Reliable communication via semilattice properties of partial knowledge

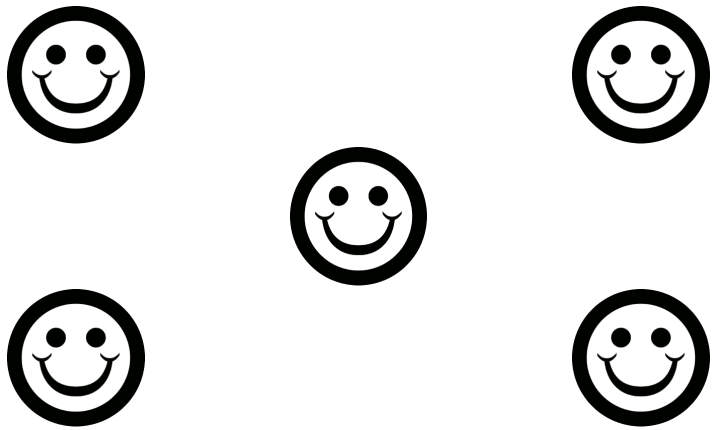
A. Pagourtzis [1] G. Panagiotakos [2] D. Sakavalas [1]

[1] School of Electrical and Computer Engineering
National Technical University of Athens

[2] School of Informatics
University of Edinburgh

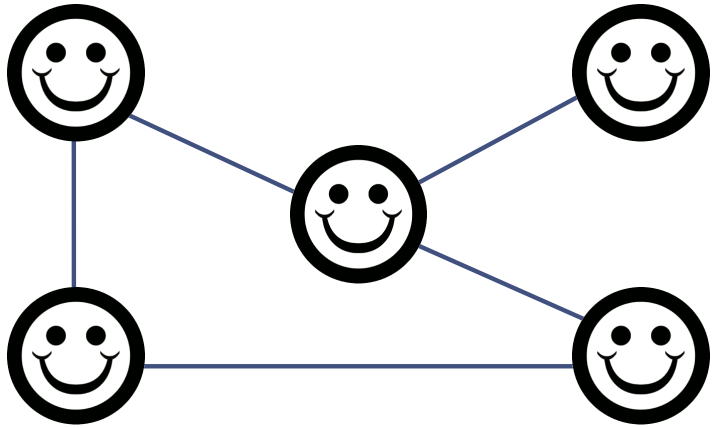
21st International Symposium on Fundamentals of Computation Theory
Bordeaux, France, September 13, 2017

Distributed Computing in an unreliable environment



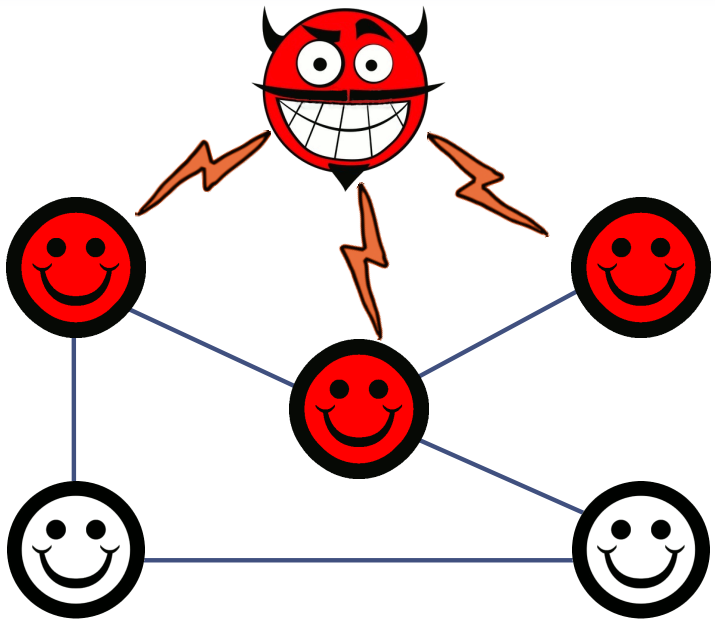
– Several interacting entities (**players/agents**) that cooperate to achieve a common goal **without central coordination**.

Distributed Computing in an unreliable environment



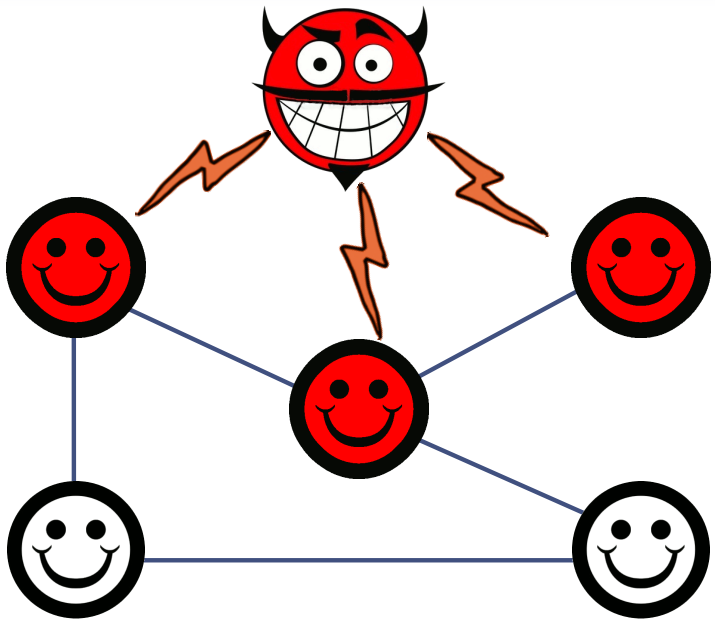
- Several interacting entities (**players/agents**) that cooperate to achieve a common goal **without central coordination**.
- Players arranged in a communication network G.

Distributed Computing in an unreliable environment



- Several interacting entities (**players/agents**) that cooperate to achieve a common goal **without central coordination**.
- Players arranged in a communication network G.
- Adversarial Behavior: Corrupted players controlled by a central active (Byzantine) adversary.

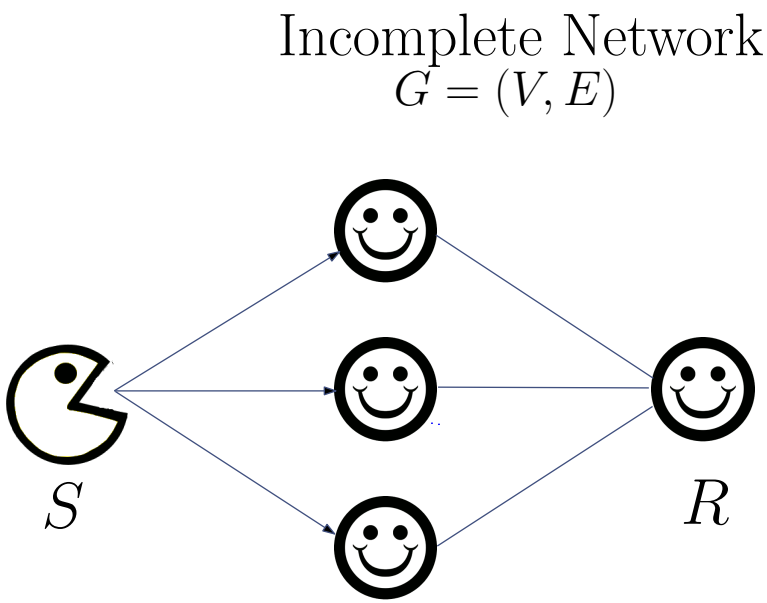
Distributed Computing in an unreliable environment



- Several interacting entities (**players/agents**) that cooperate to achieve a common goal **without central coordination**.
- Players arranged in a communication network G.
- Adversarial Behavior: Corrupted players controlled by a central active (Byzantine) adversary.
- Achieve goal despite the presence of corruptions.

Reliable Communication

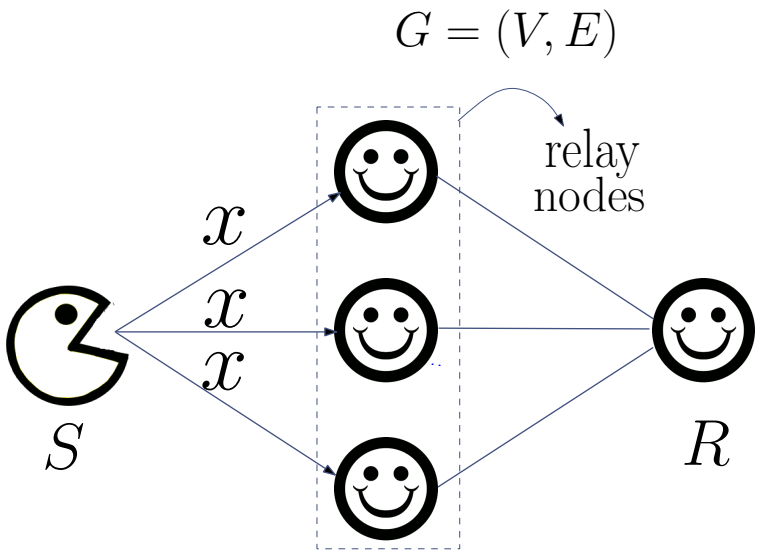
– Reliable Message Transmission (RMT) problem:
Correct delivery of message x from **Sender** S to **Receiver** R, despite the existence of corrupted players.



Reliable Communication

– Reliable Message Transmission (RMT) problem:
Correct delivery of message x from **Sender** S to **Receiver** R, despite the existence of corrupted players.

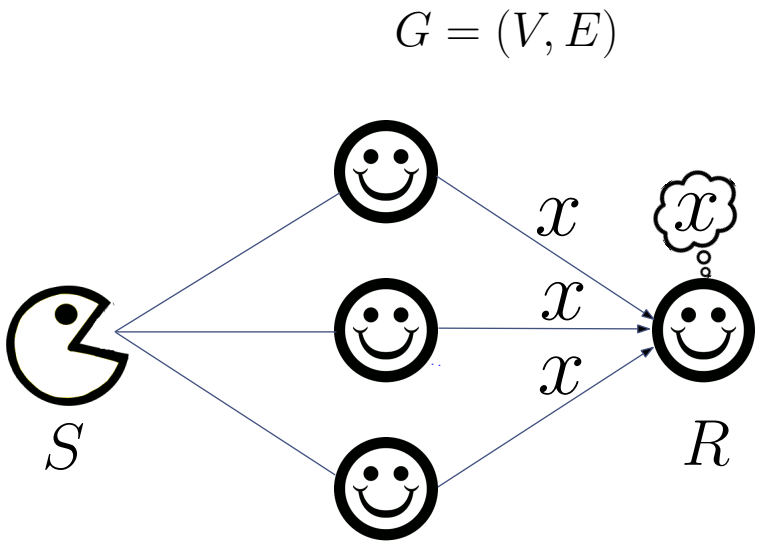
Sender's input: x



Reliable Communication

– Reliable Message Transmission (RMT) problem:
Correct delivery of message x from **Sender** S to **Receiver** R, despite the existence of corrupted players.

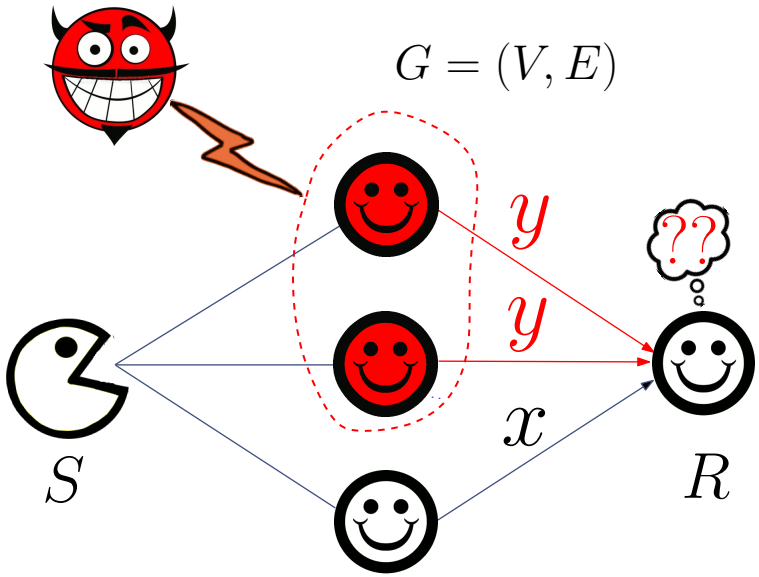
(**Sender's input**: x, **Receiver's output** (decision): x)



Reliable Communication

– Reliable Message Transmission (RMT) problem:
Correct delivery of message x from **Sender** S to **Receiver** R, despite the existence of corrupted players.

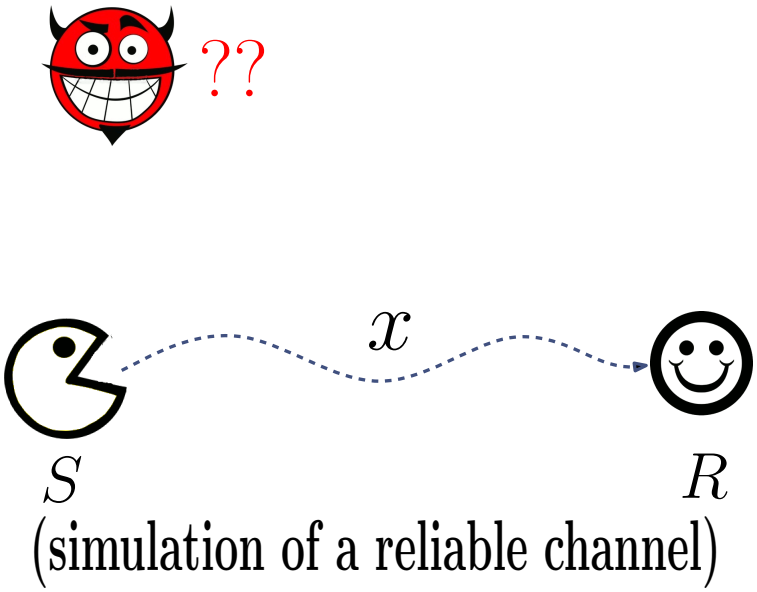
(**Sender's input**: x, **Receiver's output** (decision): x)



Reliable Communication

– Reliable Message Transmission (RMT) problem:
Correct delivery of message x from **Sender** S to **Receiver** R, despite the existence of corrupted players.

