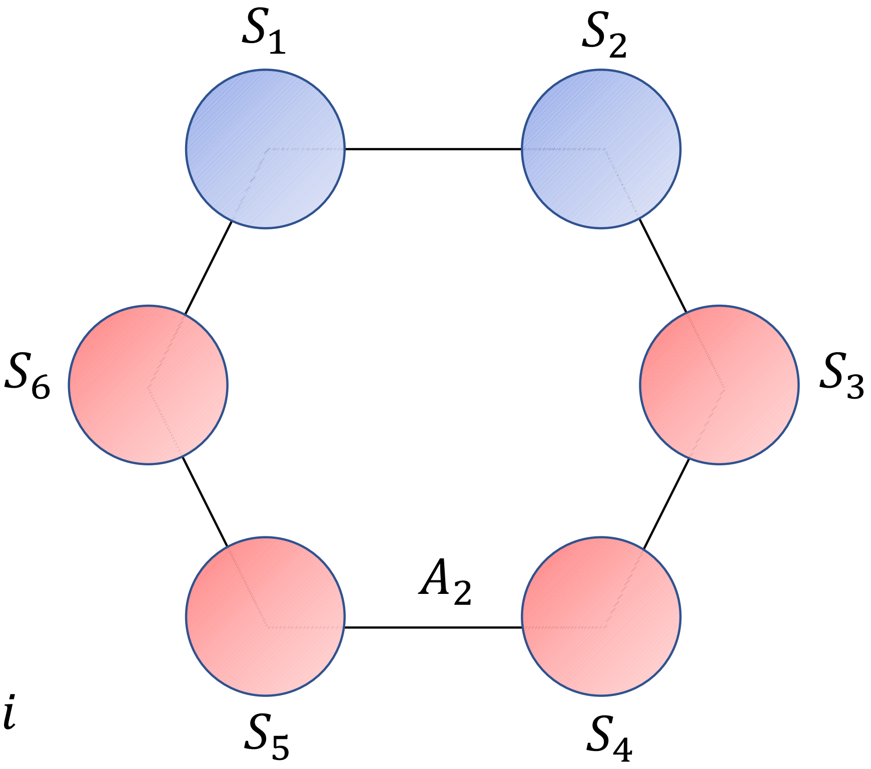


# Chain conditions

- Parties: $P = \{P_1, P_2, .., P_n\}$
- General: $A = \{A_1, A_2, .., A_k\}$,
  $A_i \subseteq P$

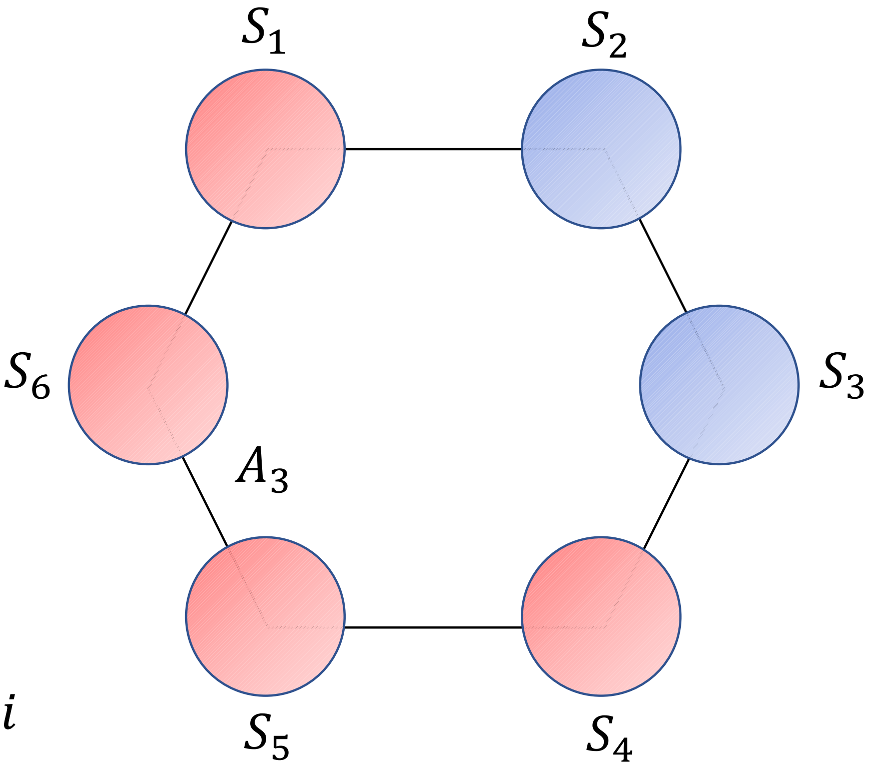
- Partition: $S = (S_1, S_2, .., S_b)$
  - $\cup_{i=1}^{b} S_i = P$
  - $S_i \cap S_j = \emptyset$
  - non-empty $S_i$'s

- $P \setminus (S_i \cup S_{i+1}) \in A$, for every $i$



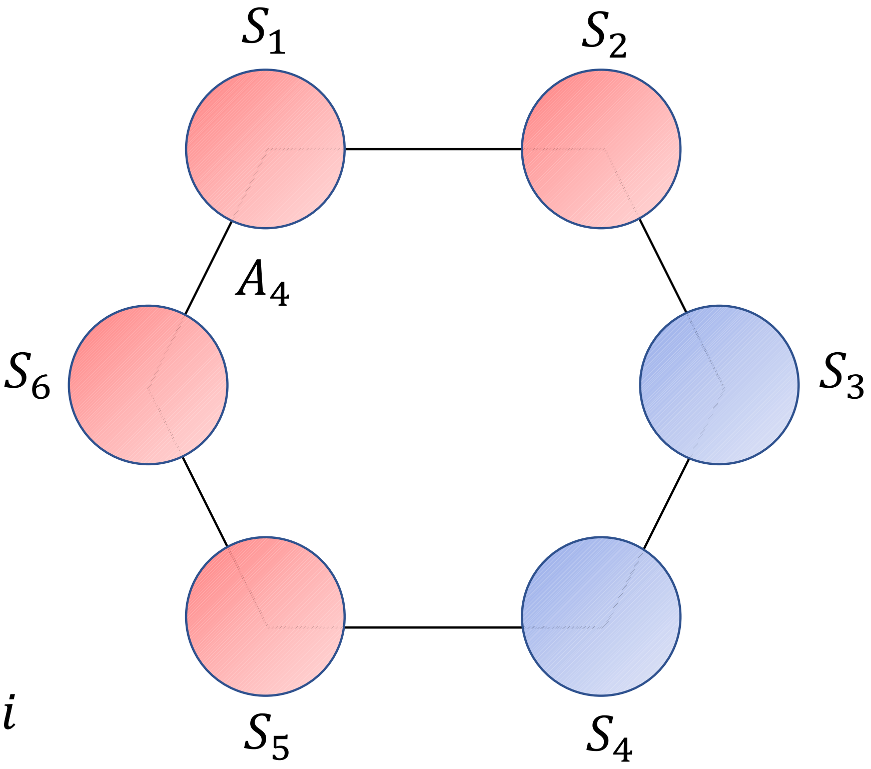
# Chain conditions

- Parties: $P = \{P_1, P_2, .., P_n\}$
- General: $A = \{A_1, A_2, .., A_k\}$,
  $A_i \subseteq P$
- Partition: $S = (S_1, S_2, .., S_b)$
  - $\cup_{i=1}^{b} S_i = P$
  - $S_i \cap S_j = \emptyset$
  - non-empty $S_i$'s
- $P \setminus (S_i \cup S_{i+1}) \in A$, for every $i$



# Chain conditions

- Parties: $P = \{P_1, P_2, .., P_n\}$
- General: $A = \{A_1, A_2, .., A_k\}$,
  $A_i \subseteq P$
- Partition: $S = (S_1, S_2, .., S_b)$
  - $\bigcup_{i=1}^{b} S_i = P$
  - $S_i \cap S_j = \emptyset$
  - non-empty $S_i$'s
- $P \setminus (S_i \cup S_{i+1}) \in A$, for every $i$

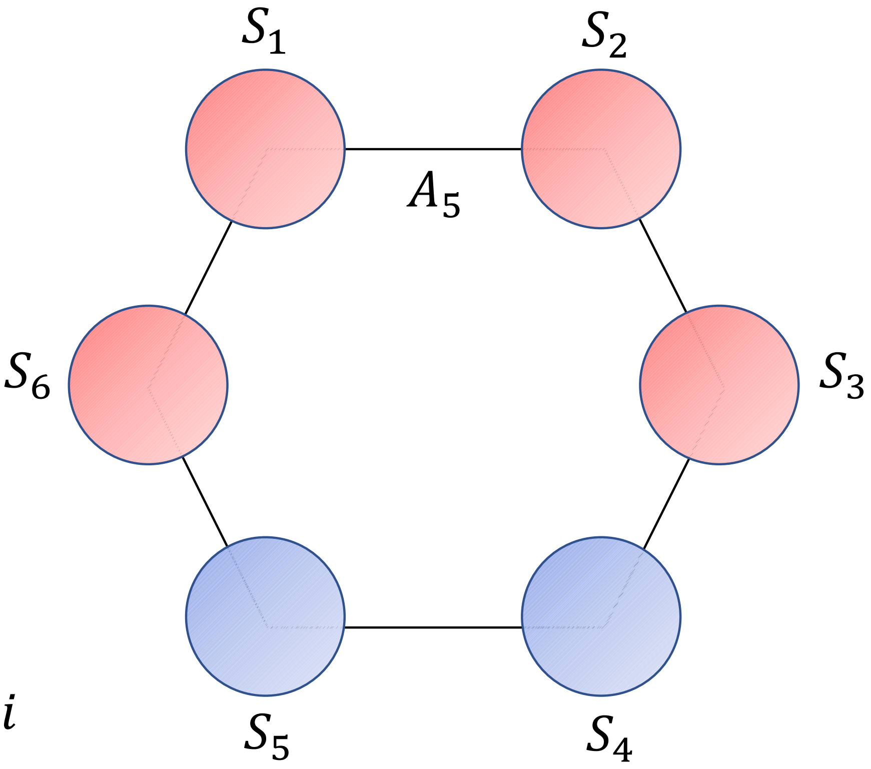


# Chain conditions

- Parties: $P = \{P_1, P_2, .., P_n\}$
- General: $A = \{A_1, A_2, .., A_k\}$, $A_i \subseteq P$

