

Information-Theoretic Topology-Hiding Broadcast: Wheels, Stars, Friendship, and Beyond

D'or Banoun



Elette Boyle



Ran Cohen



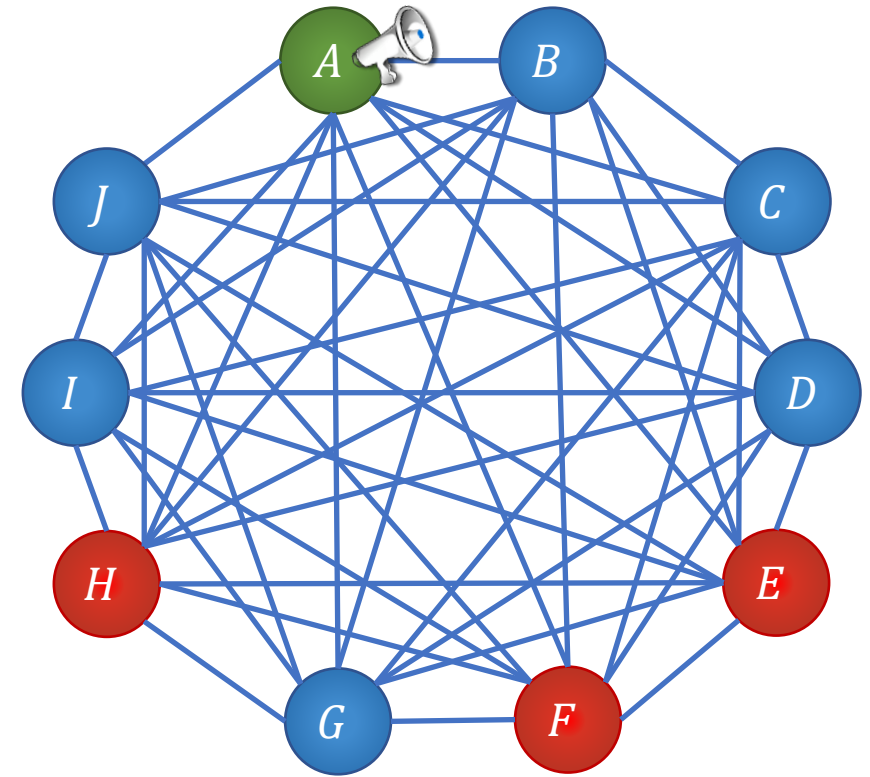
Broadcast

n parties t corrupted

Sender with an input message

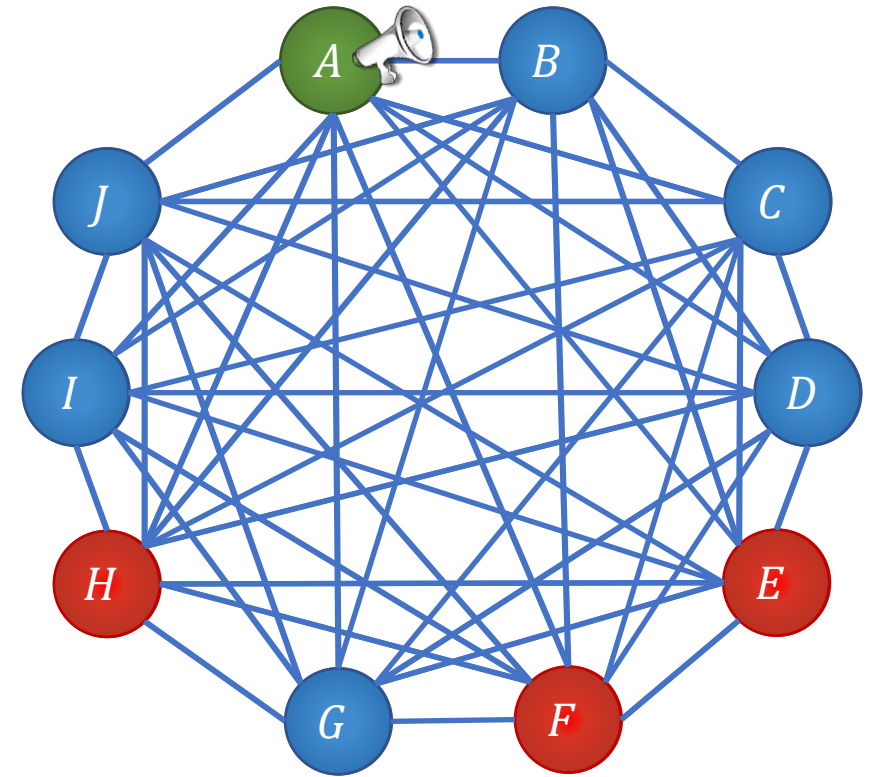
Agreement: all honest parties output the same value