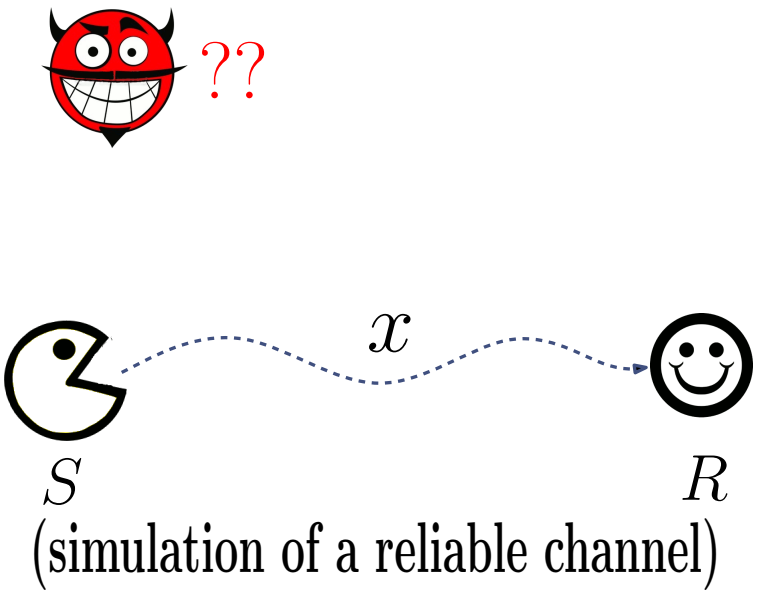
(**Sender's input**: x, **Receiver's output** (decision): x)



Reliable Communication

– Reliable Message Transmission (RMT) problem:
Correct delivery of message x from **Sender** S to **Receiver** R, despite the existence of corrupted players.

(**Sender's input**: x, **Receiver's output** (decision): x)

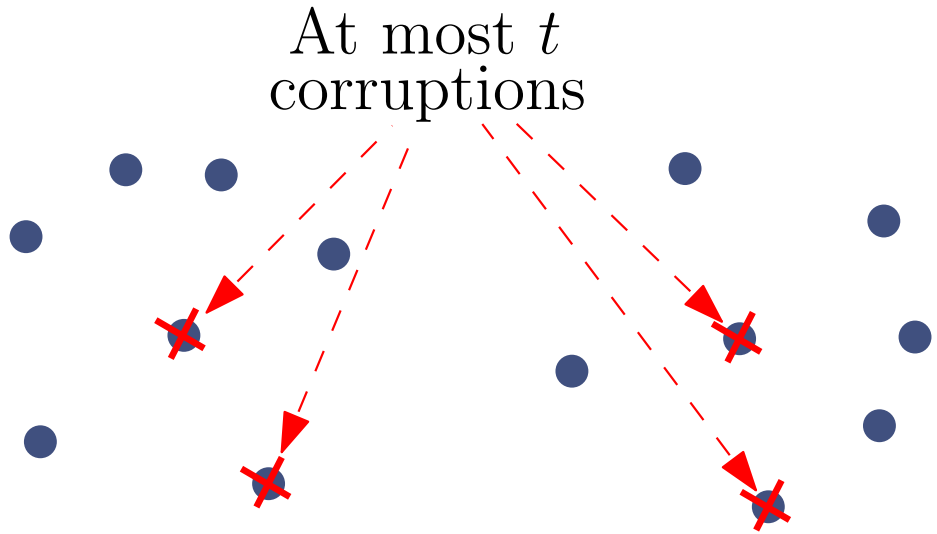


– Main result: Exact characterization of instances where RMT is feasible (impossibility condition, matching algorithm)

The Adversary

Corruption sets

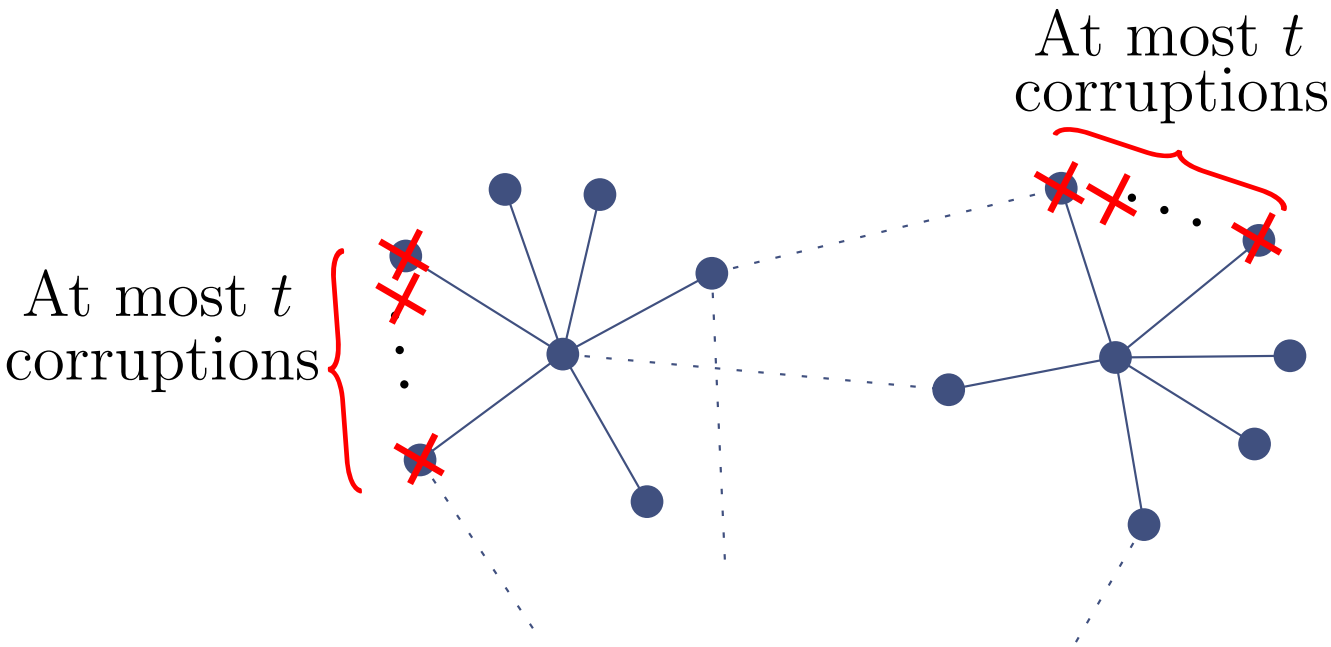
– t-Global [Lamport, Shostak, Pease, '82]:
At most t corruptions.



The Adversary

Corruption sets

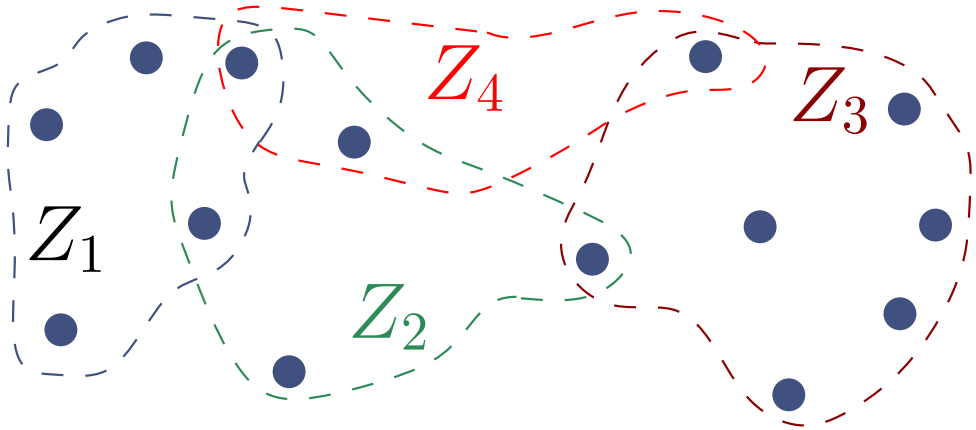
- t-Global [Lamport, Shostak, Pease, '82]:
  At most t corruptions.
- t-Local [Koo, '04]:
  At most t corruptions in each neighborhood



The Adversary

Corruption sets

- t-Global [Lamport, Shostak, Pease, '82]:
  At most t corruptions.
- t-Local [Koo, '04]:
  At most t corruptions in each neighborhood
- General Adversary [Hirt, Maurer, '97]:
  Defined by the monotone family of all possible corruption sets $\mathcal{Z} \subseteq 2^V$ (**adversary structure**).

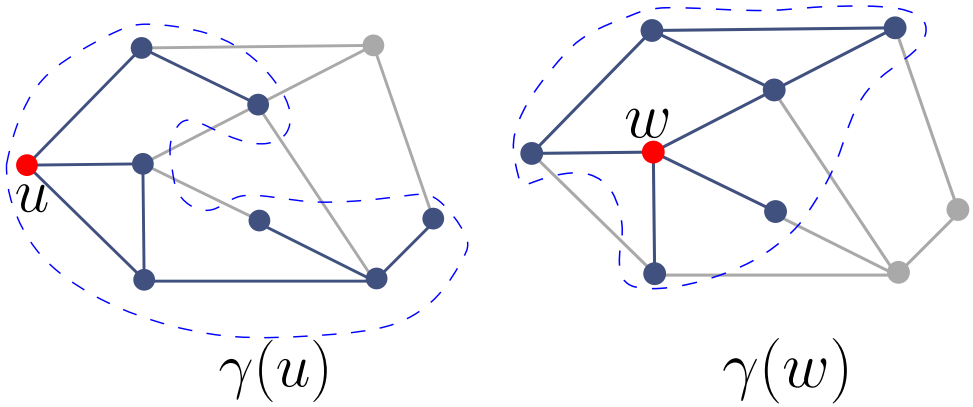


$$\mathcal{Z} = \{Z_1, Z_2, Z_3, Z_4\}$$

Initial knowledge of players

Partial knowledge model [Pagourtzis, Panagiotakos, Sakavalas, '14]

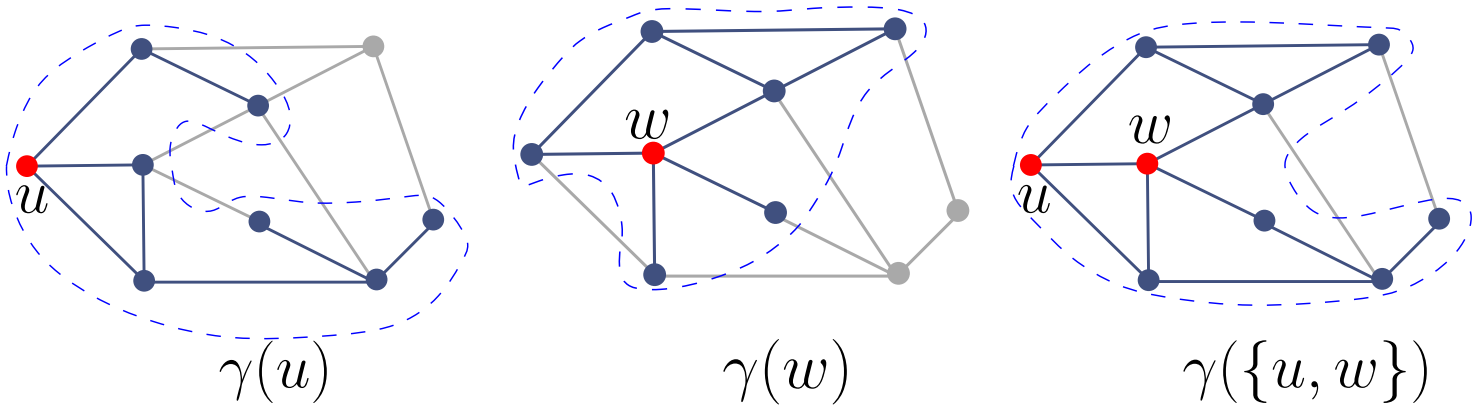
– Topology knowledge: Player u knows subgraph $\gamma(u) = (V_u, E_u)$.



Initial knowledge of players

Partial knowledge model [Pagourtzis, Panagiotakos, Sakavalas, '14]

– Topology knowledge: Player u knows subgraph $\gamma(u) = (V_u, E_u)$. For set $S \subseteq V$, $\gamma(S) = (\bigcup_{u \in S} V_u, \bigcup_{u \in S} E_u)$.

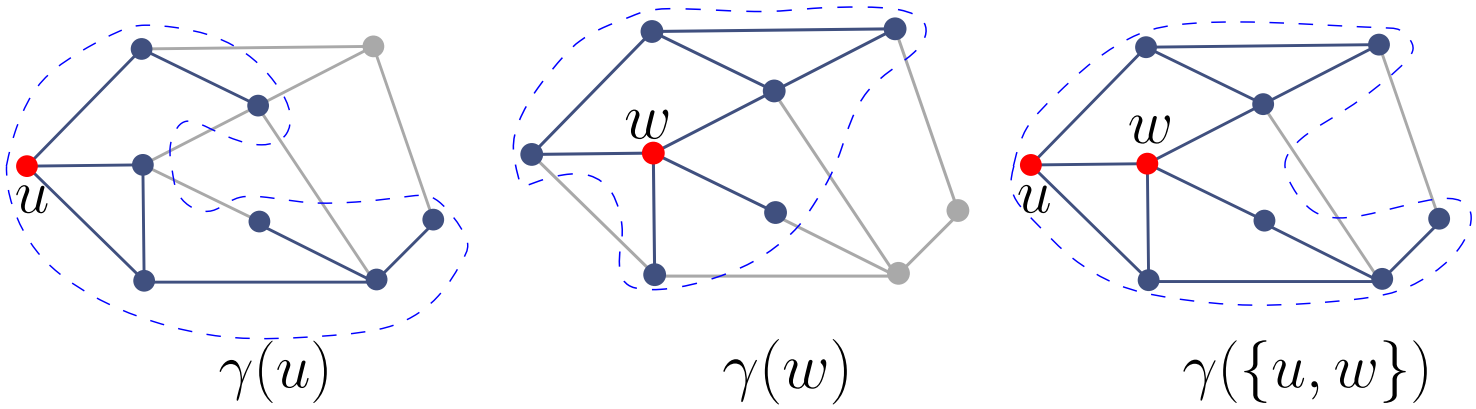


$\gamma(u)$ $\gamma(w)$ $\gamma(\{u, w\})$

Initial knowledge of players

Partial knowledge model [Pagourtzis, Panagiotakos, Sakavalas, '14]

– Topology knowledge: Player u knows subgraph $\gamma(u) = (V_u, E_u)$. For set $S \subseteq V$, $\gamma(S) = (\bigcup_{u \in S} V_u, \bigcup_{u \in S} E_u)$.