- Partition: $S = (S_1, S_2, .., S_b)$
  - $\cup_{i=1}^{b} S_i = P$
  - $S_i \cap S_j = \emptyset$
  - non-empty $S_i$'s

- $P \setminus (S_i \cup S_{i+1}) \in A$, for every $i$

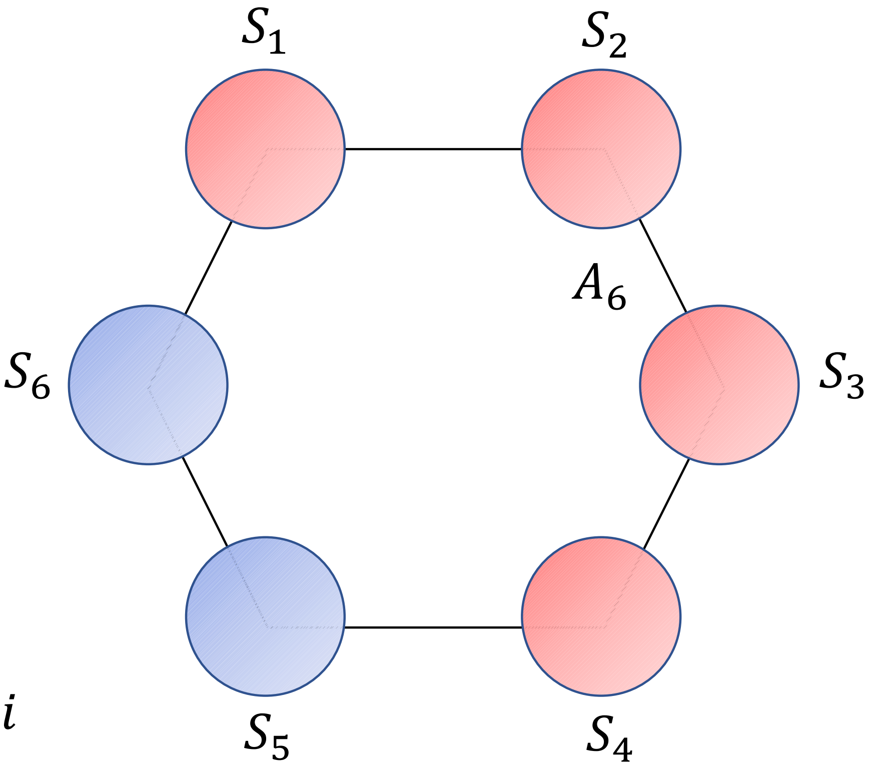


# Chain conditions

- Parties: $P = \{P_1, P_2, .., P_n\}$
- General: $A = \{A_1, A_2, .., A_k\}$,
  $A_i \subseteq P$

- Partition: $S = (S_1, S_2, .., S_b)$
  - $\bigcup_{i=1}^{b} S_i = P$
  - $S_i \cap S_j = \emptyset$
  - non-empty $S_i$'s

- $P \setminus (S_i \cup S_{i+1}) \in A$, for every $i$



# [Ray15] impossibility

- $n$ parties
- adversary has $b$-chain
- $(b-1)$-minicast model

- Broadcast is impossible

# [Ray15] impossibility

- $b$ parties
- adversary has $b$-chain
- $(b-1)$-minicast model

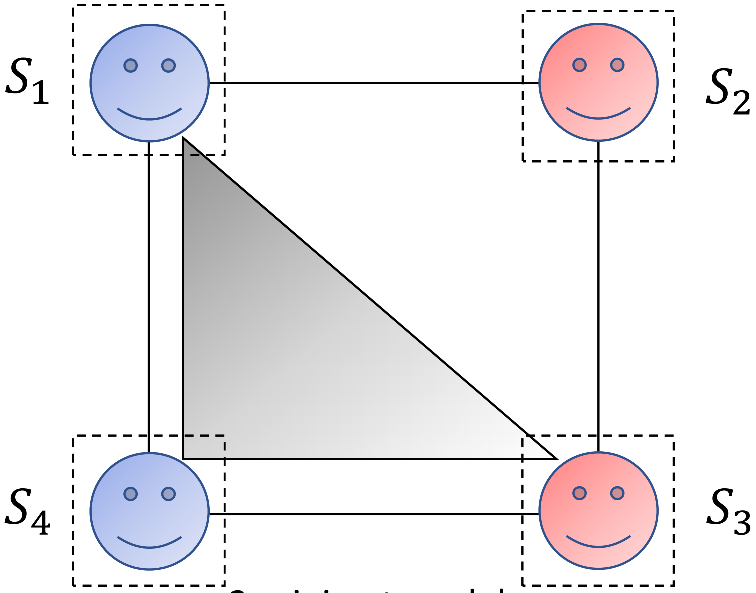
- Broadcast is impossible

⇒

- $n$ parties
- adversary has $b$-chain
- $(b-1)$-minicast model

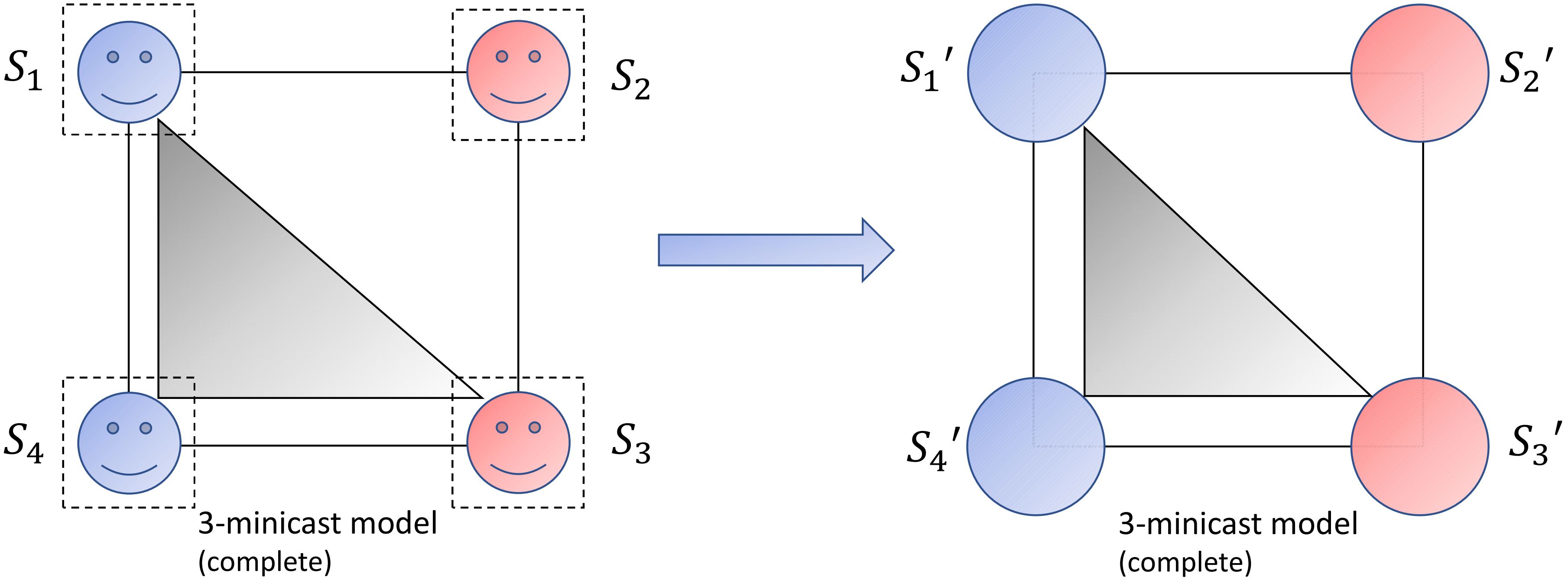
- Broadcast is impossible

# [Ray15] impossibility



3-minicast model
(complete)

# [Ray15] impossibility



# Essential minicasts

- $b$ parties
- adversary has $b$-chain
- $(b-1)$-minicast model
  (complete)

- Broadcast is impossible

# Essential minicasts

- $b$ parties
- adversary has $b$-chain
- $(b-1)$-minicast model (complete)

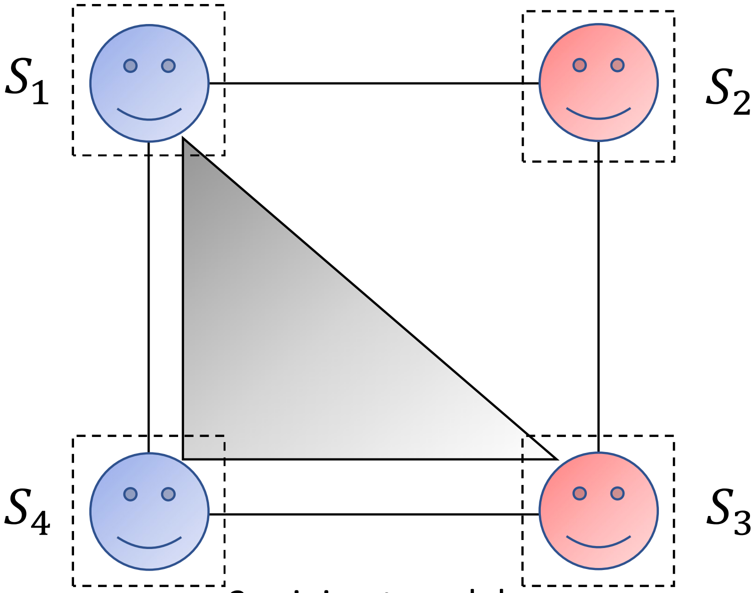
- Broadcast is impossible

→

- $n$ parties
- adversary has $b$-chain
- $b$-minicast model (incomplete)