Validity: if sender is honest, the common output is its message



Broadcast on incomplete graph

Each party talks to its neighbors in the communication graph

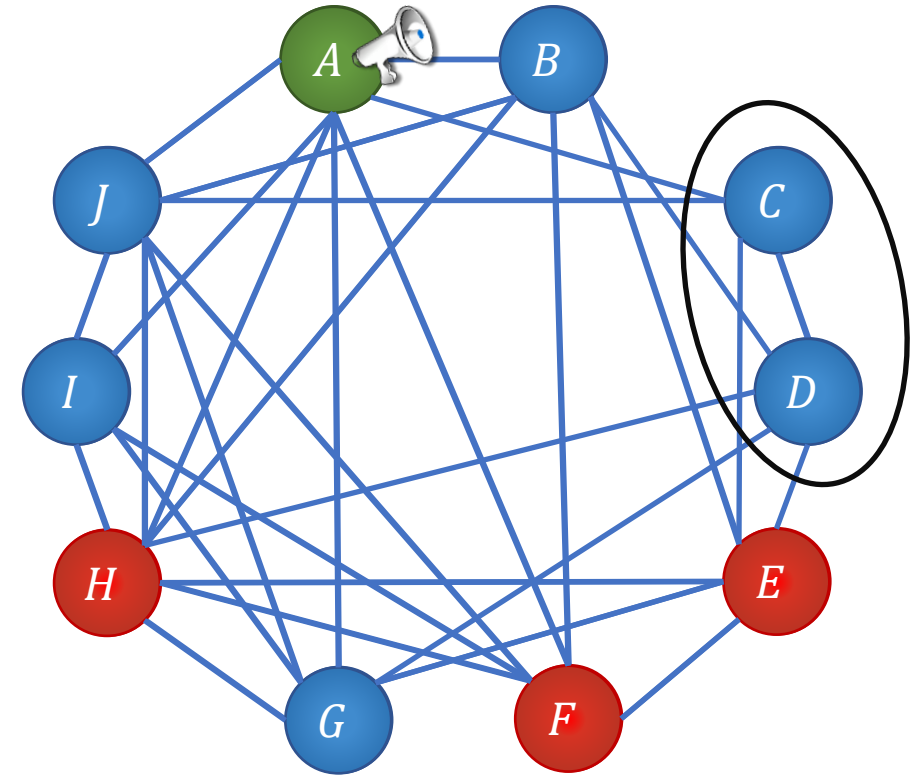


Broadcast on incomplete graph

Each party talks to its neighbors in the communication graph

Potentially disconnected graphs

- Agreement in each component
- Validity in sender's component

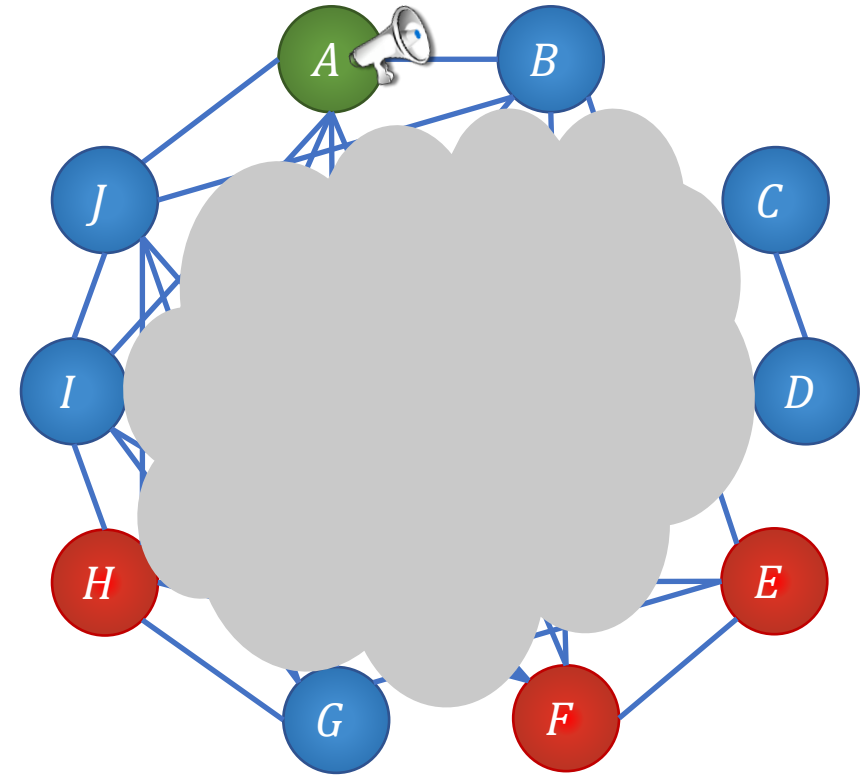


Topology-Hiding Broadcast [Moran, Orlov, Richelson '15]