$\gamma(u)$ $\gamma(w)$ $\gamma(\{u, w\})$

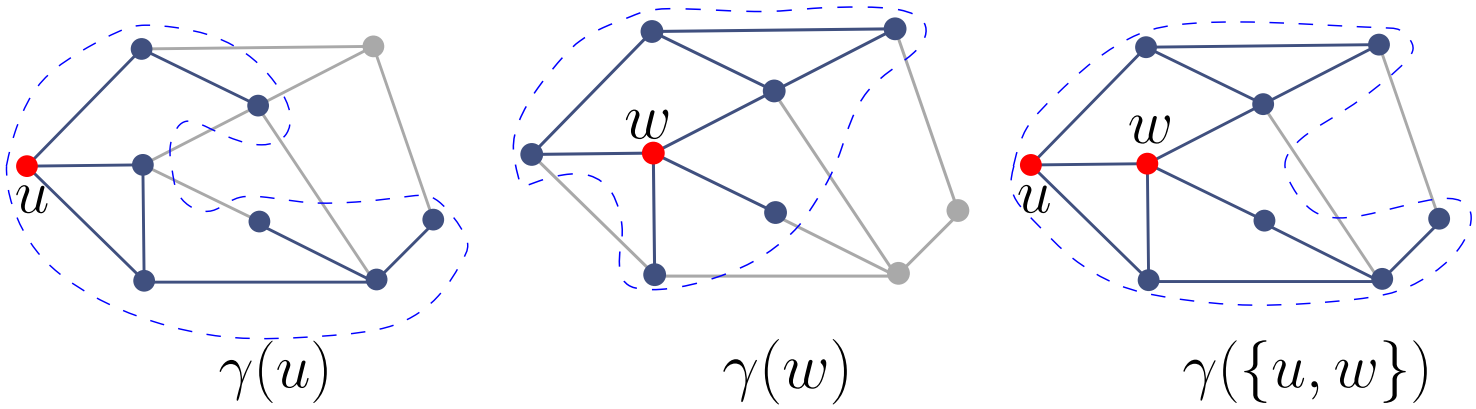
– Knowledge of the adversary structure:

Each player u knows only
the **local adversary structure**
$\mathcal{Z}_u = \{S \cap V_u : S \in \mathcal{Z}\}$
(also denoted as $\mathcal{Z}^{V_u}$).

Initial knowledge of players

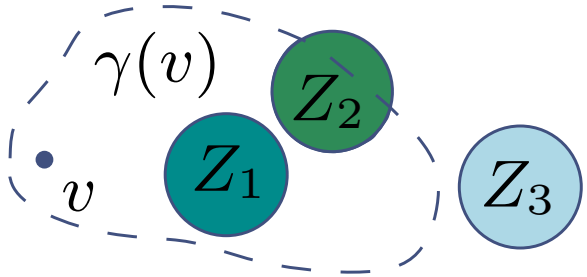
Partial knowledge model [Pagourtzis, Panagiotakos, Sakavalas, '14]

– Topology knowledge: Player u knows subgraph $\gamma(u) = (V_u, E_u)$. For set $S \subseteq V$, $\gamma(S) = (\bigcup_{u \in S} V_u, \bigcup_{u \in S} E_u)$.



– Knowledge of the adversary structure:

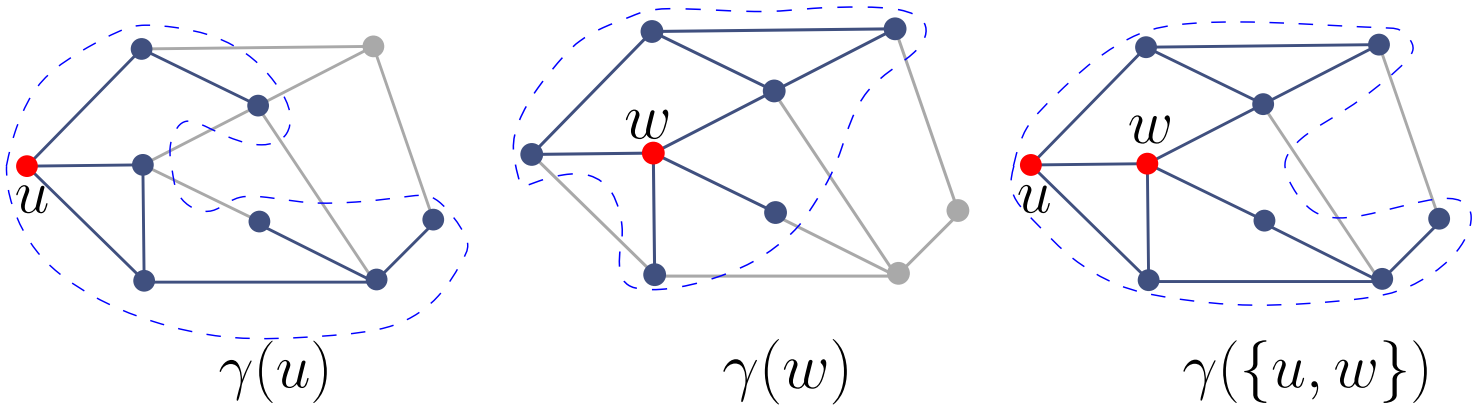
Each player u knows only the **local adversary structure** $\mathcal{Z}_u = \{S \cap V_u : S \in \mathcal{Z}\}$ (also denoted as $\mathcal{Z}^{V_u}$).



Initial knowledge of players

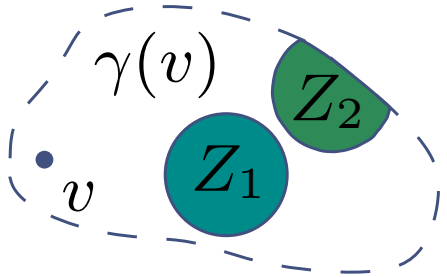
Partial knowledge model [Pagourtzis, Panagiotakos, Sakavalas, '14]

– Topology knowledge: Player u knows subgraph $\gamma(u) = (V_u, E_u)$. For set $S \subseteq V$, $\gamma(S) = (\bigcup_{u \in S} V_u, \bigcup_{u \in S} E_u)$.



– Knowledge of the adversary structure:

Each player u knows only the **local adversary structure** $\mathcal{Z}_u = \{S \cap V_u : S \in \mathcal{Z}\}$ (also denoted as $\mathcal{Z}^{V_u}$).



The Model

Adversary

- Byzantine.
- General.
- Unbounded.

The Model

Adversary

- Byzantine.
- General.
- Unbounded.

Network

- Arbitrary topology (aka incomplete).
- Synchronous.
- Authenticated channels (no tampering, known sender id).

The Model

Adversary

- Byzantine.
- General.
- Unbounded.

Network

- Arbitrary topology (aka incomplete).
- Synchronous.
- Authenticated channels (no tampering, known sender id).

Initial knowledge

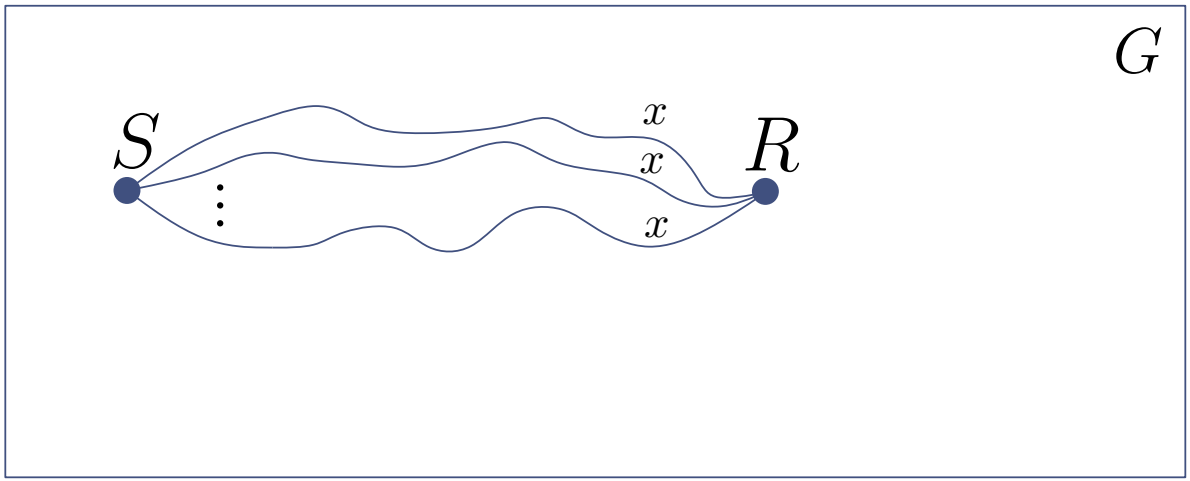
- Partial knowledge over topology and adversary.

Safe RMT algorithms [Pelc, Peleg, '05]

- Never make the receiver output (decide on) an incorrect value.

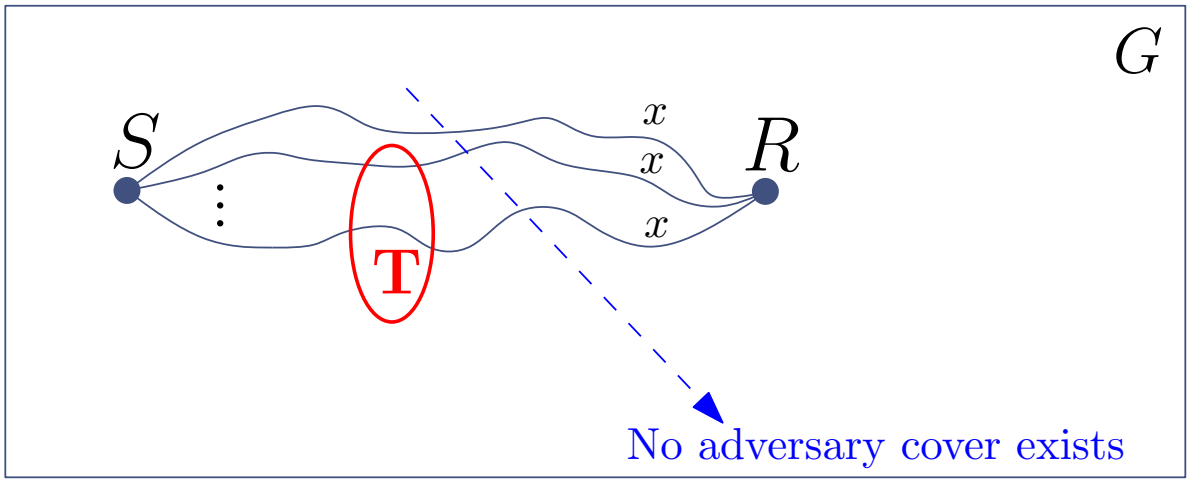
Intuition behind RMT protocols

– Known Topology: R **decides on** x upon receiving x from a set of $S \rightsquigarrow R$ paths not fully "covered" by a corruptible set.



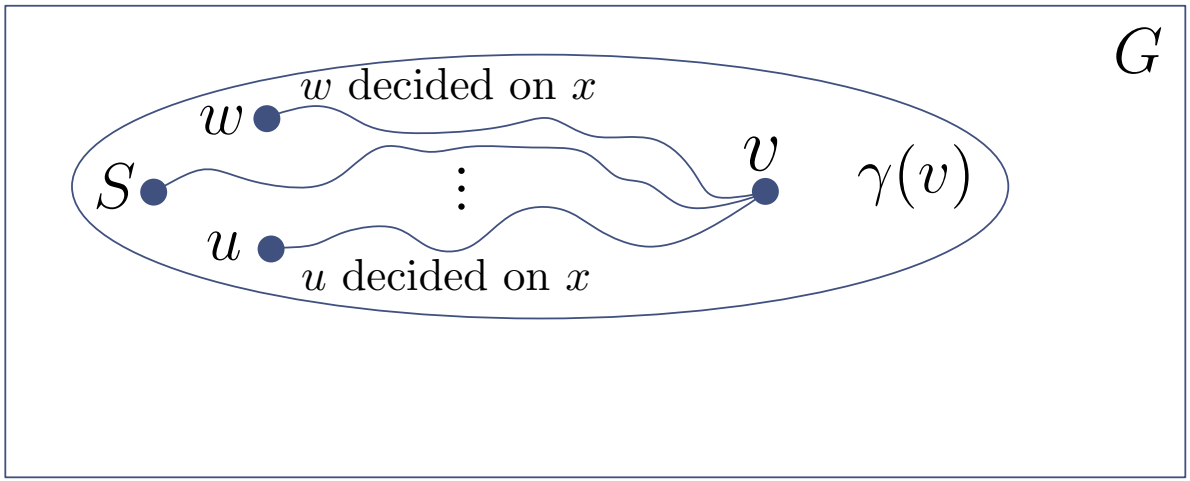
Intuition behind RMT protocols

– Known Topology: R **decides on** x upon receiving x from a set of $S \rightsquigarrow R$ paths not fully "covered" by a corruptible set.



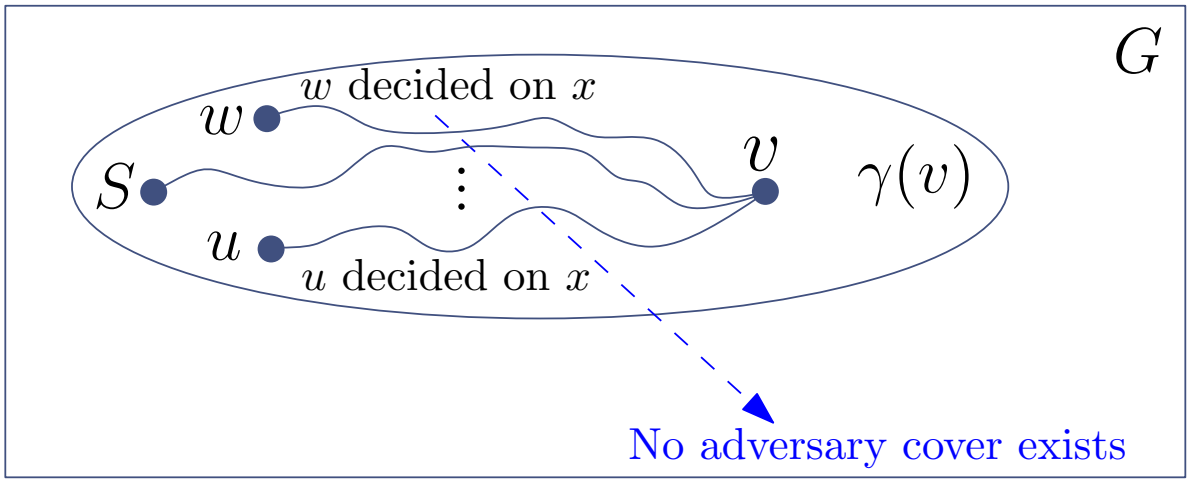
Intuition behind RMT protocols

- Known Topology: R **decides on** x upon receiving x from a set of $S \rightsquigarrow R$ paths not fully "covered" by a corruptible set.
- Partial knowledge: Node v decides on x upon receipt from a set of paths in $\gamma(v)$ not "covered" by a corruptible set.