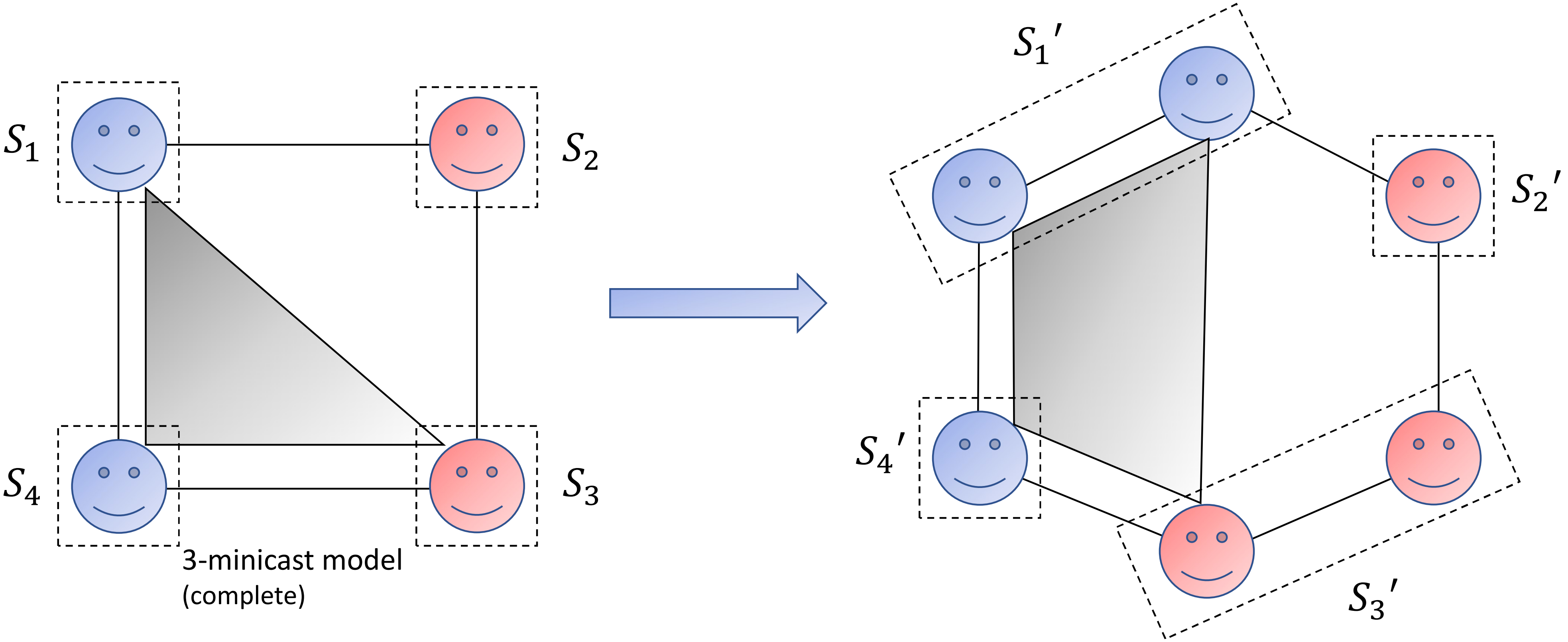
- Broadcast is impossible

# Essential minicasts



3-minicast model
(complete)

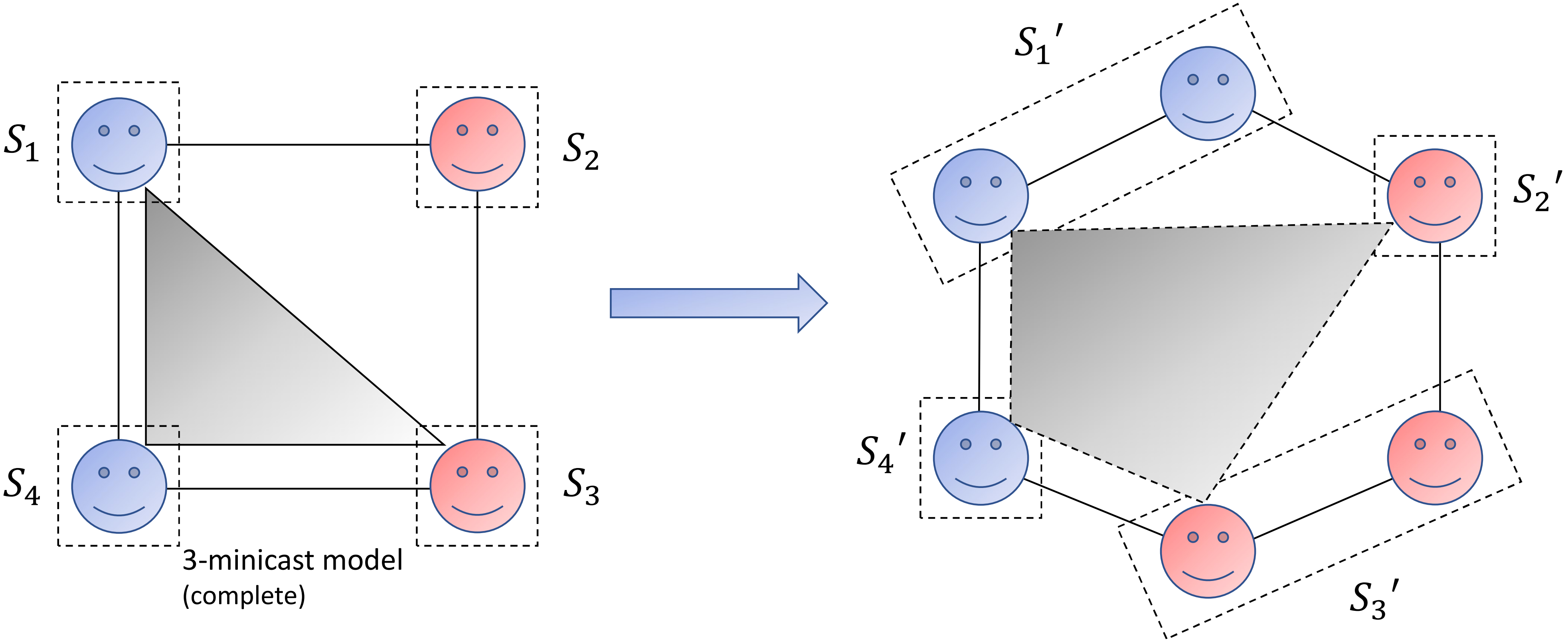
# Essential minicasts



3-minicast model
(complete)

4-minicast model
(incomplete)

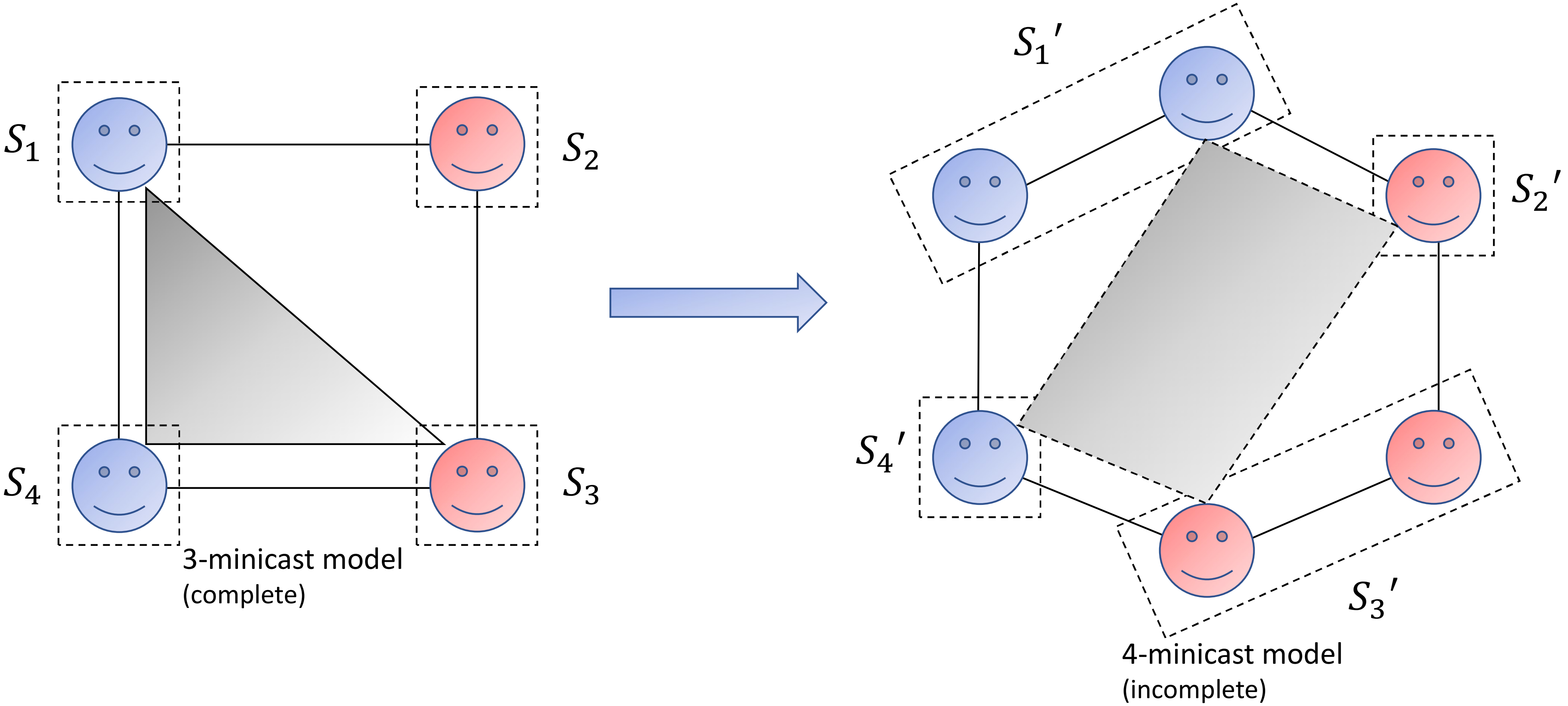
# Essential minicasts



3-minicast model
(complete)

4-minicast model
(incomplete)