The **communication graph** itself
can be **sensitive** information

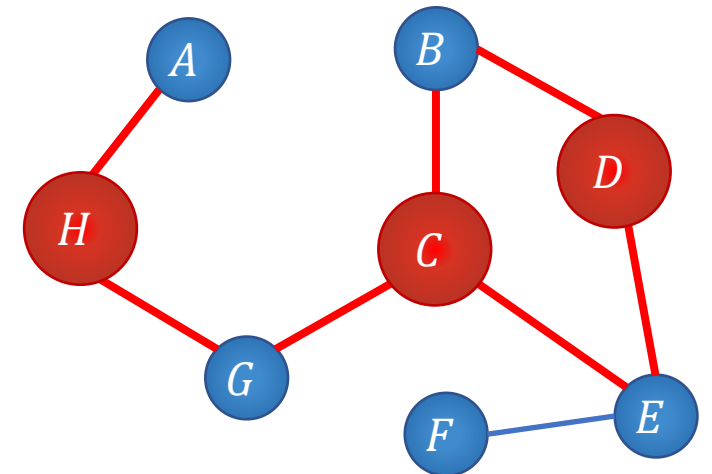
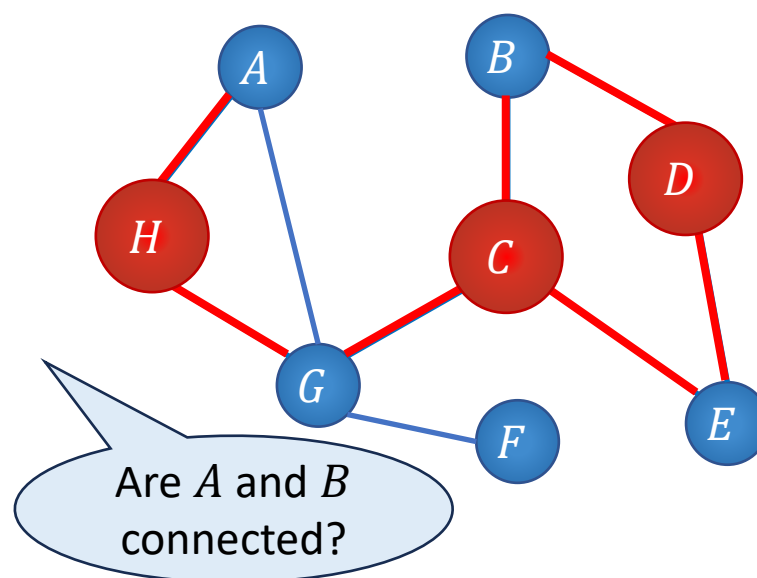
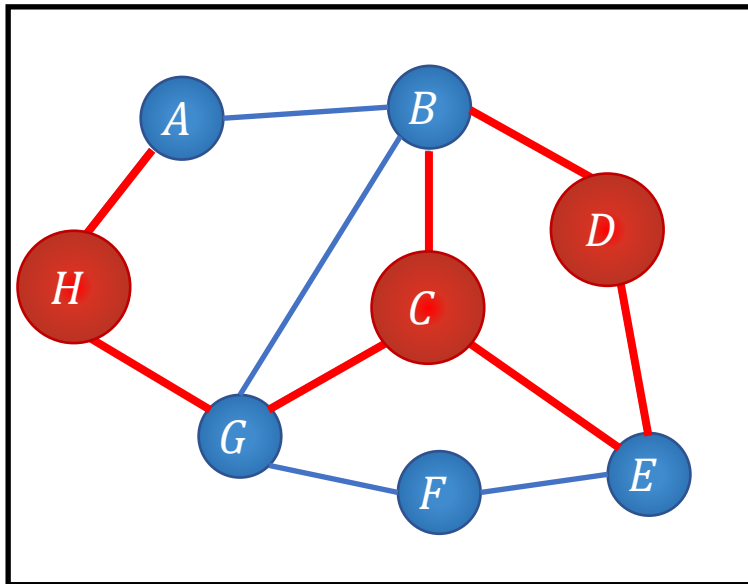
Can we run a broadcast protocol while
hiding the network topology?

What does it even mean?



Topology-Hiding Broadcast [Moran, Orlov, Richelson '15]

- Class of potential communication graphs
- Protocol is executed on one of the graphs
- Every node knows only its immediate neighbors
- Adv doesn't learn honest-to-honest communication patterns

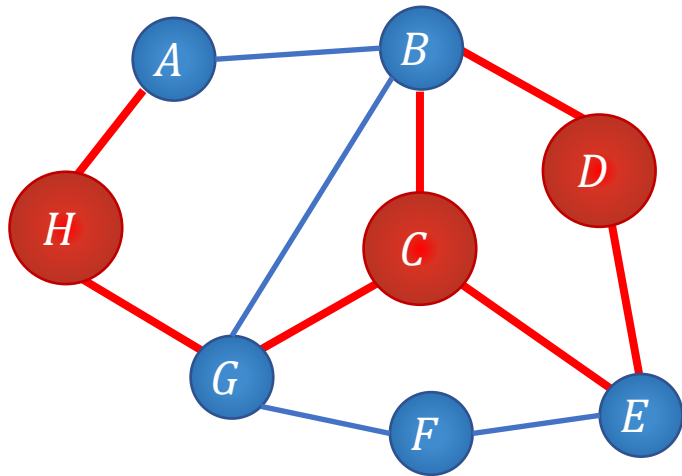


Topology-Hiding Broadcast [Moran, Orlov, Richelson '15]