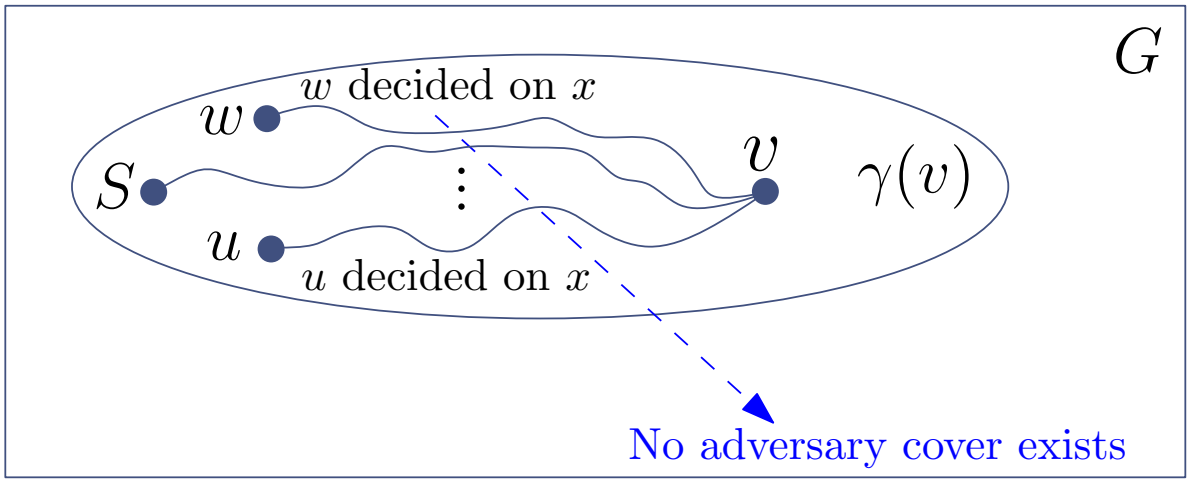
Intuition behind RMT protocols

- Known Topology: R **decides on** x upon receiving x from a set of $S \rightsquigarrow R$ paths not fully "covered" by a corruptible set.
- Partial knowledge: Node v decides on x upon receipt from a set of paths in $\gamma(v)$ not "covered" by a corruptible set.



Intuition behind RMT protocols

- Known Topology: R **decides on** x upon receiving x from a set of $S \rightsquigarrow R$ paths not fully "covered" by a corruptible set.
- Partial knowledge: Node v decides on x upon receipt from a set of paths in $\gamma(v)$ not "covered" by a corruptible set.



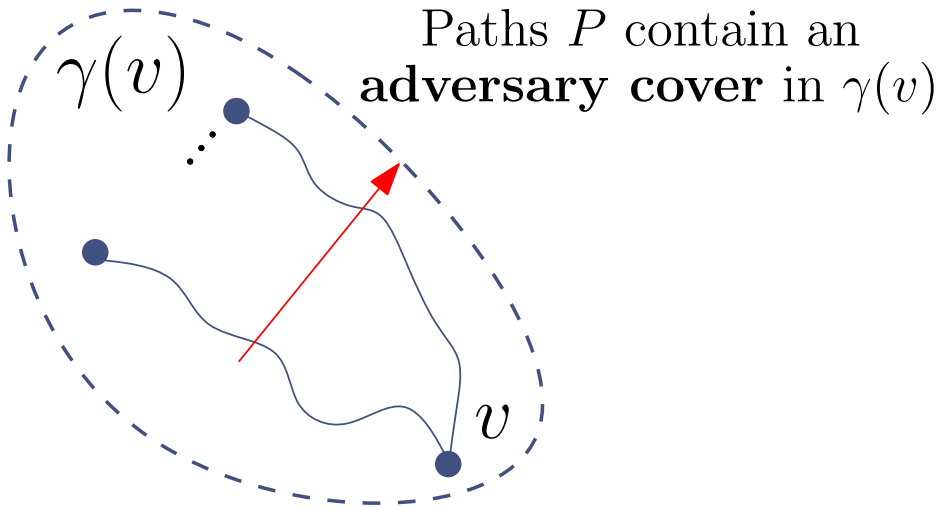
Algorithm (GPPA) tight for local knowledge [PPS14]!

Exchange of Knowledge

- GPPA not generally tight.
- **Knowledge exchange** helps in the general case.

Exchange of Knowledge

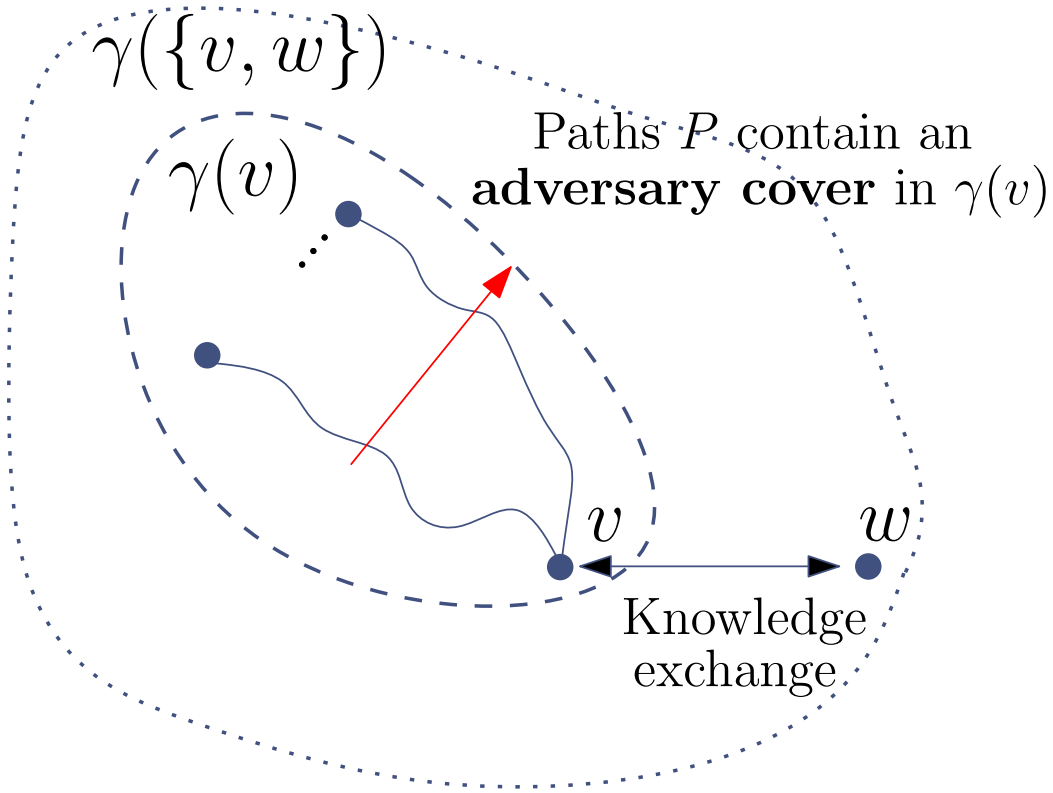
- GPPA not generally tight.
- **Knowledge exchange** helps in the general case.



Exchange of Knowledge

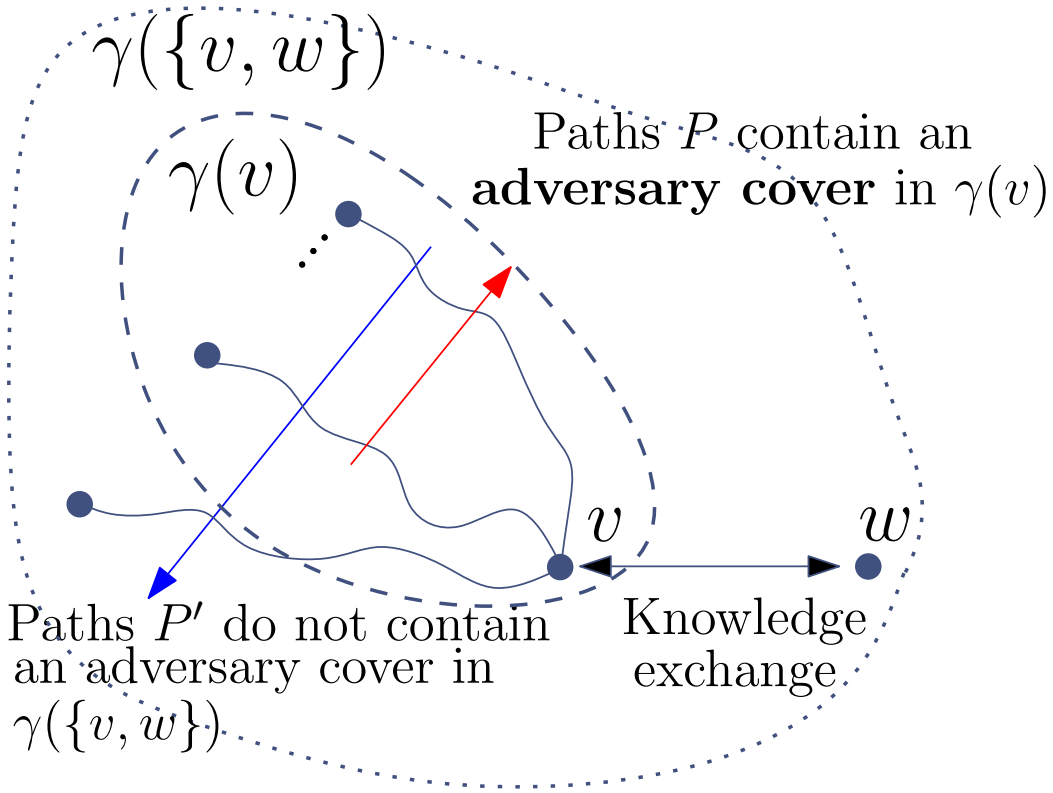
– GPPA not generally tight.

– **Knowledge exchange** helps in the general case.



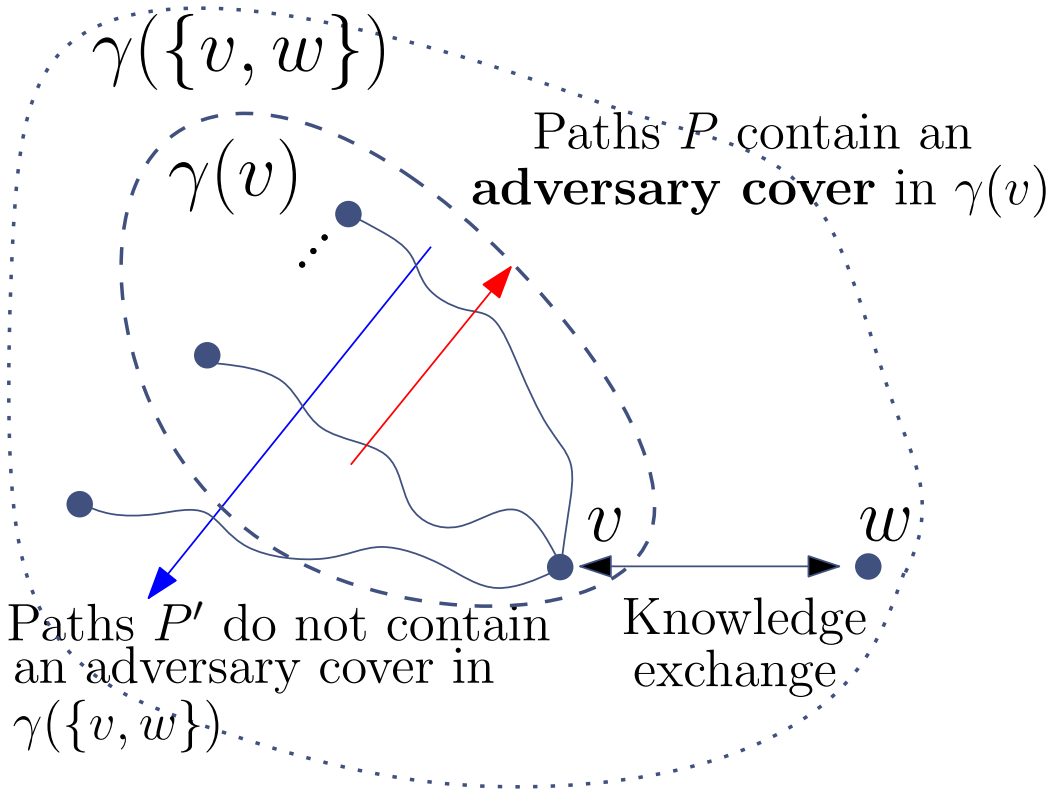
Exchange of Knowledge

- GPPA not generally tight.
- **Knowledge exchange** helps in the general case.



Exchange of Knowledge

- GPPA not generally tight.
- **Knowledge exchange** helps in the general case.



Knowledge Exchange between v, w

- **Joining topology knowledge**: trivially $\gamma(\{v, w\})$
- **Joining local adversary structures** $\mathcal{Z}_v, \mathcal{Z}_w$?

Joining Local Adversary Structures

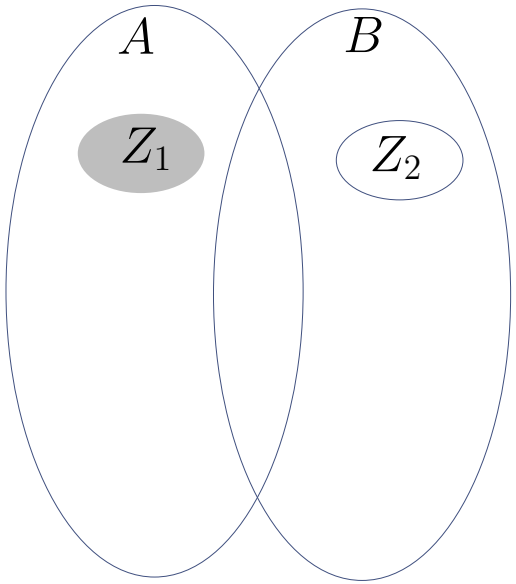
$\mathcal{Z}^A = \{Z \cap A \mid Z \in \mathcal{Z}\}$.

For $\mathcal{Z}^A, \mathcal{Z}^B$, define (worst case) joint structure $\mathcal{Z}^A \oplus \mathcal{Z}^B$:

Joining Local Adversary Structures

$\mathcal{Z}^A = \{Z \cap A \mid Z \in \mathcal{Z}\}$.