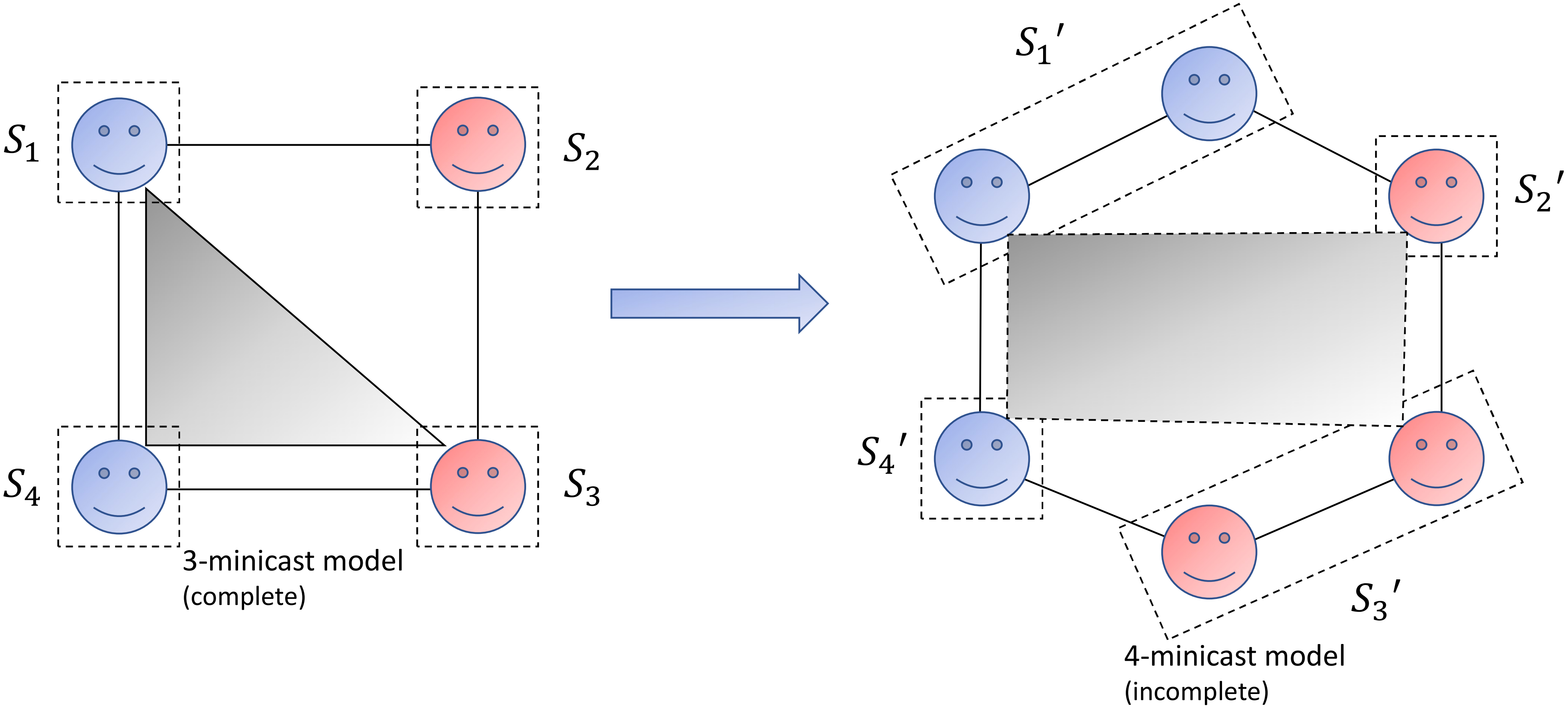
# Essential minicasts



3-minicast model
(complete)

4-minicast model
(incomplete)

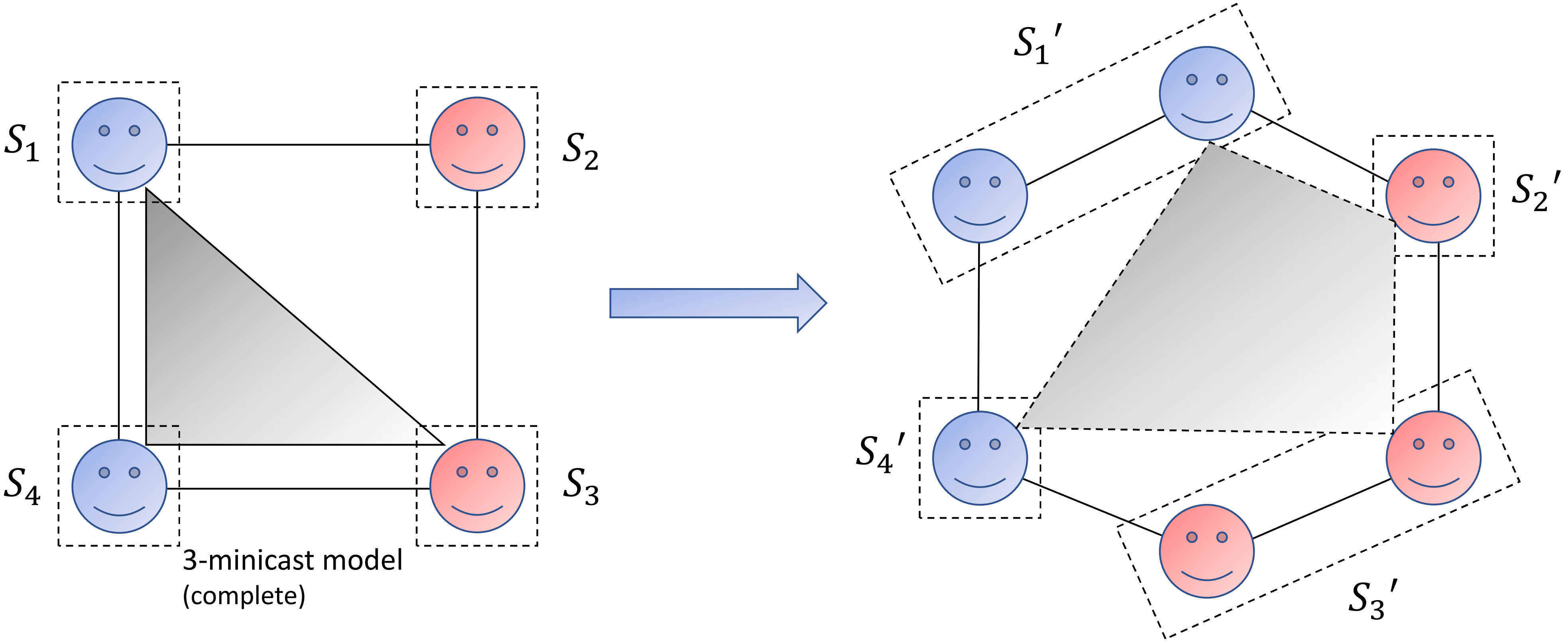
# Essential minicasts



3-minicast model
(complete)

4-minicast model
(incomplete)

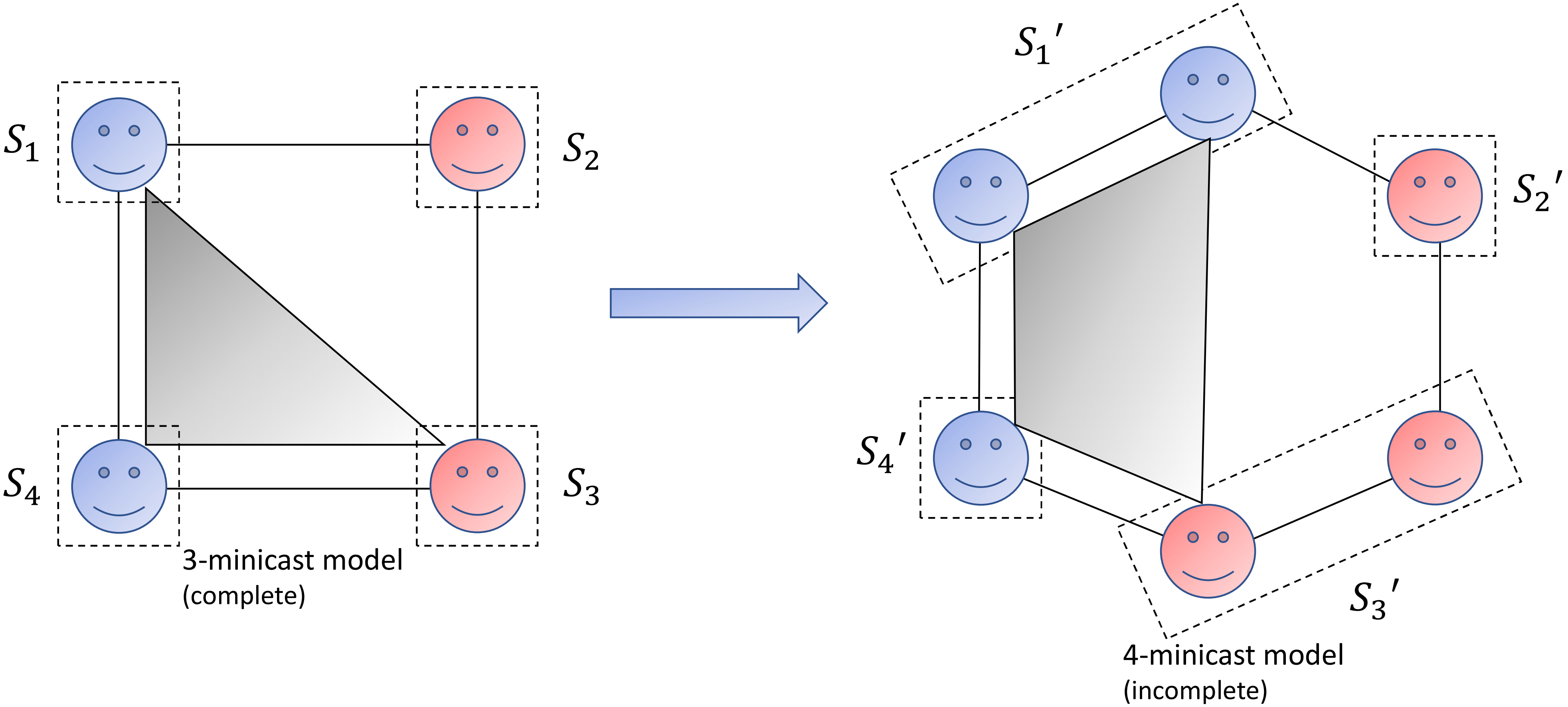
# Essential minicasts



3-minicast model
(complete)

4-minicast model
(incomplete)

# Essential minicasts



3-minicast model
(complete)

4-minicast model
(incomplete)

# Necessary condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks only if:

# Necessary condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks only if:

- for every $b$-chain in $A$ of the form $(S_1, S_2, .., S_b)$,

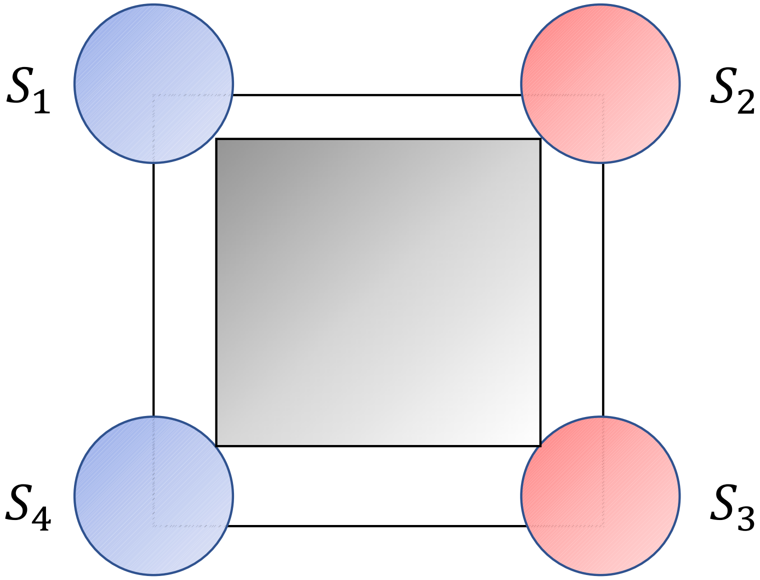
# Necessary condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks only if:

- for every $b$-chain in $A$ of the form $(S_1, S_2, .., S_b)$,
- there is a $b$-minicast channel that has non-empty intersection with each of the sets $S_1, S_2, .., S_b$.