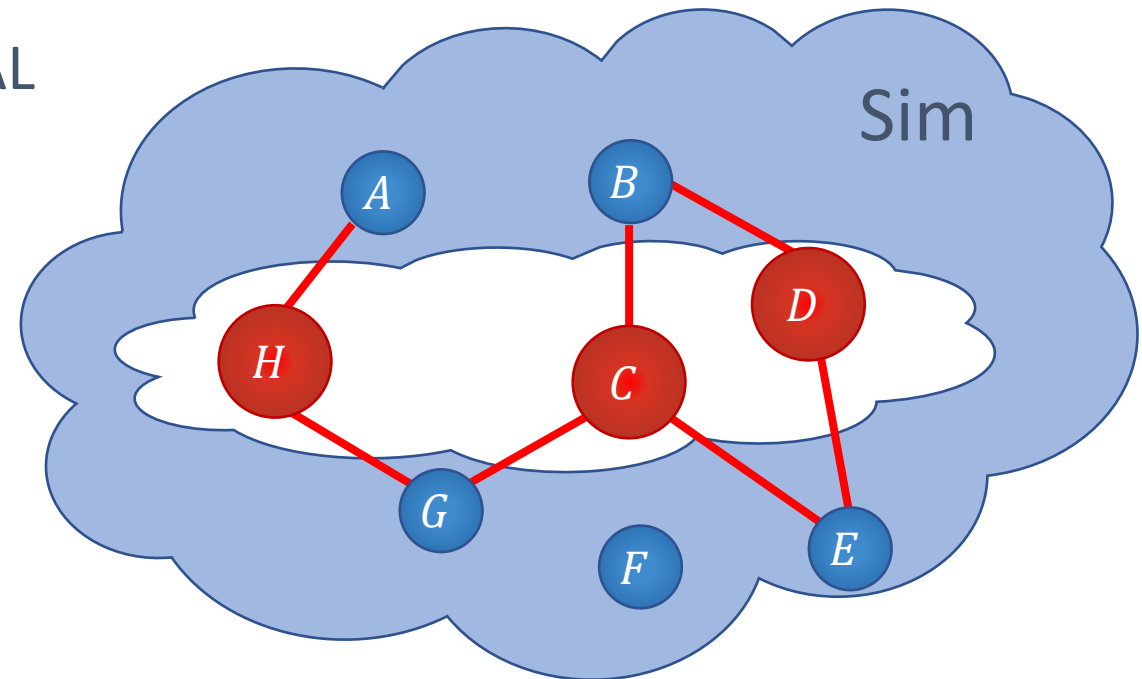
Everything Adv learns can be simulated from:

- Corrupted party's neighbor-set
- Class of potential graphs

REAL

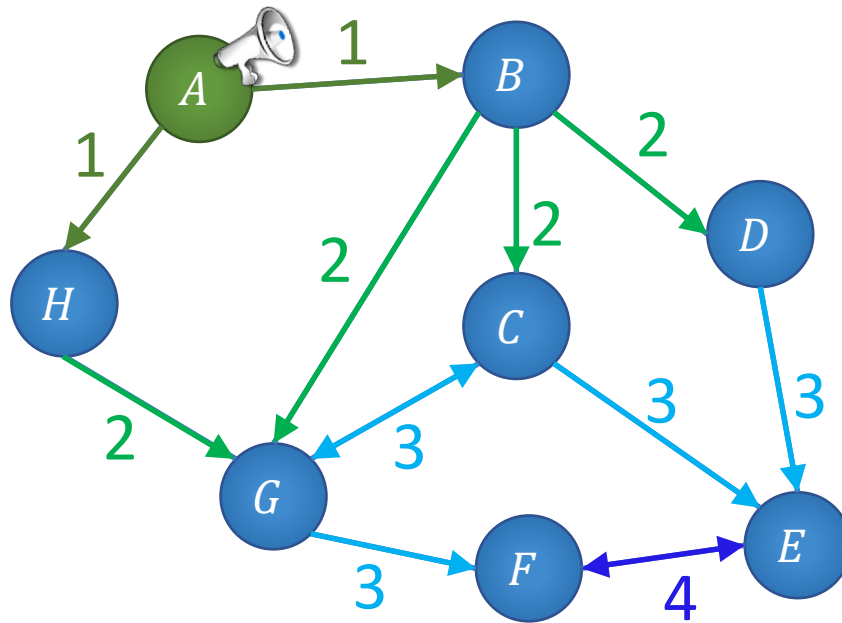


IDEAL



Topology-Hiding Broadcast isn't easy (even for semi-honest corruptions)

We focus on **semi-honest** corruptions, in a **synchronous** model



Each party learns:

- Its **distance** from the sender
- Its neighbors' **distances**

Can we achieve THB?