For $\mathcal{Z}^A, \mathcal{Z}^B$, define (worst case) joint structure $\mathcal{Z}^A \oplus \mathcal{Z}^B$:

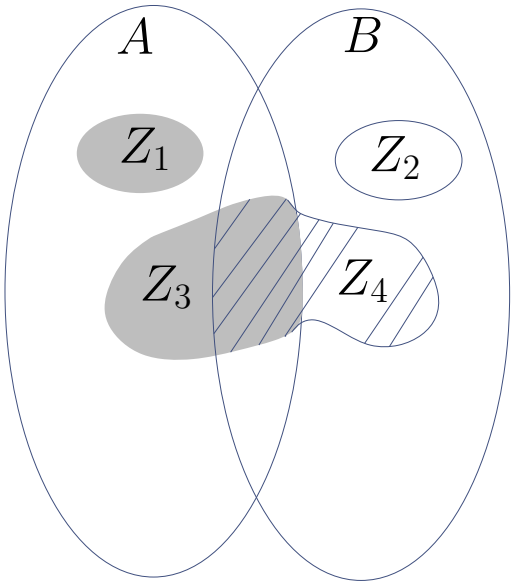


– $\mathcal{Z}^A \oplus \mathcal{Z}^B$ should contain $Z_1 \cup Z_2$.

Joining Local Adversary Structures

$\mathcal{Z}^A = \{Z \cap A \mid Z \in \mathcal{Z}\}$.

For $\mathcal{Z}^A, \mathcal{Z}^B$, define (worst case) joint structure $\mathcal{Z}^A \oplus \mathcal{Z}^B$:

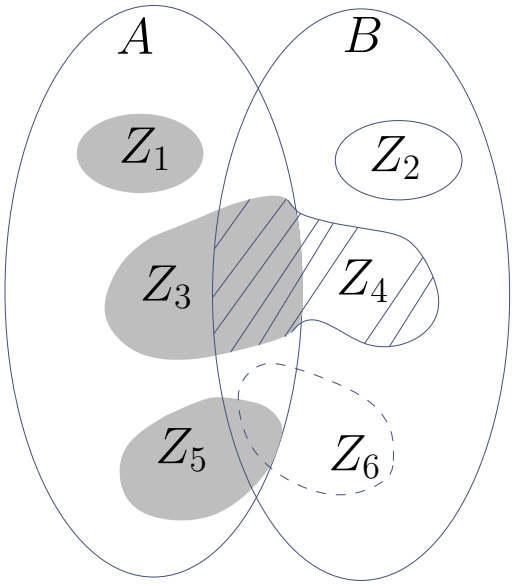


- $\mathcal{Z}^A \oplus \mathcal{Z}^B$ should contain $Z_1 \cup Z_2$.
- $\mathcal{Z}^A \oplus \mathcal{Z}^B$ should contain $Z_3 \cup Z_4$.

Joining Local Adversary Structures

$\mathcal{Z}^A = \{Z \cap A \mid Z \in \mathcal{Z}\}$.

For $\mathcal{Z}^A, \mathcal{Z}^B$, define (worst case) joint structure $\mathcal{Z}^A \oplus \mathcal{Z}^B$:

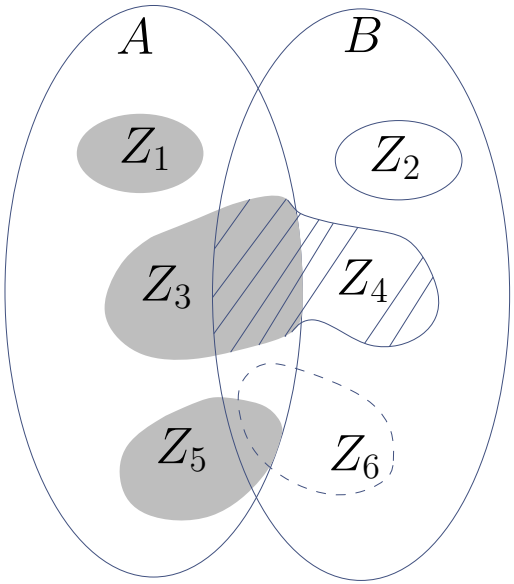


- $\mathcal{Z}^A \oplus \mathcal{Z}^B$ should contain $Z_1 \cup Z_2$.
- $\mathcal{Z}^A \oplus \mathcal{Z}^B$ should contain $Z_3 \cup Z_4$.
- $\mathcal{Z}^A \oplus \mathcal{Z}^B$ should not contain $Z_5 \cup Z_6$.

Joining Local Adversary Structures

$\mathcal{Z}^A = \{Z \cap A \mid Z \in \mathcal{Z}\}$.

For $\mathcal{Z}^A, \mathcal{Z}^B$, define (worst case) joint structure $\mathcal{Z}^A \oplus \mathcal{Z}^B$:



- $\mathcal{Z}^A \oplus \mathcal{Z}^B$ should contain $Z_1 \cup Z_2$.
- $\mathcal{Z}^A \oplus \mathcal{Z}^B$ should contain $Z_3 \cup Z_4$.
- $\mathcal{Z}^A \oplus \mathcal{Z}^B$ should not contain $Z_5 \cup Z_6$.

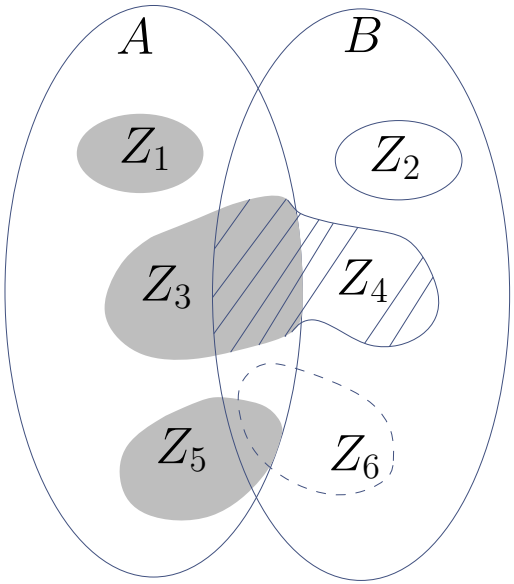
Join Operation $\oplus$

$$\mathcal{Z}^A \oplus \mathcal{Z}^B = \{Z_1 \cup Z_2 | (Z_1 \in \mathcal{Z}^A) \wedge (Z_2 \in \mathcal{Z}^B) \wedge (Z_1 \cap B = Z_2 \cap A)\}$$

Joining Local Adversary Structures

$\mathcal{Z}^A = \{Z \cap A \mid Z \in \mathcal{Z}\}$.

For $\mathcal{Z}^A, \mathcal{Z}^B$, define (worst case) joint structure $\mathcal{Z}^A \oplus \mathcal{Z}^B$:



- $\mathcal{Z}^A \oplus \mathcal{Z}^B$ should contain $Z_1 \cup Z_2$.
- $\mathcal{Z}^A \oplus \mathcal{Z}^B$ should contain $Z_3 \cup Z_4$.
- $\mathcal{Z}^A \oplus \mathcal{Z}^B$ should not contain $Z_5 \cup Z_6$.

Join Operation $\oplus$

$$\mathcal{Z}^A \oplus \mathcal{Z}^B = \{Z_1 \cup Z_2 | (Z_1 \in \mathcal{Z}^A) \wedge (Z_2 \in \mathcal{Z}^B) \wedge (Z_1 \cap B = Z_2 \cap A)\}$$

Definition extends to different structures: $\mathcal{Z}^A \oplus \mathcal{Z}'^B$ (false structure report by adversary).

Semilattice structure of partial knowledge

Theorem

Let $\mathbb{T} = \{\mathcal{Z}^A \mid \mathcal{Z} \subseteq 2^V, A \subseteq V\}$ *the space of all possible* $\mathcal{Z}^A$.
$\langle \mathbb{T}, \oplus \rangle$ *is a semilattice.*

Semilattice structure of partial knowledge

Theorem

Let $\mathbb{T} = \{\mathcal{Z}^A \mid \mathcal{Z} \subseteq 2^V, A \subseteq V\}$ *the space of all possible* $\mathcal{Z}^A$. $\langle \mathbb{T}, \oplus \rangle$ *is a semilattice.*

Proof. Operation $\oplus$ is commutative, associative, idempotent. $\square$

Semilattice structure of partial knowledge

Theorem

Let $\mathbb{T} = \{\mathcal{Z}^A \mid \mathcal{Z} \subseteq 2^V, A \subseteq V\}$ *the space of all possible* $\mathcal{Z}^A$. $\langle \mathbb{T}, \oplus \rangle$ *is a semilattice.*

Proof. Operation $\oplus$ is commutative, associative, idempotent. $\square$

Semilattices facts

1. $\oplus$ induces a partial order " $\succcurlyeq$ " on $\mathbb{T}$ by $x \succcurlyeq y \Leftrightarrow x = x \oplus y$.

Semilattice structure of partial knowledge

Theorem

Let $\mathbb{T} = \{\mathcal{Z}^A \mid \mathcal{Z} \subseteq 2^V, A \subseteq V\}$ *the space of all possible* $\mathcal{Z}^A$. $\langle \mathbb{T}, \oplus \rangle$ *is a semilattice.*

Proof. Operation $\oplus$ is commutative, associative, idempotent. $\square$

Semilattices facts

1. $\oplus$ induces a partial order "$\succcurlyeq$" on $\mathbb{T}$ by $x \succcurlyeq y \Leftrightarrow x = x \oplus y$.
2. Every nonempty finite subset of $\mathbb{T}$ has a supremum w.r.t. $\succcurlyeq$.

Semilattice structure of partial knowledge

Theorem

Let $\mathbb{T} = \{\mathcal{Z}^A \mid \mathcal{Z} \subseteq 2^V, A \subseteq V\}$ *the space of all possible* $\mathcal{Z}^A$. $\langle \mathbb{T}, \oplus \rangle$ *is a semilattice.*

Proof. Operation $\oplus$ is commutative, associative, idempotent. $\square$

Semilattices facts

1. $\oplus$ induces a partial order "$\succcurlyeq$" on $\mathbb{T}$ by $x \succcurlyeq y \Leftrightarrow x = x \oplus y$.
2. Every nonempty finite subset of $\mathbb{T}$ has a supremum w.r.t. $\succcurlyeq$.
3. $\sup\{x, y\} = x \oplus y$ (join).

Semilattice structure of partial knowledgetle

Theorem (Induced partial order)

Operation $\oplus$ *induces partial order "* $\succcurlyeq$ *"* *on* $\mathbb{T}$*:*

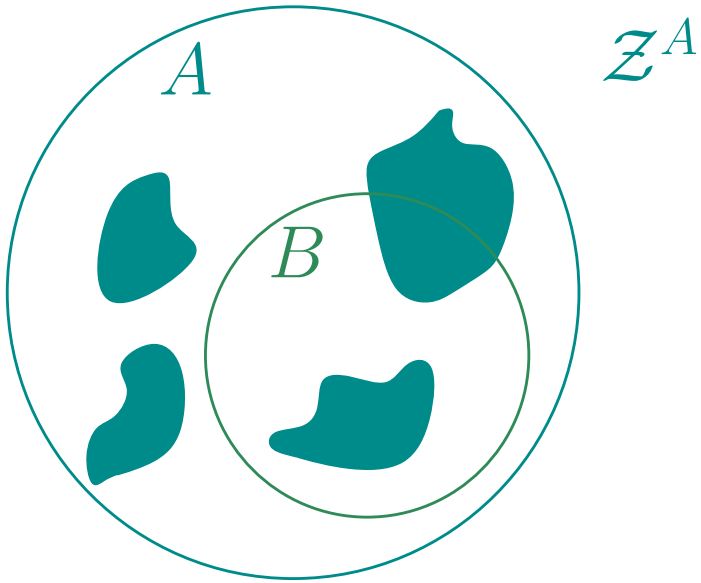
$$\mathcal{Z}^A \succcurlyeq \mathcal{Z}'^B \Leftrightarrow (A \supseteq B) \wedge \left((\mathcal{Z}^A)^B \subseteq \mathcal{Z}'^B \right)$$

Semilattice structure of partial knowledgetle

Theorem (Induced partial order)

Operation $\oplus$ *induces partial order "* $\succcurlyeq$ *"* *on* $\mathbb{T}$*:*

$$\mathcal{Z}^A \succcurlyeq \mathcal{Z}'^B \Leftrightarrow (A \supseteq B) \wedge \left((\mathcal{Z}^A)^B \subseteq \mathcal{Z}'^B \right)$$

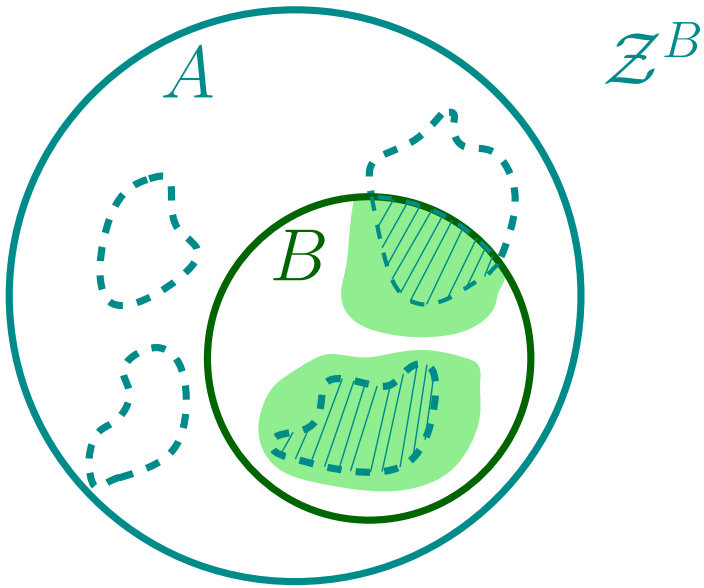


Semilattice structure of partial knowledgetle

Theorem (Induced partial order)

Operation $\oplus$ induces partial order "$\succcurlyeq$" on $\mathbb{T}$:

$$\mathcal{Z}^A \succcurlyeq \mathcal{Z}'^B \Leftrightarrow (A \supseteq B) \wedge \left((\mathcal{Z}^A)^B \subseteq \mathcal{Z}'^B \right)$$

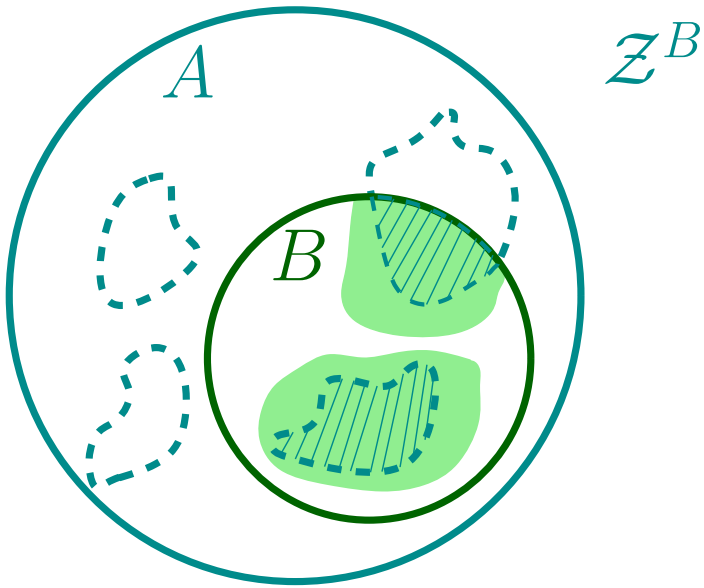


Semilattice structure of partial knowledgetle

Theorem (Induced partial order)