# Necessary condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks only if, for every $b$-chain in $A$, there is a $b$-minicast channel of a corresponding form.



# Necessary condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks only if:

- for every $b$-chain in $A$ of the form $(S_1, S_2, .., S_b)$,
- there is a $b$-minicast channel that has non-empty intersection with each of the sets $S_1, S_2, .., S_b$.

# Necessary condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks only if, for all $k$ $(3 \leq k \leq b)$:

- for every $k$-chain in $A$ of the form $(S_1, S_2, .., S_k)$,
- there is a $k$-minicast channel that has non-empty intersection with each of the sets $S_1, S_2, .., S_k$.

# Non-essential minicasts

- $n$ parties
- adv. is $(b+1)$-chain free
- $b$-minicast model
  (complete)

- Broadcast is possible [Ray15]

# Non-essential minicasts

- $n$ parties
- adv. is $(b+1)$-chain free
- $b$-minicast model
  (complete)

- Broadcast is possible [Ray15]

- $n$ parties
- adv. is $(b+1)$-chain free
- $b$-minicast model
  (incomplete)

- Broadcast is possible

# Non-essential minicasts

- $n$ parties
- adv. is $(b + 1)$-chain free
- $b$-minicast model
  (complete)

- Broadcast is possible [Ray15]

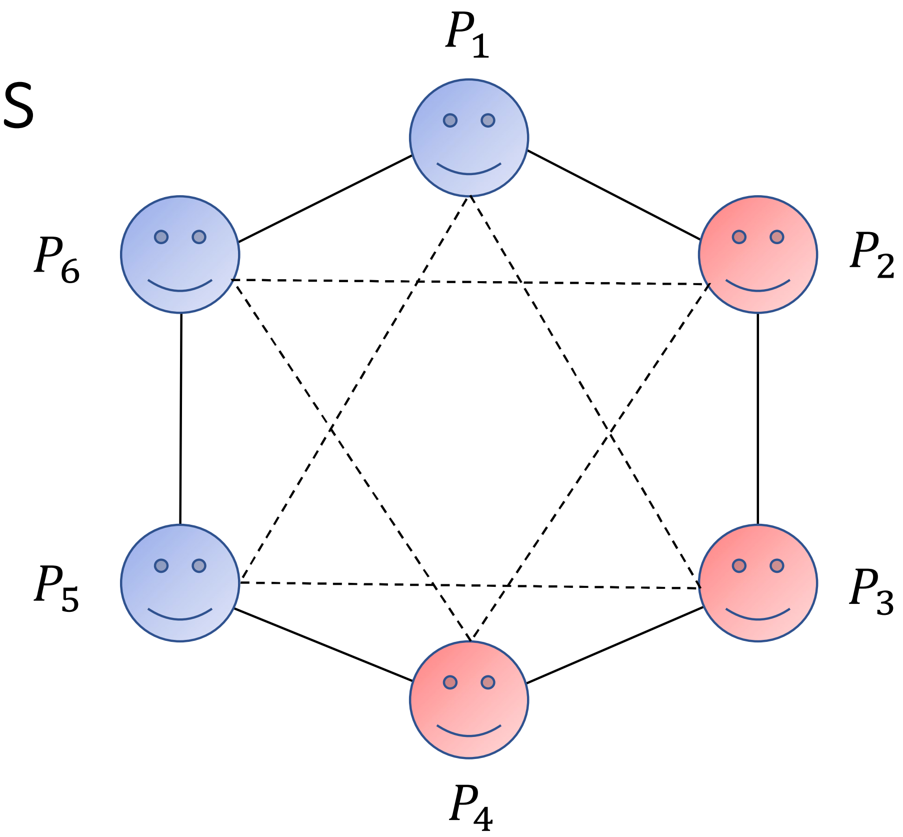
⇒

- $n$ parties
- adv. is $(b + 1)$-chain free
- $b$-minicast model
  (incomplete)

- Broadcast is possible

Idea: Simulate *missing/non-essential* $b$-minicast channels with *local* executions of [Ray15]’s protocol.

# Non-essential minicasts

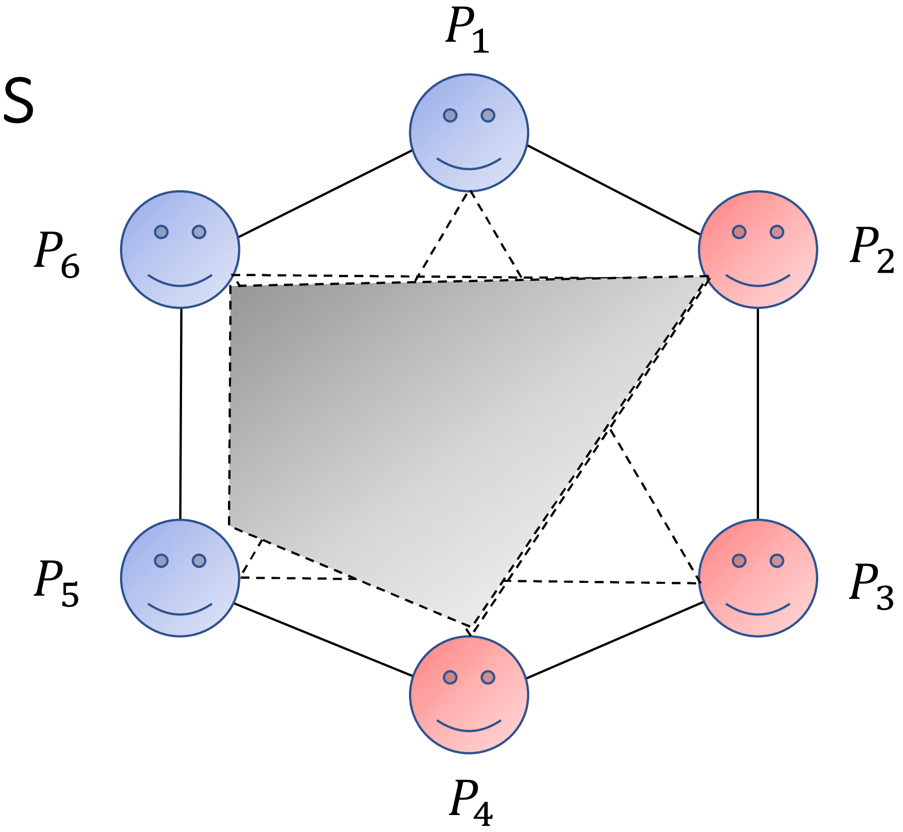


Idea: Simulate *non-essential* $b$-minicast channels with *local* executions of [Ray15]'s protocol.

# Non-essential minicasts

- $b$ parties
- adv. is $b$-chain free
- $(b-1)$-minicast model (complete)

- Broadcast is possible [Ray15]

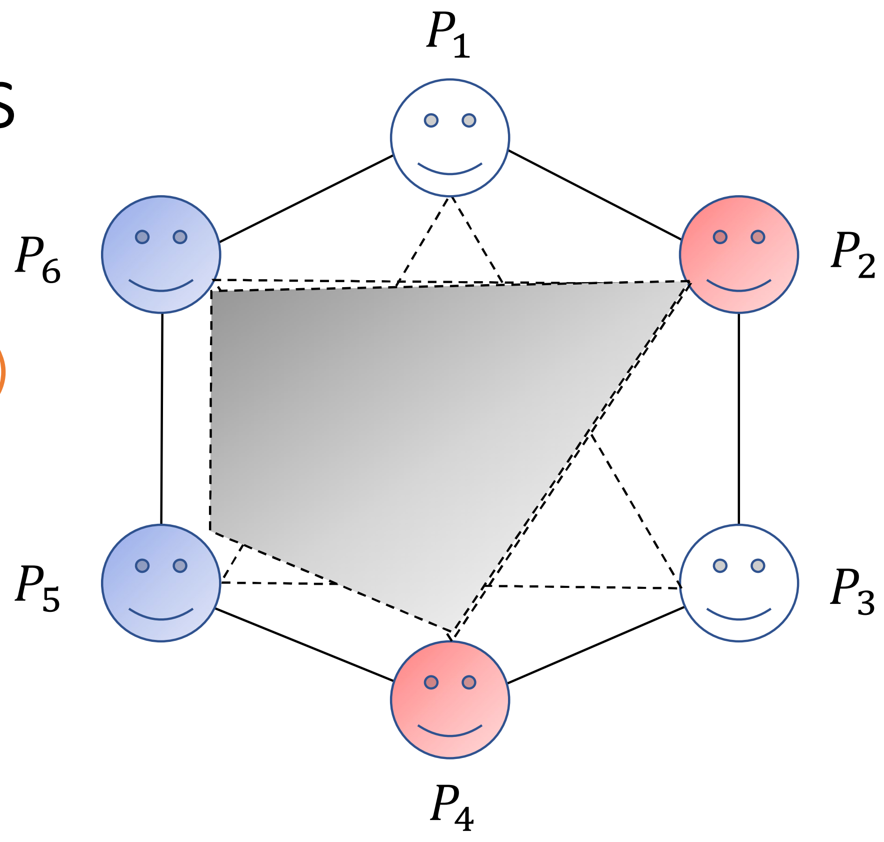


Idea: Simulate *non-essential* $b$-minicast channels with *local* executions of [Ray15]'s protocol.