Yes!

- THB for $t < n$ under standard cryptography assumptions
 - DDH, LWE, or QR [MOR'15,HMTZ'16,AM'17,ALM'17,LLMMMT'18]
 - Constant-round constant-rate OT [BBKM'23]

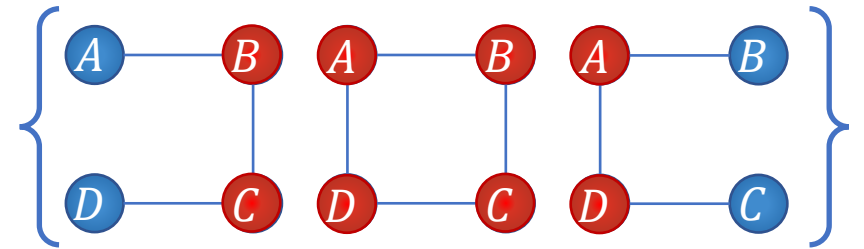
But, do we need cryptography?



THB requires cryptography

Sometimes, yes

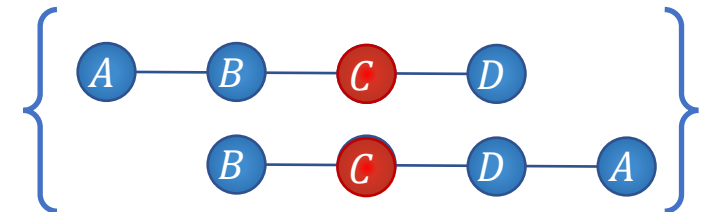
- 2-secure THB on 4-node class \Rightarrow OT [BBMM'18]



Can we trade cryptography with honest majority?

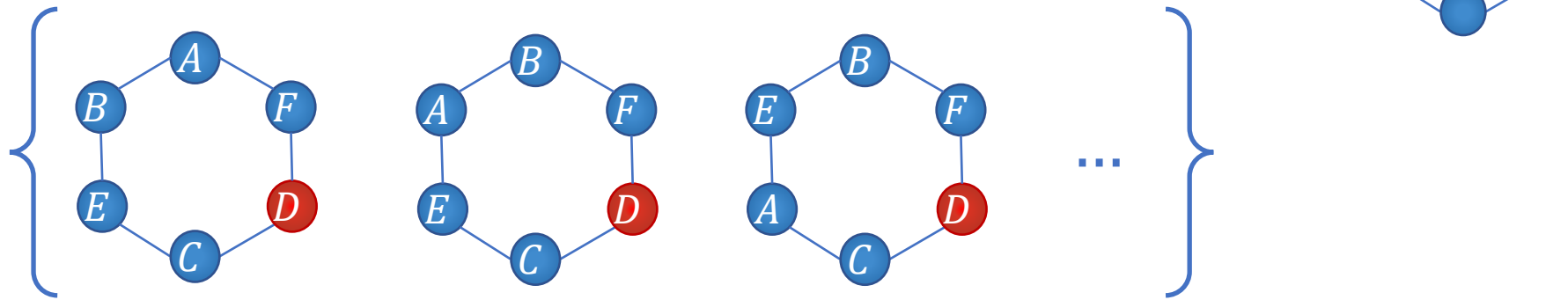
- Extreme case: what if $t = 1$?
- 1-secure THB on 4-node class \Rightarrow KA [BBCMM'19]

Do we **really** need cryptography?



Information-Theoretic THB

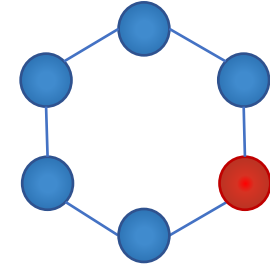
- IT-THB over n -node cycle with $t = 1$ [BBCMM'19]



Notation: Labelless graphs contain all the permutations on the labels

Information-Theoretic THB

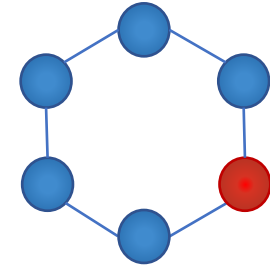
- IT-THB over n -node cycle with $t = 1$ [BBCMM'19]
- Note: cycles are 2-connected



Removing 2 nodes can disconnect
Removing 1 node cannot

Information-Theoretic THB

- IT-THB over n -node cycle with $t = 1$ [BBCMM'19]
- Note: cycles are 2-connected

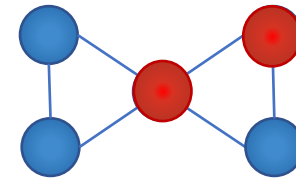


Conjecture: $t + 1$ connectivity $\Leftrightarrow t$ -security

- Conjecture holds for **TH-MPC** with $t = 1$ [BBCKMMM'20]
 - *2-connectivity* \Rightarrow generic IT-TH-MPC (with statistical error)
 - *1-connectivity* \Rightarrow no generic IT-TH-MPC (KA necessary)

What about THB?