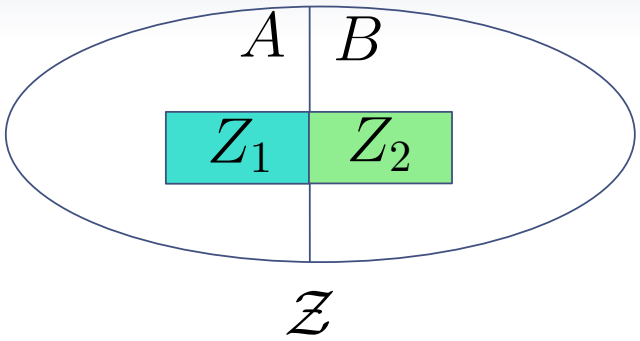
Operation $\oplus$ induces partial order "$\succcurlyeq$" on $\mathbb{T}$:

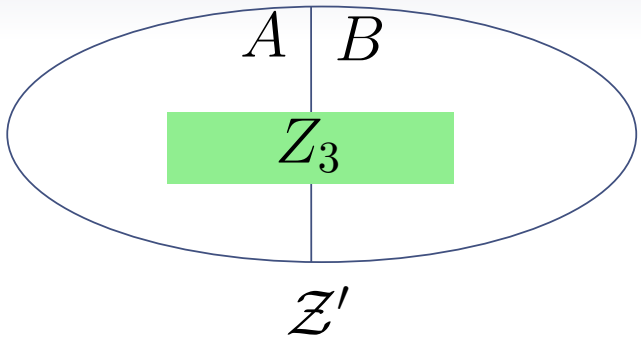
$$\mathcal{Z}^A \succcurlyeq \mathcal{Z}'^B \Leftrightarrow (A \supseteq B) \wedge \left((\mathcal{Z}^A)^B \subseteq \mathcal{Z}'^B \right)$$



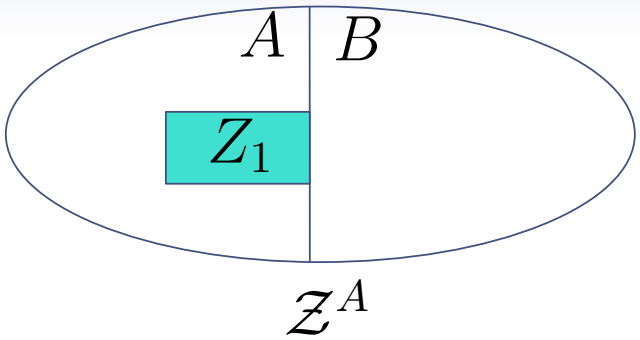
Proof. By (1) and definition of $\oplus$.

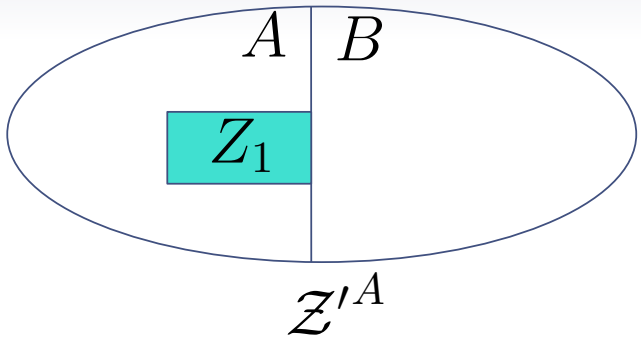
Maximality of $\mathcal{Z}^A \oplus \mathcal{Z}^B$



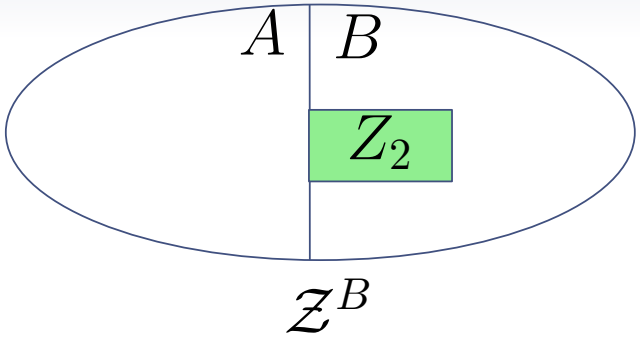


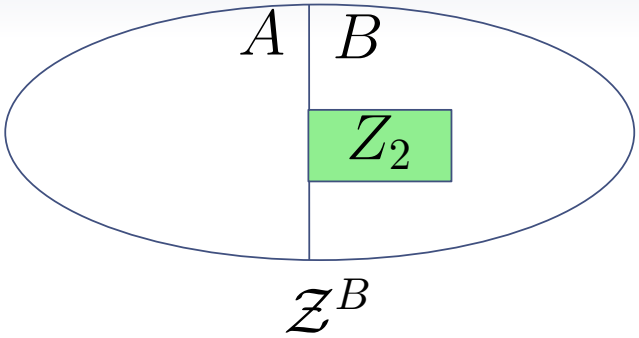
Maximality of $\mathcal{Z}^A \oplus \mathcal{Z}^B$



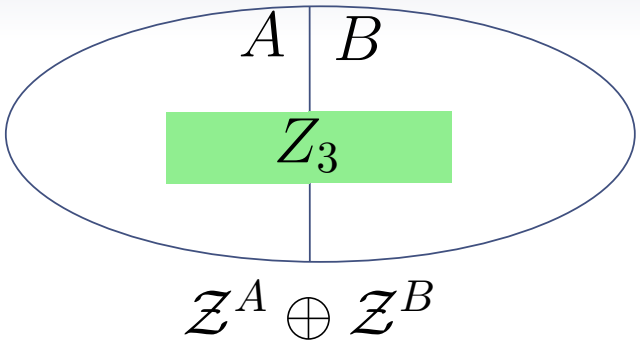


Maximality of $\mathcal{Z}^A \oplus \mathcal{Z}^B$

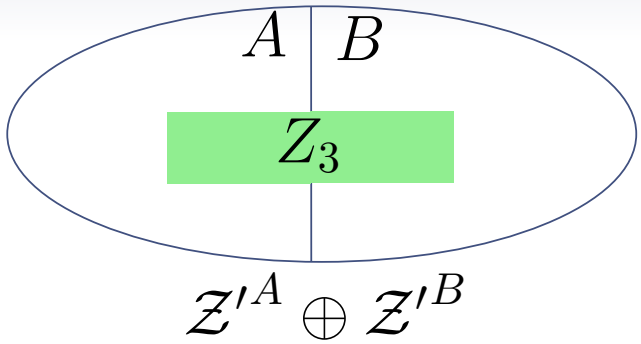




Maximality of $\mathcal{Z}^A \oplus \mathcal{Z}^B$

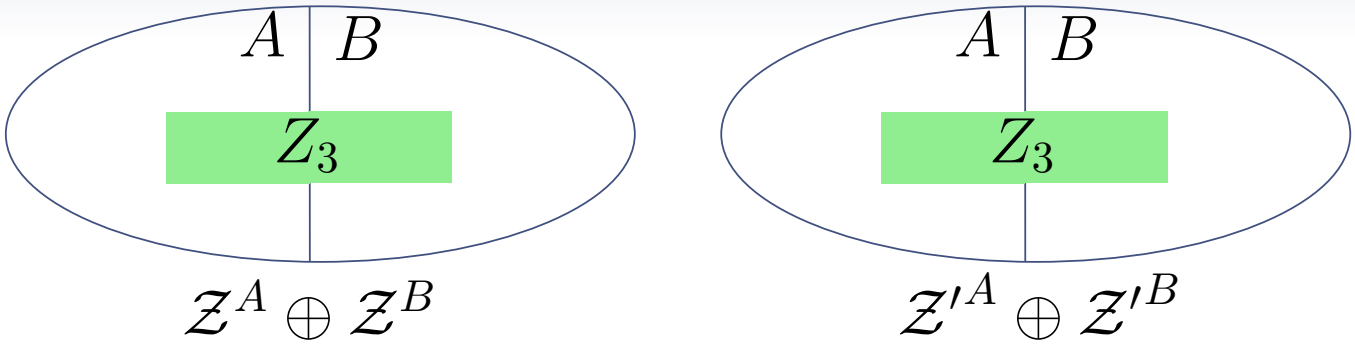


$\mathcal{Z}^A \oplus \mathcal{Z}^B$



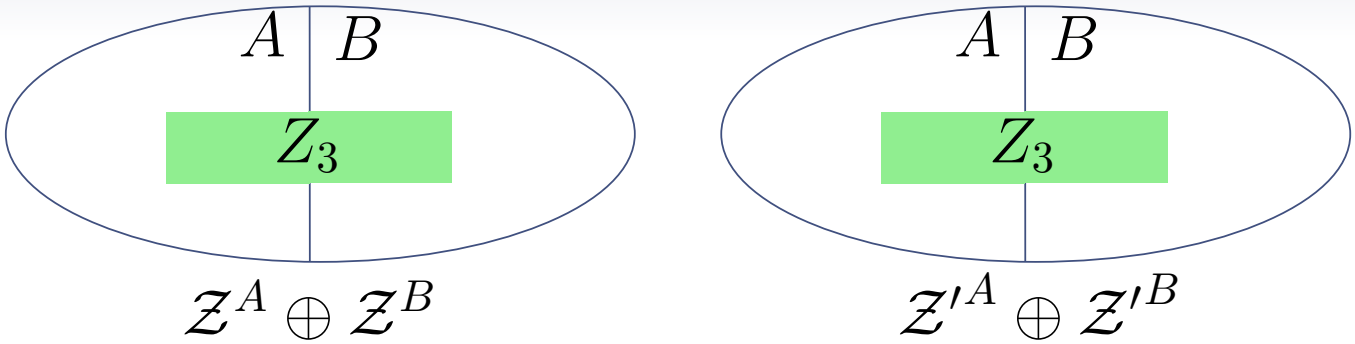
$\mathcal{Z}'^A \oplus \mathcal{Z}'^B$

Maximality of $\mathcal{Z}^A \oplus \mathcal{Z}^B$



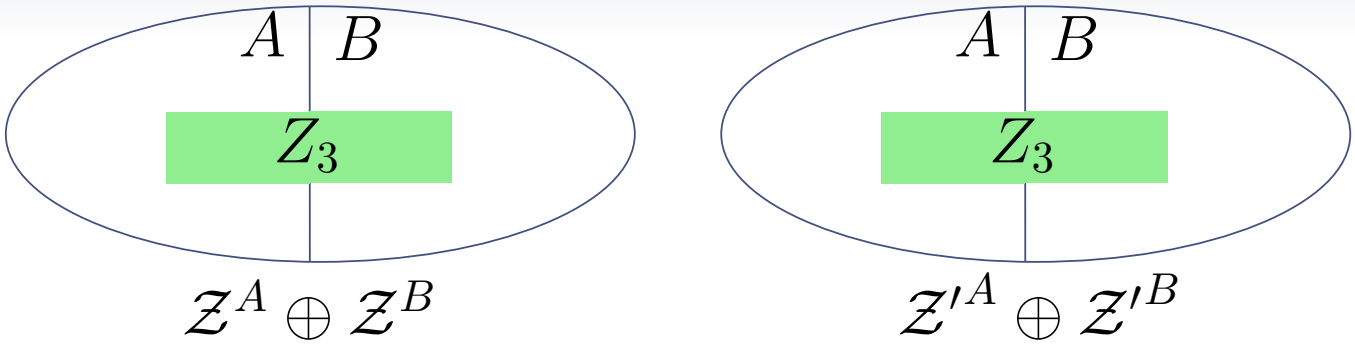
– $\mathcal{Z}^A \oplus \mathcal{Z}^B$: worst possible case compatible with local knowledge?

Maximality of $\mathcal{Z}^A \oplus \mathcal{Z}^B$



– $\mathcal{Z}^A \oplus \mathcal{Z}^B$: worst possible case compatible with local knowledge?
– Are there corruptible subsets of $A \cup B$ not included in $\mathcal{Z}^A \oplus \mathcal{Z}^B$?

Maximality of $\mathcal{Z}^A \oplus \mathcal{Z}^B$

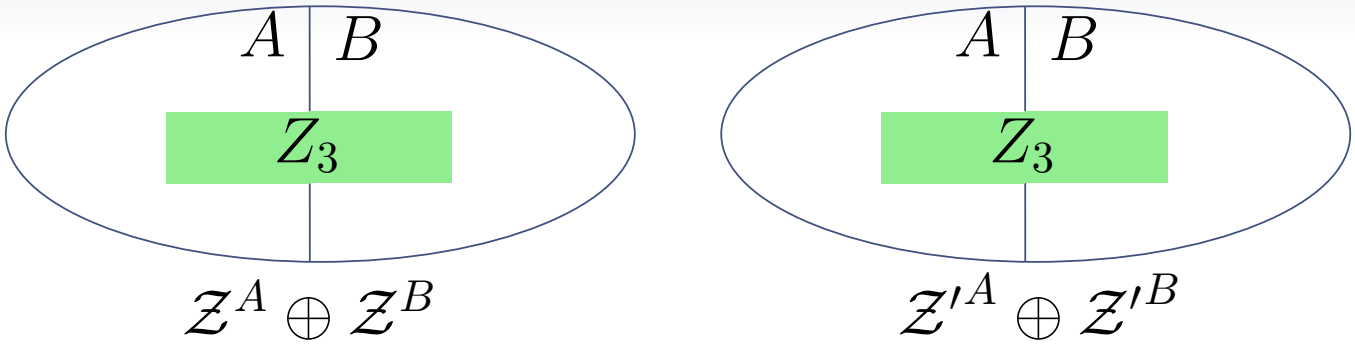


– $\mathcal{Z}^A \oplus \mathcal{Z}^B$: worst possible case compatible with local knowledge?
– Are there corruptible subsets of $A \cup B$ not included in $\mathcal{Z}^A \oplus \mathcal{Z}^B$?

Theorem

For structure $\mathcal{Z}$ and $A, B \subseteq V$, it holds that $\mathcal{Z}^{(A \cup B)} \subseteq \mathcal{Z}^A \oplus \mathcal{Z}^B$.

Maximality of $\mathcal{Z}^A \oplus \mathcal{Z}^B$



– $\mathcal{Z}^A \oplus \mathcal{Z}^B$: worst possible case compatible with local knowledge?
– Are there corruptible subsets of $A \cup B$ not included in $\mathcal{Z}^A \oplus \mathcal{Z}^B$?