# Non-essential minicasts

- $b$ parties
- adv. is $b$-chain free (locally restricted)
- $(b-1)$-minicast model (complete)

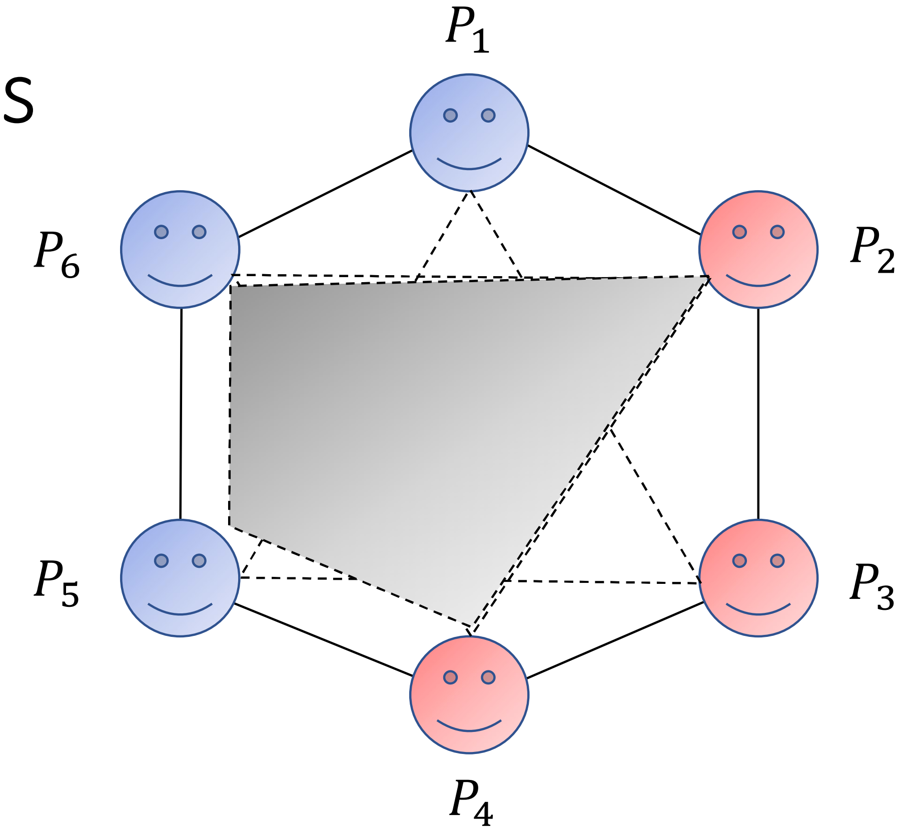
- Broadcast is possible [Ray15]



<u>Idea</u>: Simulate *non-essential* $b$-minicast channels with *local* executions of [Ray15]'s protocol.

# Non-essential minicasts

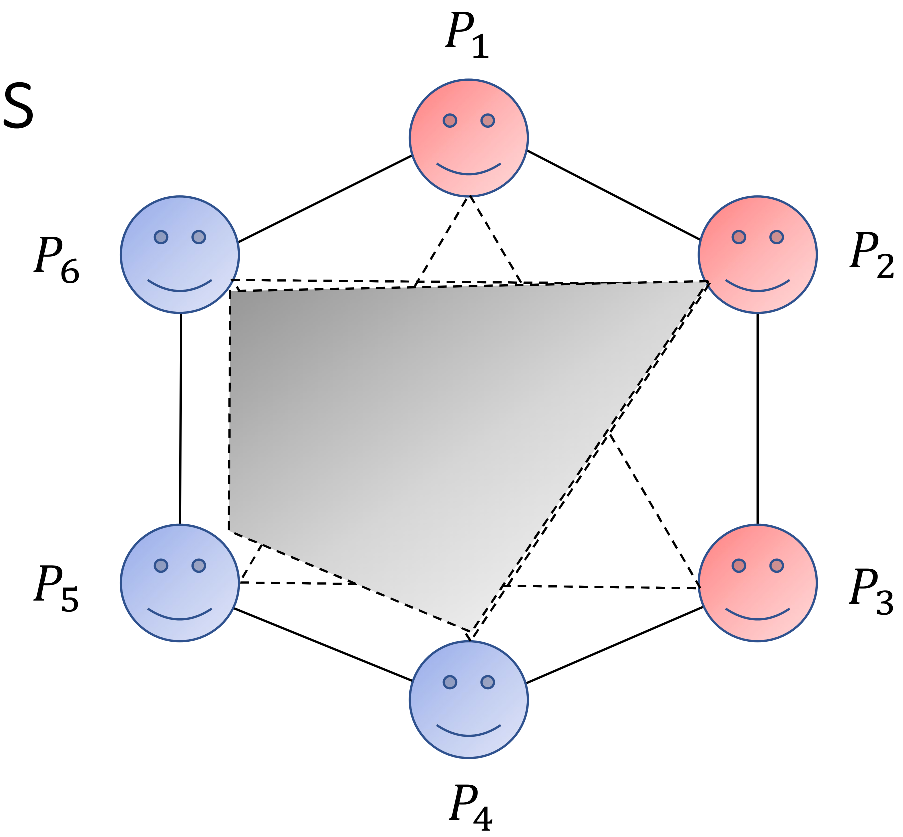
- $A = \{A_1, A_2, .., A_k\}$



Idea: Simulate *non-essential* $b$-minicast channels with *local* executions of [Ray15]'s protocol.

# Non-essential minicasts

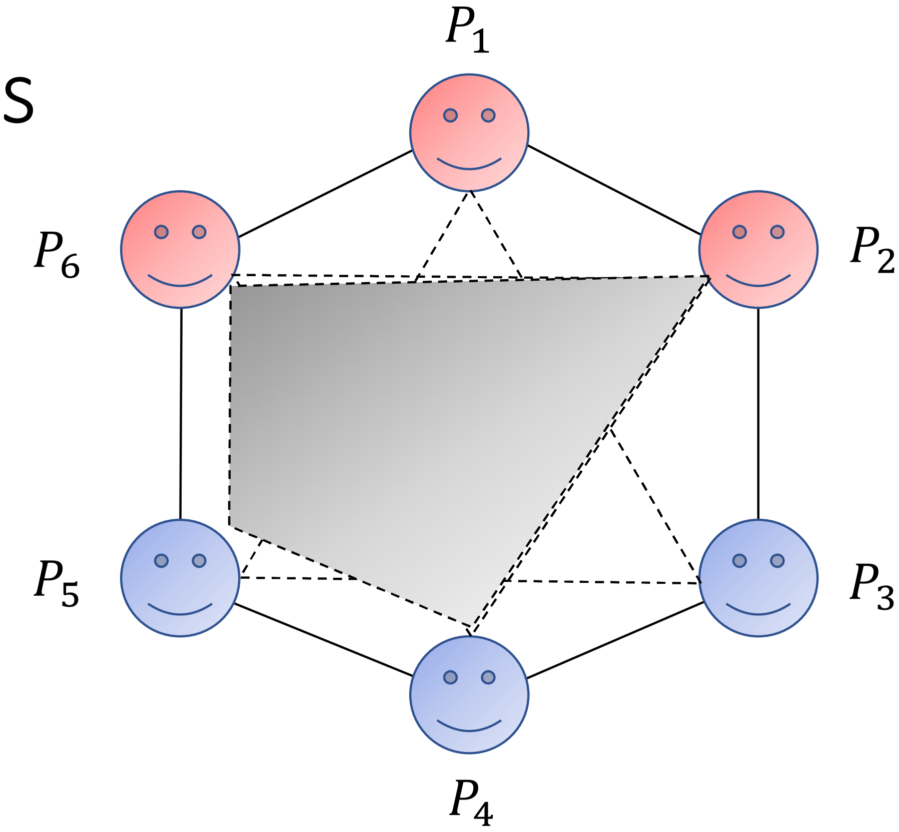
- $A = \{A_1, A_2, .., A_k\}$



<u>Idea</u>: Simulate *non-essential* $b$-minicast channels with *local* executions of [Ray15]'s protocol.

# Non-essential minicasts

- $A = \{A_1, A_2, .., A_k\}$

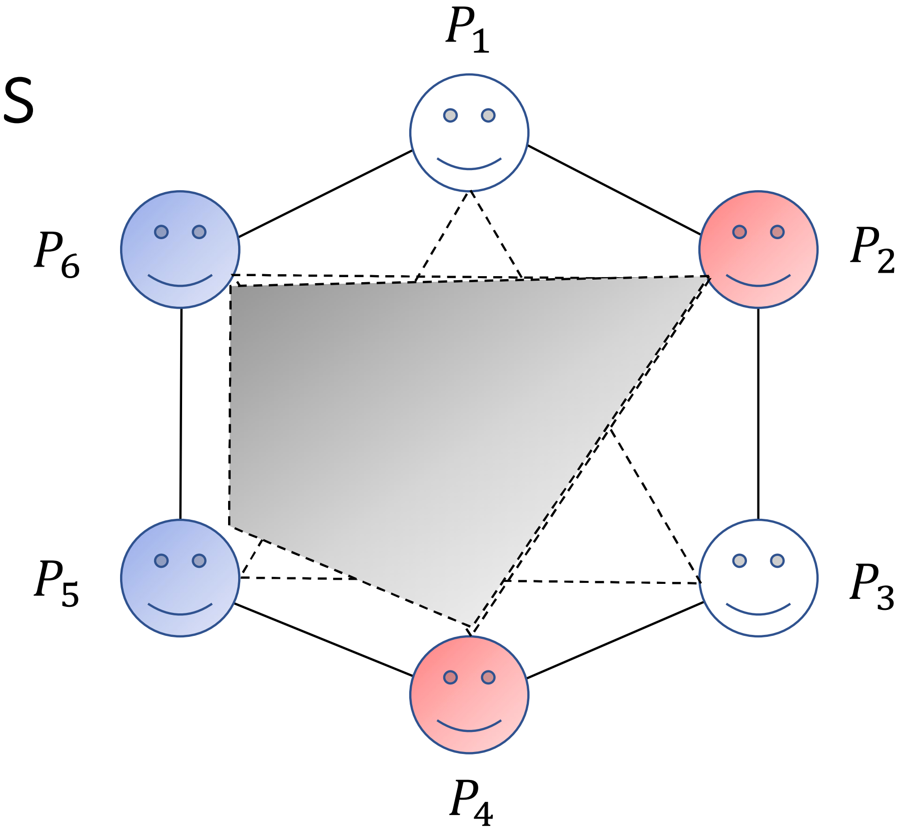


Idea: Simulate *non-essential* $b$-minicast channels with *local* executions of [Ray15]'s protocol.