- Conjecture doesn't hold [BBCKMMM'20]
- IT-THB over 1-connected butterfly with $t = 1$



Agenda

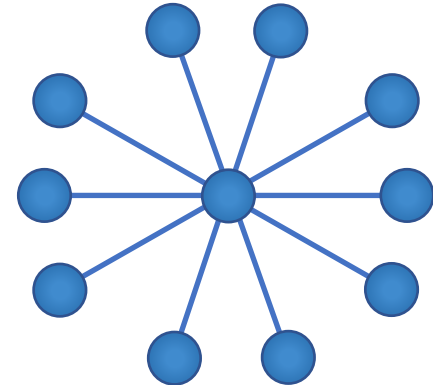
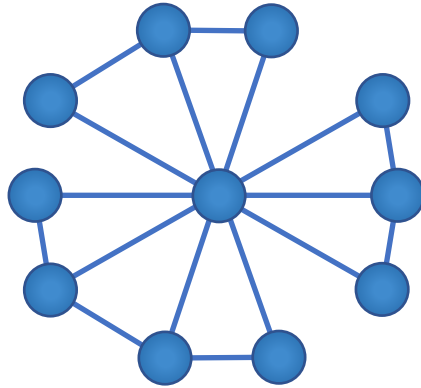
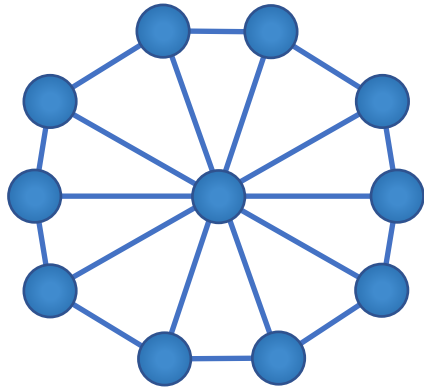
- Our results in a nutshell
- Characterization of wheel subgraphs
- Friendship graphs
- Lower bound



Our work, question #1: feasibility

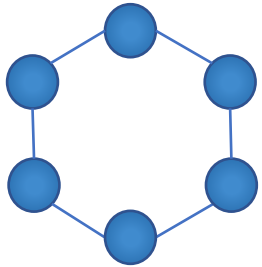
Which properties characterize feasibility of 1-secure IT-THB?

For class of subgraphs of **wheels** (star-embedded)
the answer is the **degree structure**

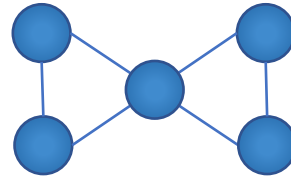


Our work, question #2: perfect security

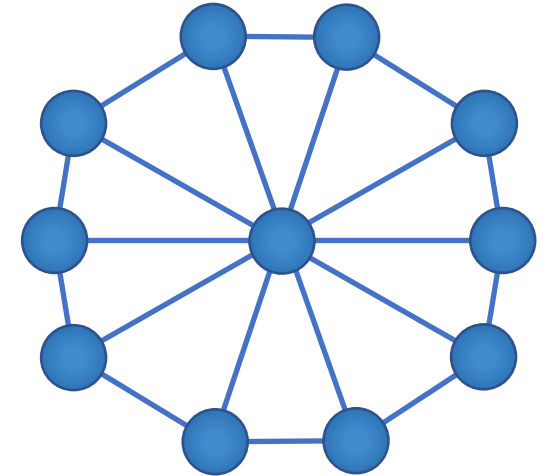
- IT-THB from [BBCKMMM'20] for 2-connected graphs has a positive error
- Perfect 1-secure IT-THB was only known for:



n -nodes cycles



5-nodes butterfly



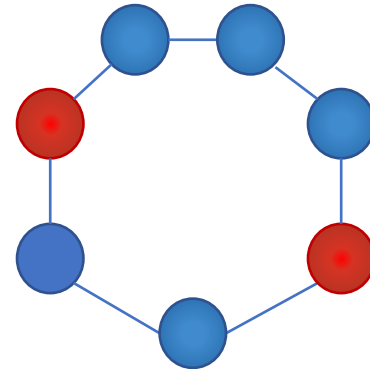
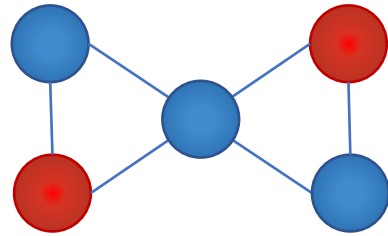
Perfect IT-THB with $n > 5$ beyond cycles?

Yes! For certain **star-embedded** subgraphs of **wheels**

Our work, question #3: $t > 1$ corruptions

Is there non-degenerate IT-THB with $t > 1$?