Theorem

For structure $\mathcal{Z}$ and $A, B \subseteq V$, it holds that $\mathcal{Z}^{(A \cup B)} \subseteq \mathcal{Z}^A \oplus \mathcal{Z}^B$.

Proof.

$$\left.\begin{array}{l} \mathcal{Z}^{(A\cup B)} \succcurlyeq \mathcal{Z}^A, \mathcal{Z}^B \\ \mathcal{Z}^A \oplus \mathcal{Z}^B = \sup\{\mathcal{Z}^A, \mathcal{Z}^B\} \end{array}\right\} \Rightarrow \mathcal{Z}^{(A\cup B)} \succcurlyeq \mathcal{Z}^A \oplus \mathcal{Z}^B \Rightarrow \ldots \quad \square$$

RMT cut

Joint Adversary Structure: Maximum possible adversary structure w.r.t the initial knowledge of players in B.

$$\mathcal{Z}_B = \bigoplus_{u \in B} \mathcal{Z}^{V_u}$$

RMT cut

Joint Adversary Structure: Maximum possible adversary structure w.r.t the initial knowledge of players in B.

$$\mathcal{Z}_B = \bigoplus_{u \in B} \mathcal{Z}^{V_u}$$

RMT cut

Node cut $C = T \cup H$, cut of G, disconnecting $S \in A$ from $R \in B$ s.t. $T \in \mathcal{Z}$ and $H \cap \gamma(B) \in \mathcal{Z}_B$. ($B$: connected component)

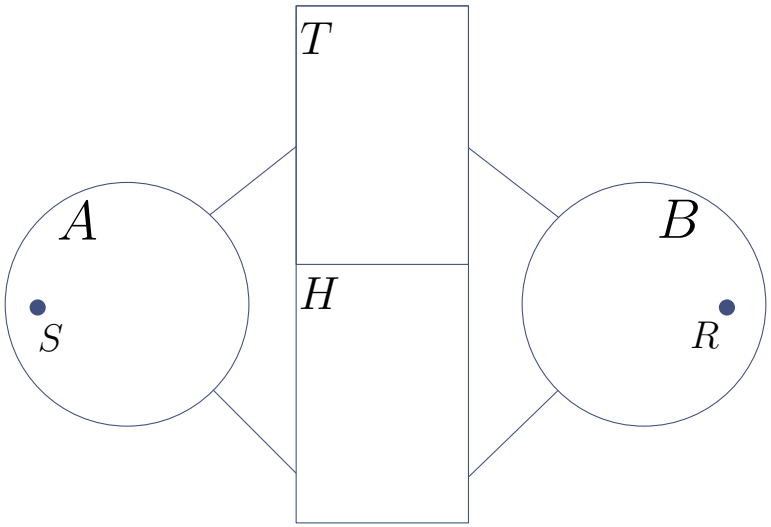
RMT cut

Joint Adversary Structure: Maximum possible adversary structure w.r.t the initial knowledge of players in B.

$$\mathcal{Z}_B = \bigoplus_{u \in B} \mathcal{Z}^{V_u}$$

RMT cut

Node cut $C = T \cup H$, cut of G, disconnecting $S \in A$ from $R \in B$ s.t. $T \in \mathcal{Z}$ and $H \cap \gamma(B) \in \mathcal{Z}_B$. ($B$: connected component)



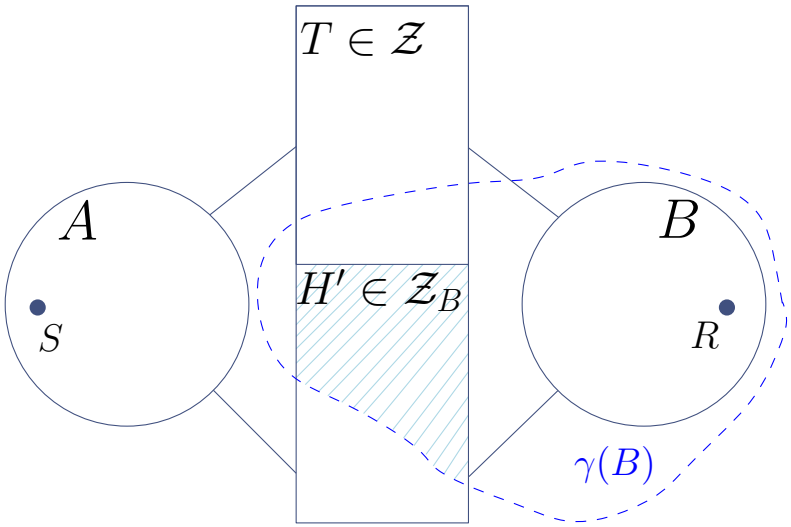
RMT cut

Joint Adversary Structure: Maximum possible adversary structure w.r.t the initial knowledge of players in B.

$$\mathcal{Z}_B = \bigoplus_{u \in B} \mathcal{Z}^{V_u}$$

RMT cut

Node cut $C = T \cup H$, cut of G, disconnecting $S \in A$ from $R \in B$ s.t. $T \in \mathcal{Z}$ and $H \cap \gamma(B) \in \mathcal{Z}_B$. ($B$: connected component)



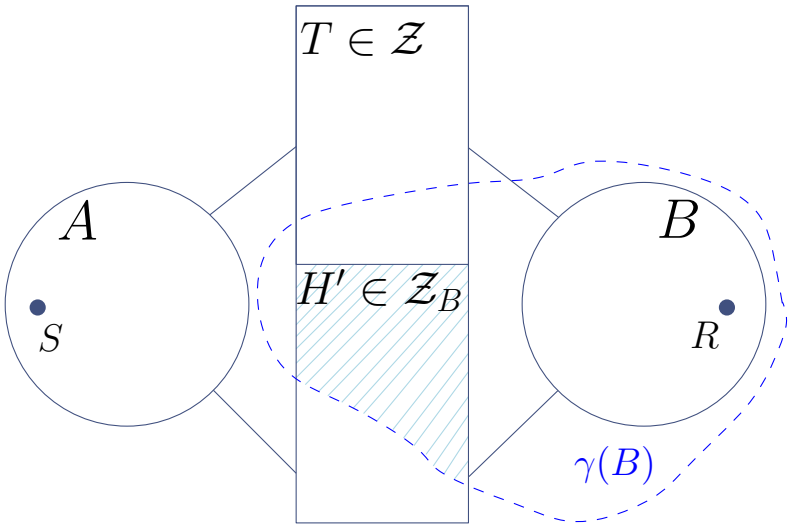
RMT cut

Joint Adversary Structure: Maximum possible adversary structure w.r.t the initial knowledge of players in B.

$$\mathcal{Z}_B = \bigoplus_{u \in B} \mathcal{Z}^{V_u}$$

RMT cut

Node cut $C = T \cup H$, cut of G, disconnecting $S \in A$ from $R \in B$ s.t. $T \in \mathcal{Z}$ and $H \cap \gamma(B) \in \mathcal{Z}_B$. ($B$: connected component)



- T is corruptible.
- H "looks" corruptible to B.

RMT Impossibility

Theorem (Necessary condition for safe RMT)

If an RMT-cut exists for instance $(G, \mathcal{Z}, S, R)$ then no safe algorithm $\mathcal{A}$ can achieve RMT in $(G, \mathcal{Z}, S, R)$.

RMT Impossibility

Theorem (Necessary condition for safe RMT)

If an RMT-cut exists for instance $(G, \mathcal{Z}, S, R)$ *then no safe algorithm* $\mathcal{A}$ *can achieve RMT in* $(G, \mathcal{Z}, S, R)$.

* Safe Algorithm [Pelc, Peleg '05]: Either R is sure for the sender's value or does not decide at all.

RMT Impossibility

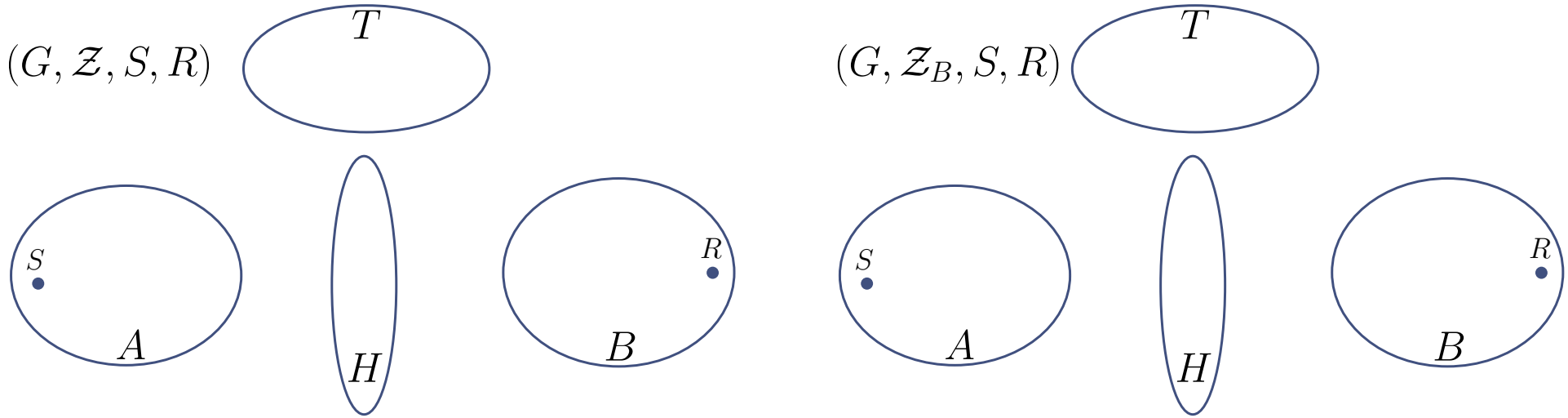
Theorem (Necessary condition for safe RMT)

If an RMT-cut exists for instance $(G, \mathcal{Z}, S, R)$ *then no safe algorithm* $\mathcal{A}$ *can achieve RMT in* $(G, \mathcal{Z}, S, R)$.

* Safe Algorithm [Pelc, Peleg '05]: Either R is sure for the sender's value or does not decide at all.
(roughly non-safe makes assumptions that might not hold.)

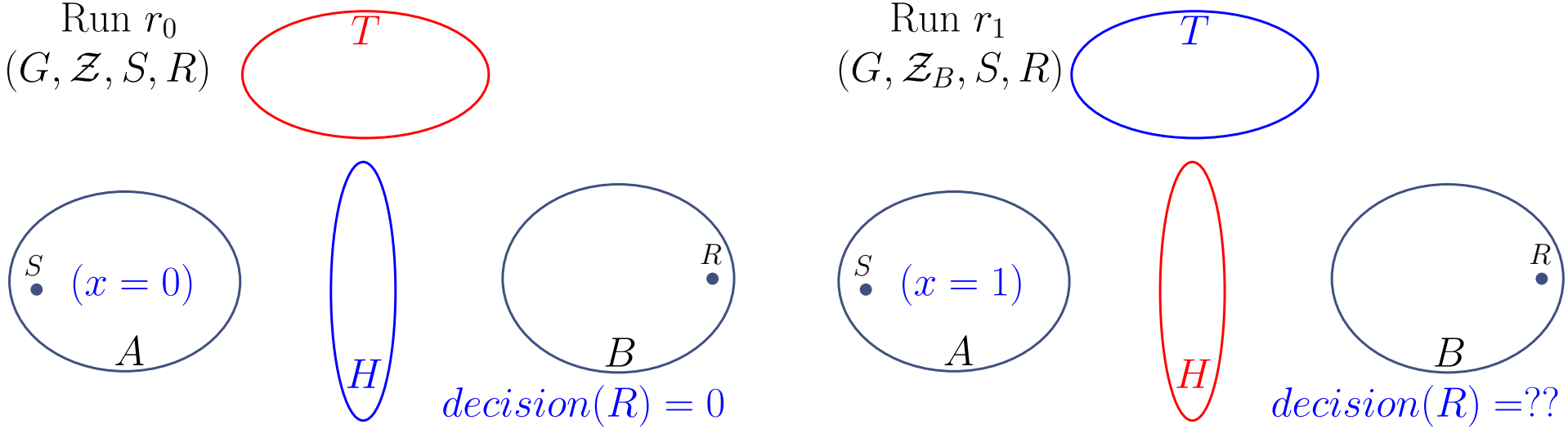
Proof Sketch
(Conflicting indistinguishable executions)

Assume that a safe algorithm $\mathcal{A}$ achieves RMT in $(G, \mathcal{Z}, S, R)$ with RMT cut $C = T \cup H$. What about $(G, \mathcal{Z}_B, S, R)$?



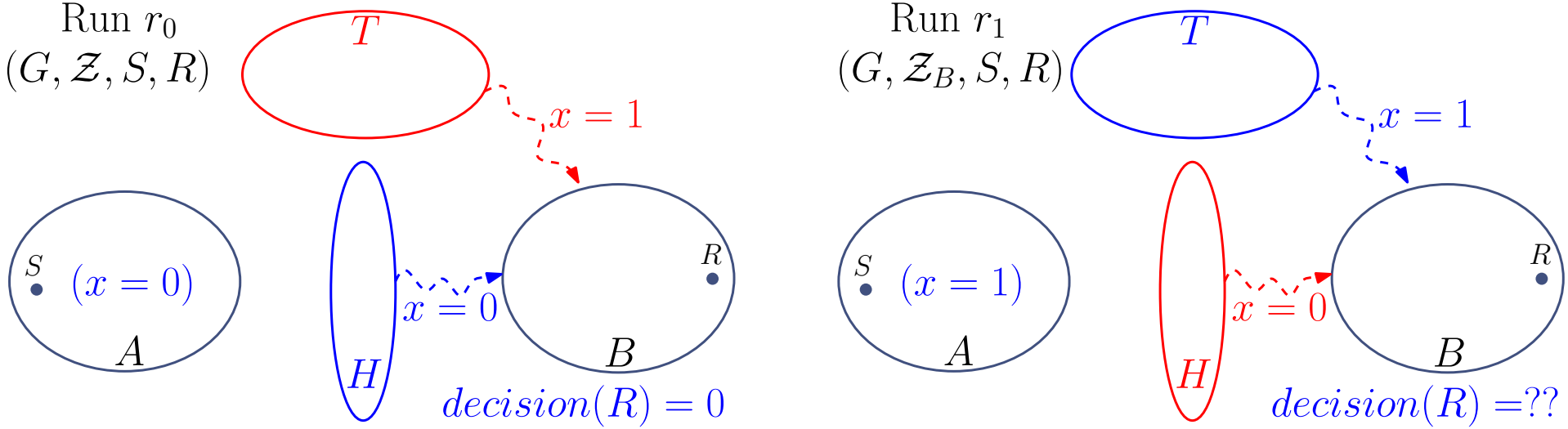
Proof Sketch
(Conflicting indistinguishable executions)

Assume that a safe algorithm $\mathcal{A}$ achieves RMT in $(G, \mathcal{Z}, S, R)$ with RMT cut $C = T \cup H$. What about $(G, \mathcal{Z}_B, S, R)$?