# Non-essential minicasts

- $A = \{A_1, A_2, .., A_k\}$

- $A[\rho] = \{A_i \cap \rho \mid A_i \in A\}$
  (projection of $A$ onto $\rho$)

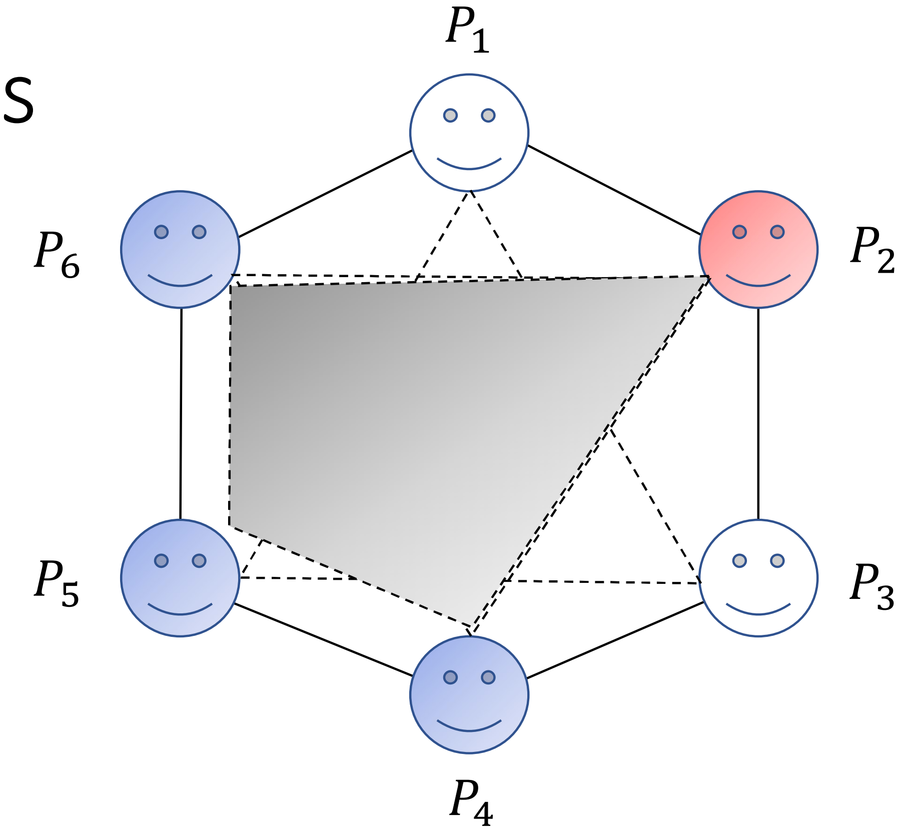


Idea: Simulate *non-essential* $b$-minicast channels with *local* executions of [Ray15]'s protocol.

# Non-essential minicasts

- $A = \{A_1, A_2, .., A_k\}$

- $A[\rho] = \{A_i \cap \rho \mid A_i \in A\}$
  (projection of $A$ onto $\rho$)

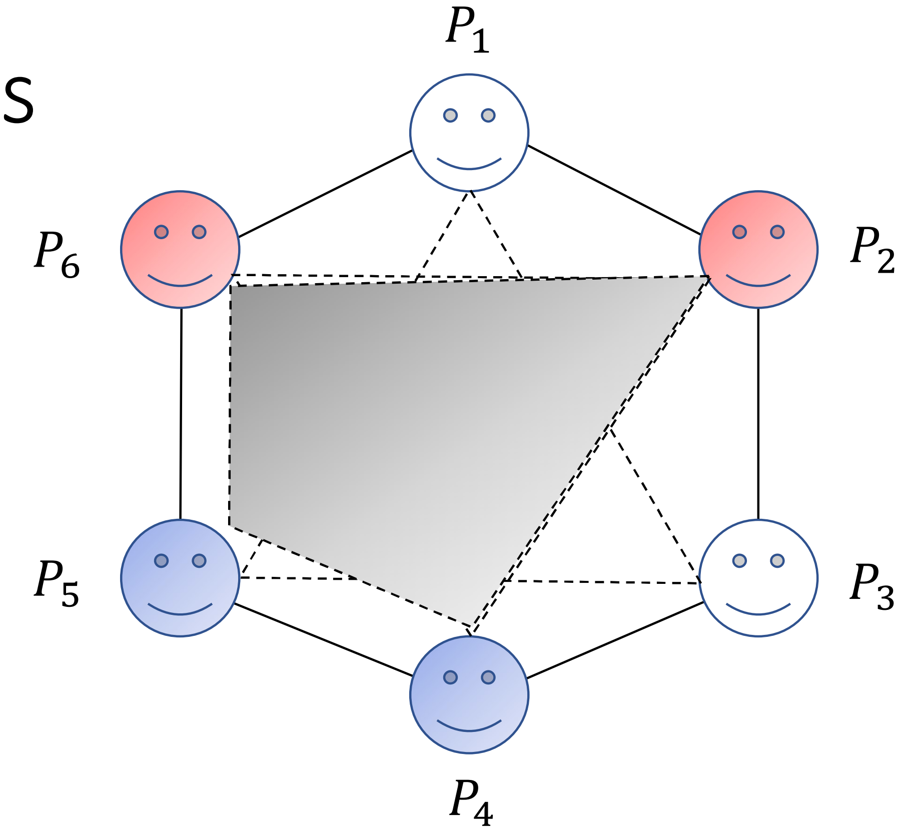


Idea: Simulate *non-essential* $b$-minicast channels with *local* executions of [Ray15]'s protocol.

# Non-essential minicasts

- $A = \{A_1, A_2, .., A_k\}$

- $A[\rho] = \{A_i \cap \rho \mid A_i \epsilon A\}$
  (projection of $A$ onto $\rho$)

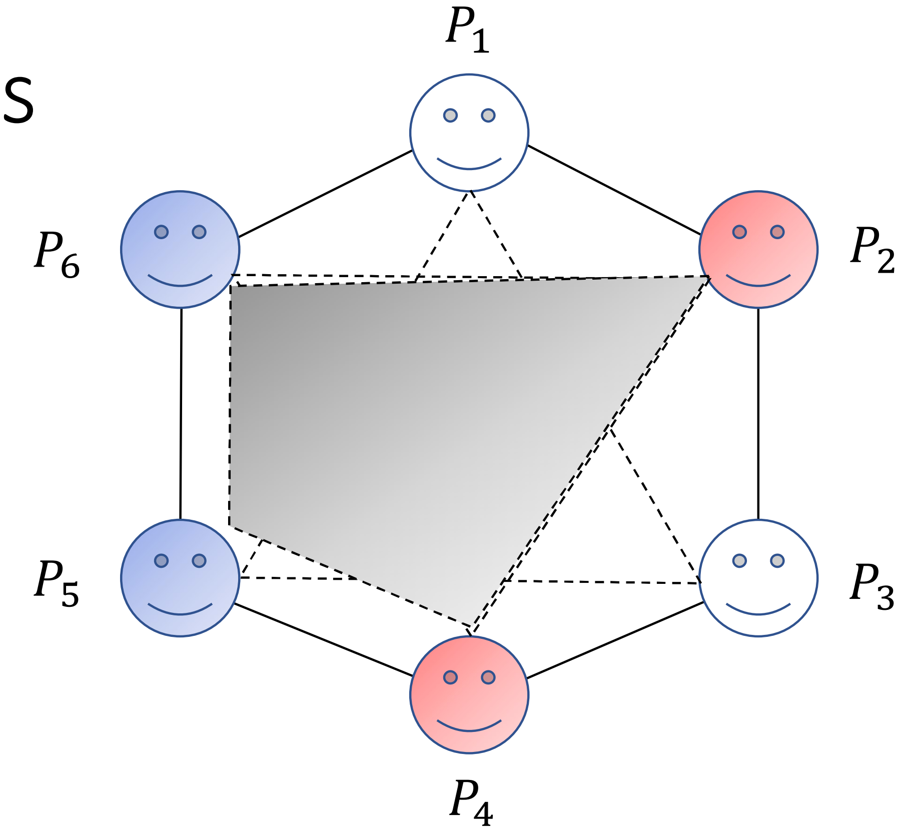


Idea: Simulate *non-essential* $b$-minicast channels with *local* executions of [Ray15]'s protocol.

# Non-essential minicasts

- $b$ parties
- The projected adv. is $b$-chain free
- $(b-1)$-minicast model (complete)

- Broadcast is possible [Ray15]



Idea: Simulate *non-essential* $b$-minicast channels with *local* executions of [Ray15]'s protocol.

# Sufficient condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks if:

# Sufficient condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks if:

- there is a complete set of $(b-1)$-minicast channels, and

# Sufficient condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks if:

- there is a complete set of $(b-1)$-minicast channels, and
- for each subset of parties $\rho$ of size $b$:

# Sufficient condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks if:

- there is a complete set of $(b-1)$-minicast channels, and
- for each subset of parties $\rho$ of size $b$:
  - if $A[\rho]$ contains a $b$-chain,

# Sufficient condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks if:

- there is a complete set of $(b-1)$-minicast channels, and
- for each subset of parties $\rho$ of size $b$:
    - if $A[\rho]$ contains a $b$-chain,
    - there is a $b$-minicast channel among $\rho$

# Sufficient condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks if:

- there is a complete set of bilateral channels, and
- for each subset of parties $\rho$ of size $k$ $(3 \leq k \leq b)$:
  - if $A[\rho]$ contains a $k$-chain,
  - there is a $k$-minicast channel among $\rho$