- 1-secure IT-THB from [BBCKMMM'20] completely breaks for $t = 2$
- The butterfly for $t = 2$ is degenerate (nothing to hide)
- [BBCMM'19] 2-secure THB for cycles \Rightarrow KA

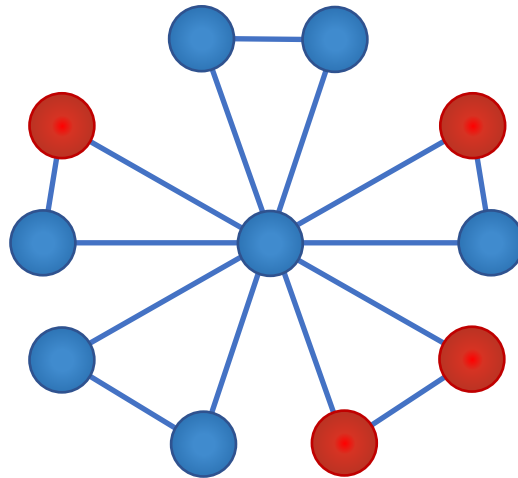


Our work, question #3: $t > 1$ corruptions

Is there non-degenerate IT-THB with $t > 1$?

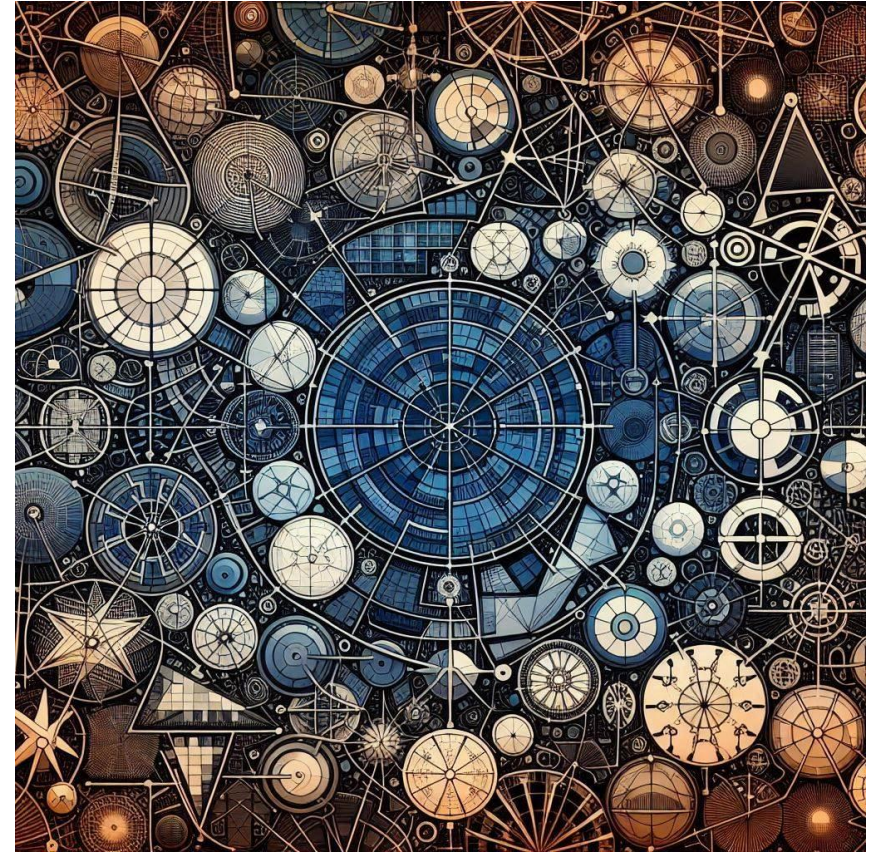
Yes!