Proof Sketch
(Conflicting indistinguishable executions)

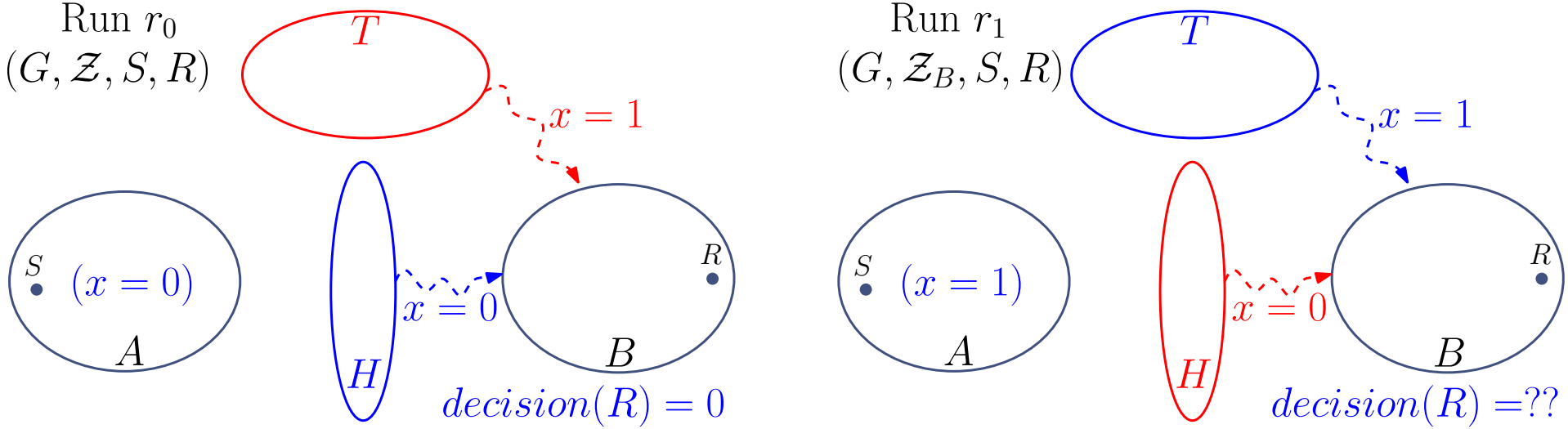
Assume that a safe algorithm $\mathcal{A}$ achieves RMT in $(G, \mathcal{Z}, S, R)$ with RMT cut $C = T \cup H$. What about $(G, \mathcal{Z}_B, S, R)$?



Corrupted players of r_i act as honest in r_{1-i}.

Proof Sketch
(Conflicting indistinguishable executions)

Assume that a safe algorithm $\mathcal{A}$ achieves RMT in $(G, \mathcal{Z}, S, R)$ with RMT cut $C = T \cup H$. What about $(G, \mathcal{Z}_B, S, R)$?

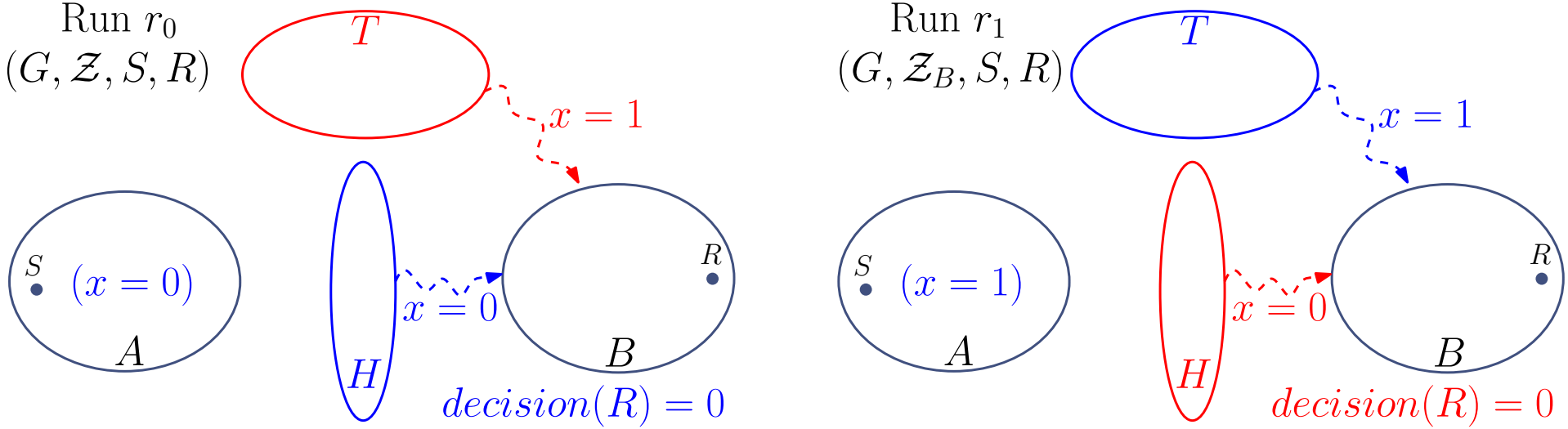


Corrupted players of r_i act as honest in r_{1-i}.

– Runs r_0, r_1, indistinguishable to the set of nodes B (same joint knowledge and joint view).

Proof Sketch
(Conflicting indistinguishable executions)

Assume that a safe algorithm $\mathcal{A}$ achieves RMT in $(G, \mathcal{Z}, S, R)$ with RMT cut $C = T \cup H$. What about $(G, \mathcal{Z}_B, S, R)$?



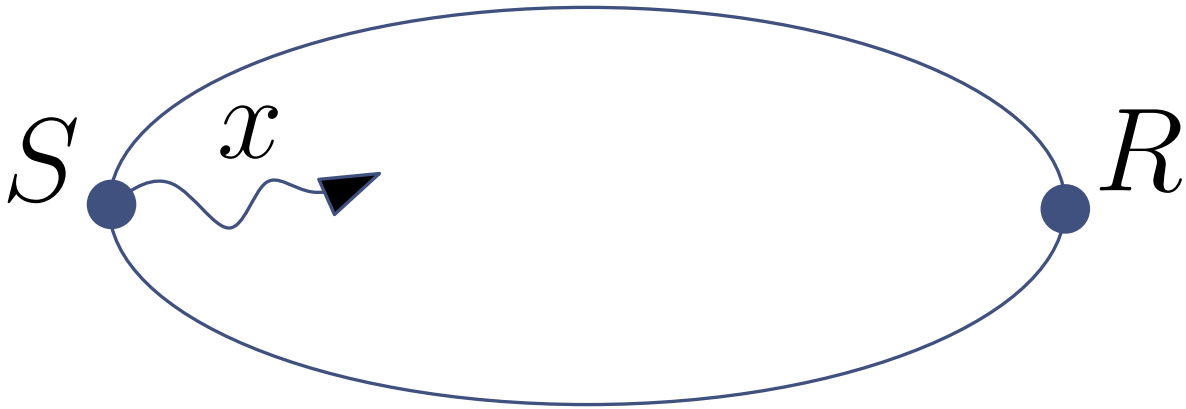
Corrupted players of r_i act as honest in r_{1-i}.

- Runs r_0, r_1, indistinguishable to the set of nodes B (same joint knowledge and joint view).
- R decides on the same value 0 in both runs, thus $\mathcal{A}$ is not safe.

RMT-PKA Outline

Propagation Phase

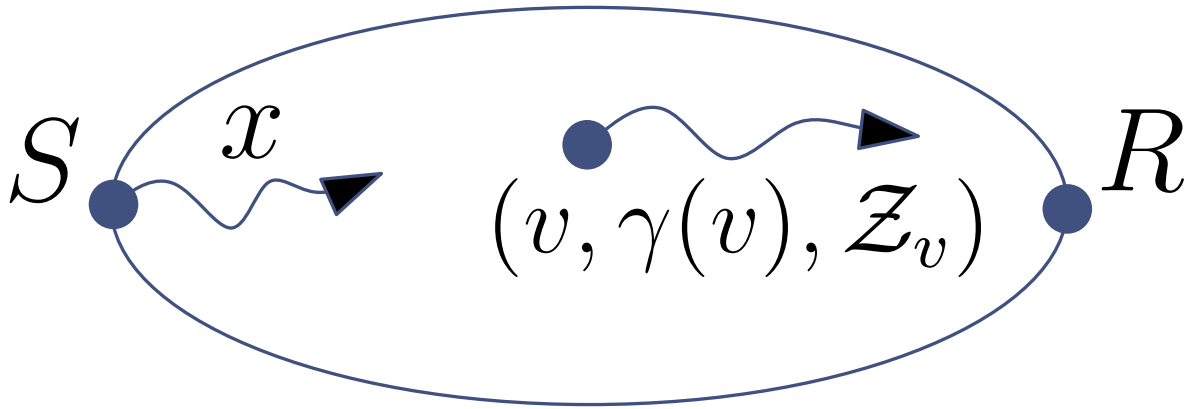
– Dealer's value is propagated throughout the graph.



RMT-PKA Outline

Propagation Phase

- Dealer's value is propagated throughout the graph.
- Each player propagates its initial knowledge $(\gamma(v), \mathcal{Z}_v)$.



RMT- Partial Knowledge Algorithm

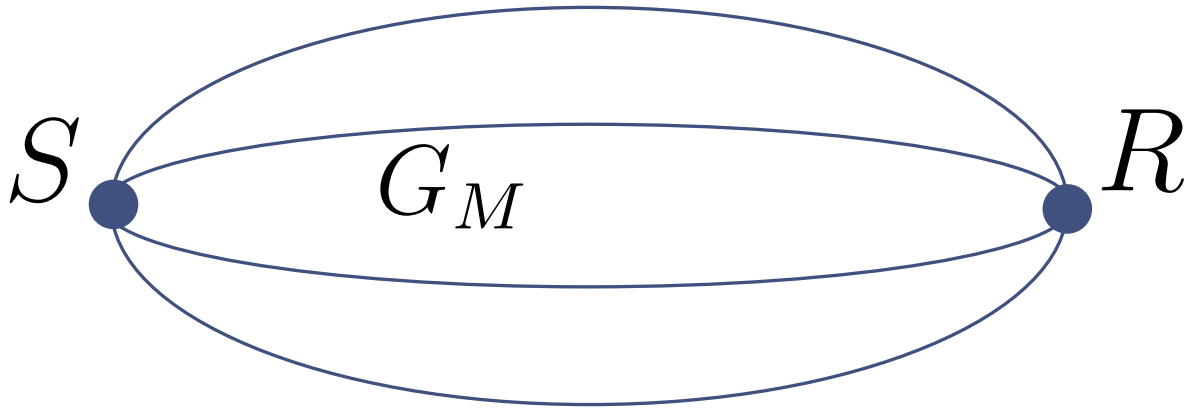
RMT-PKA Outline

Propagation Phase

- Dealer's value is propagated throughout the graph.
- Each player propagates its initial knowledge $(\gamma(v), \mathcal{Z}_v)$.

Decision Phase

- Identifies a "non-contradicting" set of messages M.
- Creates subgraph G_M implied by messages M.



RMT- Partial Knowledge Algorithm

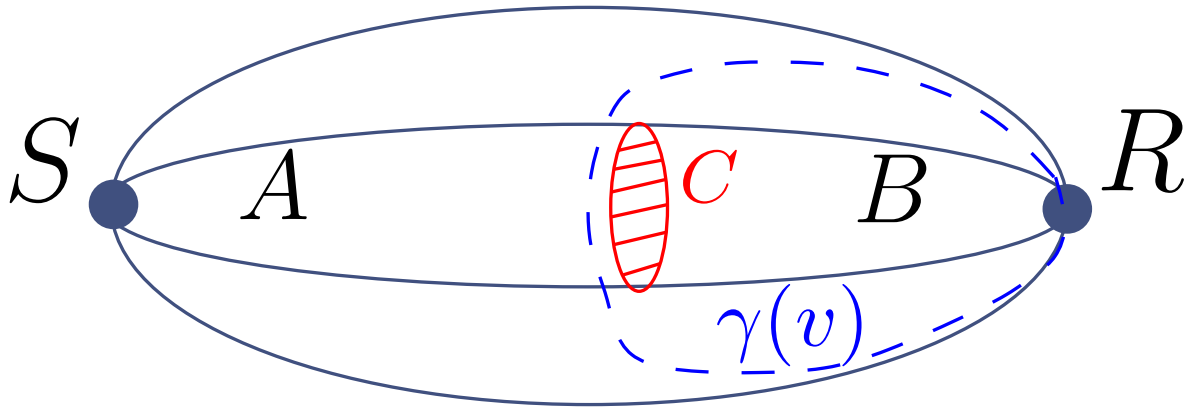
RMT-PKA Outline

Propagation Phase

- Dealer's value is propagated throughout the graph.
- Each player propagates its initial knowledge $(\gamma(v), \mathcal{Z}_v)$.

Decision Phase

- Identifies a "non-contradicting" set of messages M.
- Creates subgraph G_M implied by messages M.
- Decides on value propagated by M if G_M does not have an adversary cover. $(C \cap \gamma(B) \in \mathcal{Z}_B)$



Optimal Resilience of RMT-PKA

Theorem (Safety)

R will never decide on an incorrect value.

Optimal Resilience of RMT-PKA

Theorem (Safety)

R will never decide on an incorrect value.

Theorem (Sufficiency of RMT-cut condition)

RMT-PKA achieves RMT whenever an RMT-cut does not exist.

Optimal Resilience of RMT-PKA

Theorem (Safety)

R will never decide on an incorrect value.

Theorem (Sufficiency of RMT-cut condition)

RMT-PKA achieves RMT whenever an RMT-cut does not exist.

Non-existence of an RMT-cut is a necessary and sufficient condition for achieving RMT

Open Questions

– Efficiency study for RMT in the partial knowledge model. (Efficient algorithm known only for the t-local model under local knowledge.)

Open Questions

- Efficiency study for RMT in the partial knowledge model. (Efficient algorithm known only for the t-local model under local knowledge.)

- Resilience measures and approximation. (Existence of an RMT cut is NP-hard to check.)

Open Questions

- Efficiency study for RMT in the partial knowledge model. (Efficient algorithm known only for the t-local model under local knowledge.)
- Resilience measures and approximation. (Existence of an RMT cut is NP-hard to check.)
- Privacy requirements in partial knowledge models (SMT).

Thank you!