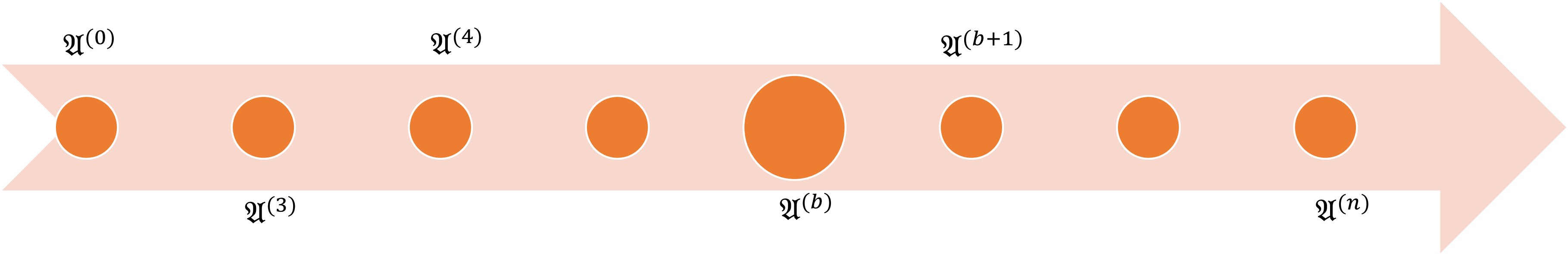
# Sufficient condition

[LMM20]: For adversary structures $A \in \mathfrak{A}^{(b)}$, broadcast is achievable in general networks if:

- there is a complete set of bilateral channels, and
- for each subset of parties $\rho$ of size $k$ $(3 \leq k \leq b)$:
  - if $A[\rho]$ contains a $k$-chain,
  - there is a $k$-minicast channel among $\rho$

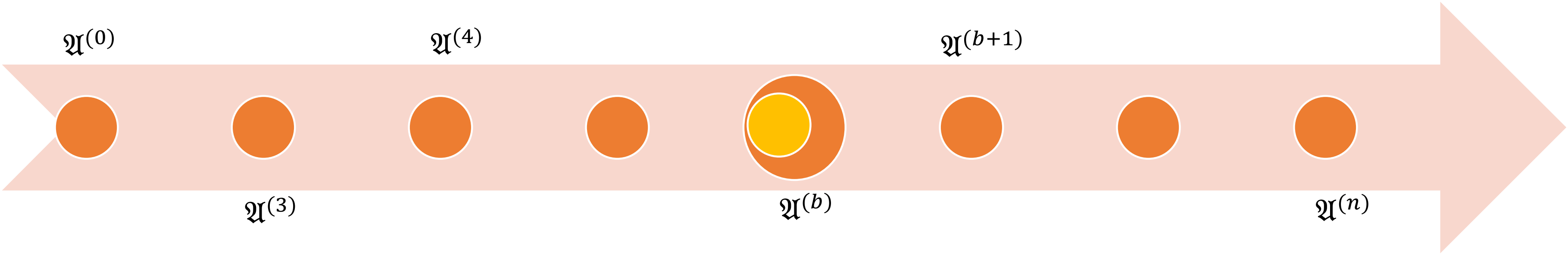
Condition *non-trivial* for certain weak class of adversaries in $\mathfrak{A}^{(b)}$, namely $b$-chain adversaries.

# Chain adversaries



$\left(A \in \mathfrak{A}^{(b)}\right)$: $A$ contains $b$-chain(s) and $A$ is $(b+1)$-chain free

# Chain adversaries

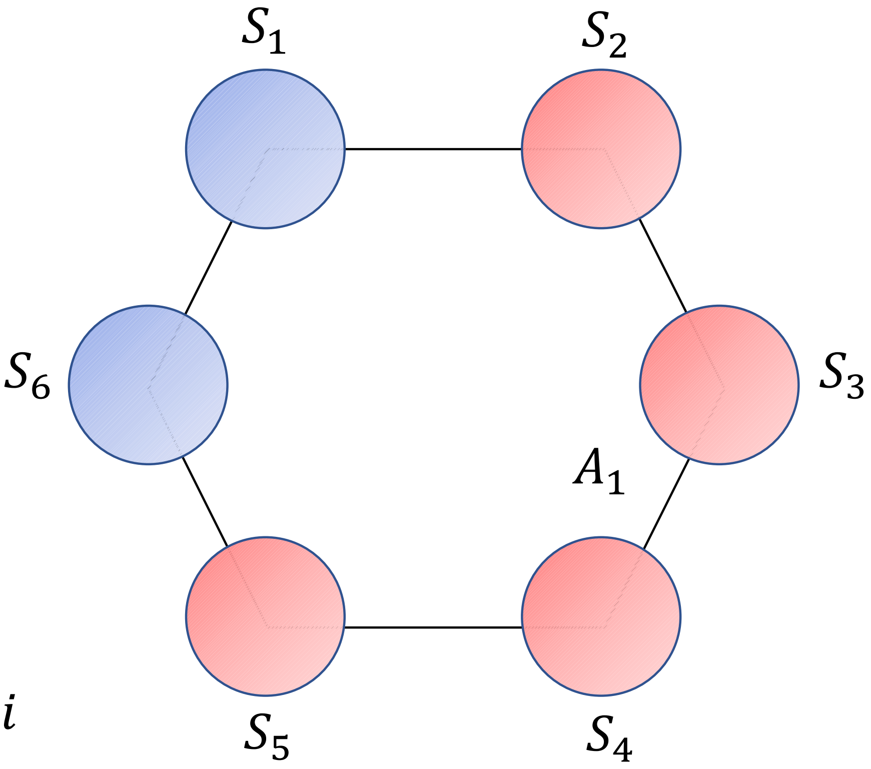


$\left(A \in \mathfrak{A}^{(b)}\right)$: $A$ contains $b$-chain(s) and $A$ is $(b+1)$-chain free

A $b$-chain adversary *just* contains a (single) $b$-chain, and nothing more

# Chain adversaries

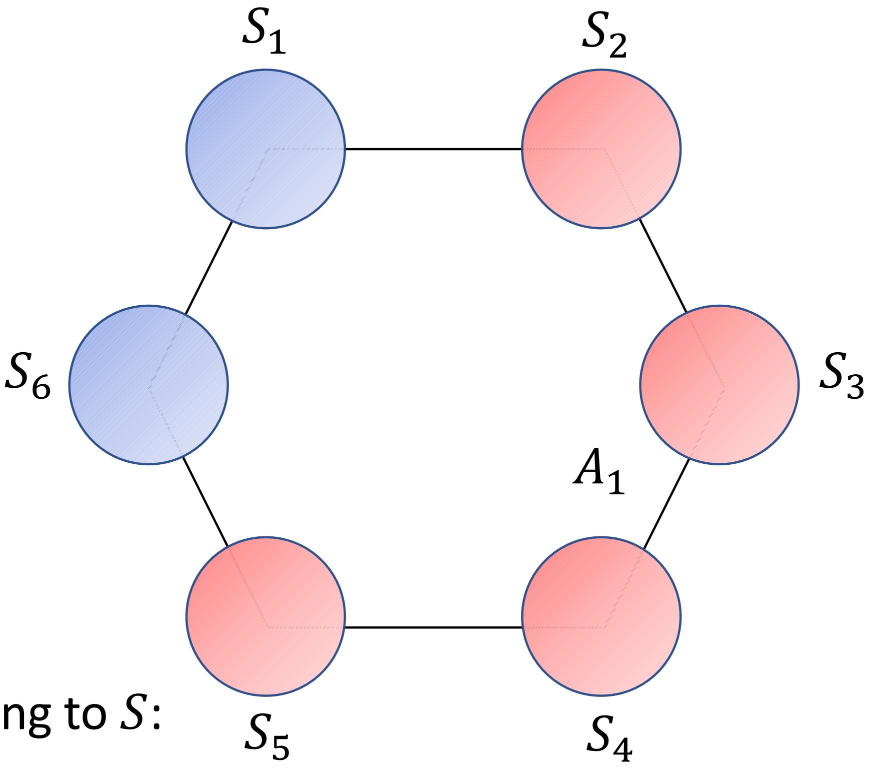
- Parties: $P = \{P_1, P_2, .., P_n\}$
- General: $A = \{A_1, A_2, .., A_k\}$,
  $A_i \subseteq P$
- Partition: $S = (S_1, S_2, .., S_b)$
  - $\bigcup_{i=1}^{b} S_i = P$
  - $S_i \cap S_j = \emptyset$
  - non-empty $S_i$'s
- $P \setminus (S_i \cup S_{i+1}) \in A$, for every $i$



# Chain adversaries

- Parties: $P = \{P_1, P_2, .., P_n\}$
- General: $A = \{A_1, A_2, .., A_k\}$, $A_i \subseteq P$
- Partition: $S = (S_1, S_2, .., S_b)$
  - $\cup_{i=1}^{b} S_i = P$
  - $S_i \cap S_j = \emptyset$
  - non-empty $S_i$'s
- *b*-chain adversary corresponding to $S$:

  $A^S = \{P \setminus (S_i \cup S_{i+1}) \mid 1 \leq i \leq b\}$



# Chain adversaries

- Given any $b$-chain adversary $A^S$:

# Chain adversaries

- Given any $b$-chain adversary $A^S$:
  - it belongs to the class $\mathfrak{A}^{(b)}$ (i.e., is also $(b+1)$-chain free). [LMM20]

# Chain adversaries

- Given any $b$-chain adversary $A^S$:
  - it belongs to the class $\mathfrak{A}^{(b)}$ (i.e., is also $(b+1)$-chain free). [LMM20]
  - there exist subsets of parties $\rho$ ($|\rho| = b$) such that $A^S[\rho]$ is $b$-chain free (i.e., $b$-minicast channel among $\rho$ is *non-essential*). [LMM20]

# Other results

- Our conditions allow us to derive bounds on the no. of $b$-minicast channels that are necessary and that suffice in achieving global broadcast in general networks secure against general adversaries.

# Other results

- Our conditions allow us to derive bounds on the no. of $b$-minicast channels that are necessary and that suffice in achieving global broadcast in general networks secure against general adversaries.
  - Thereby providing a way to extend [JMS12]’s quantitative analysis in general 3-minicast networks to higher $b$-minicast networks.

# Open problems

- Providing tighter necessary and sufficient conditions on general networks for achieving broadcast while tolerating general adversaries.

# Open problems

- Providing tighter necessary and sufficient conditions on general networks for achieving broadcast while tolerating general adversaries.
  - We showed that a straightforward extension of a technique (so-called *virtual party emulation*) used by [RVS+04] in deriving such tight conditions in general 3-minicast networks does not generalize to higher $b$-minicast networks.

# Open problems

- Providing tighter necessary and sufficient conditions on general networks for achieving broadcast while tolerating general adversaries.
  - We showed that a straightforward extension of a technique (so-called *virtual party emulation*) used by [RVS+04] in deriving such tight conditions in general 3-minicast networks does not generalize to higher $b$-minicast networks.

- Implications of such results on broadcast in general $b$-minicast networks, secure against general adversaries, in a realistic setting.