Perfect IT-THB for **friendship** graphs with $t < n$



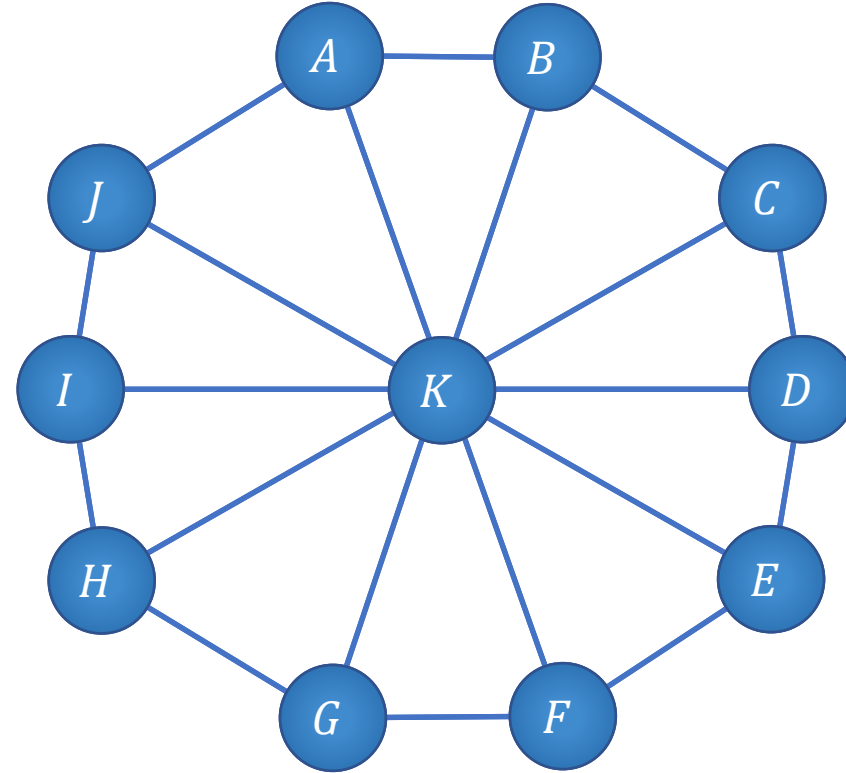
Agenda

- Our results in a nutshell
- Characterization of wheel subgraphs
- Friendship graphs
- Lower bound



Wheel graphs

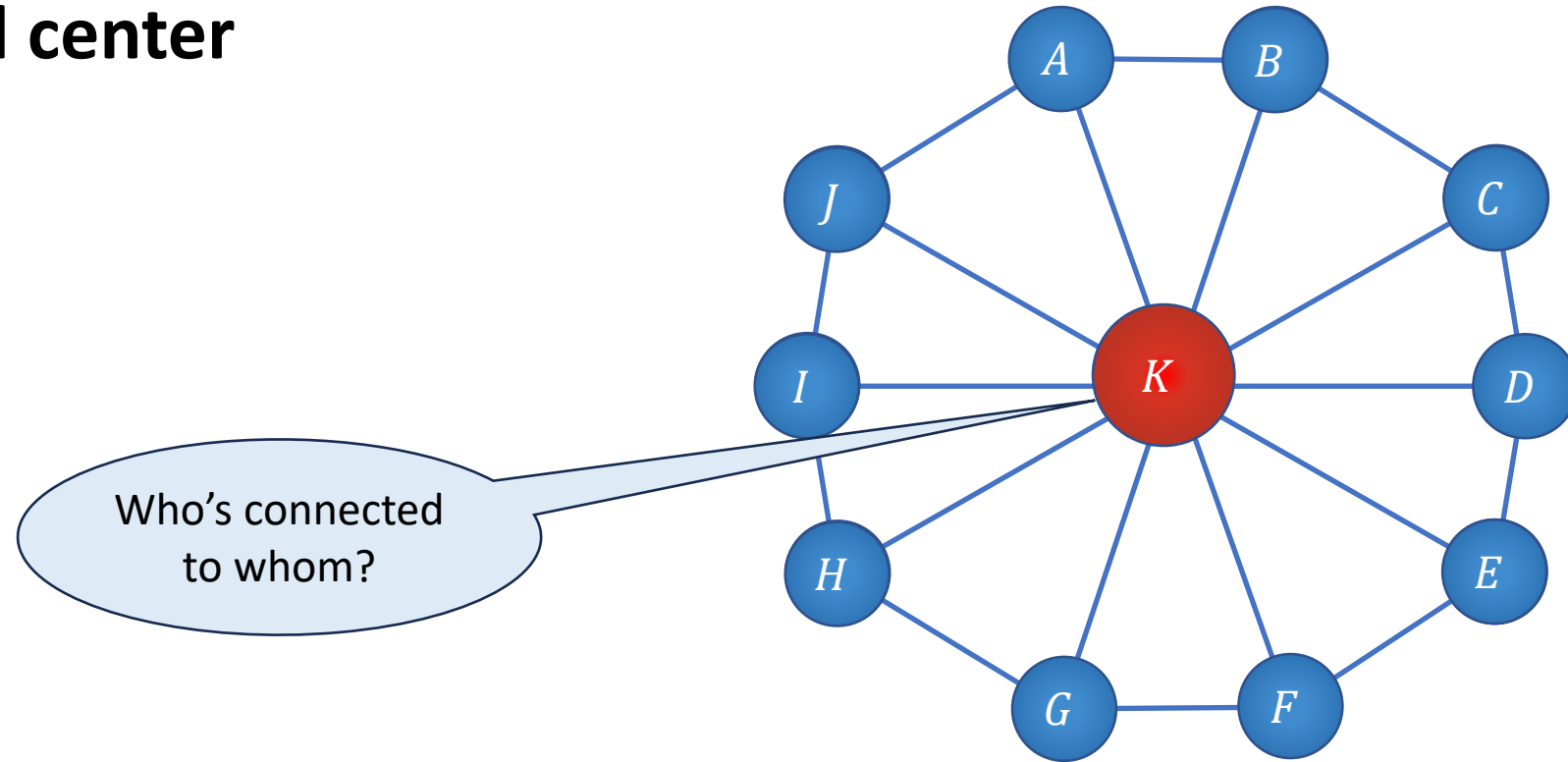
What is there to hide?



Wheel graphs

What is there to hide?

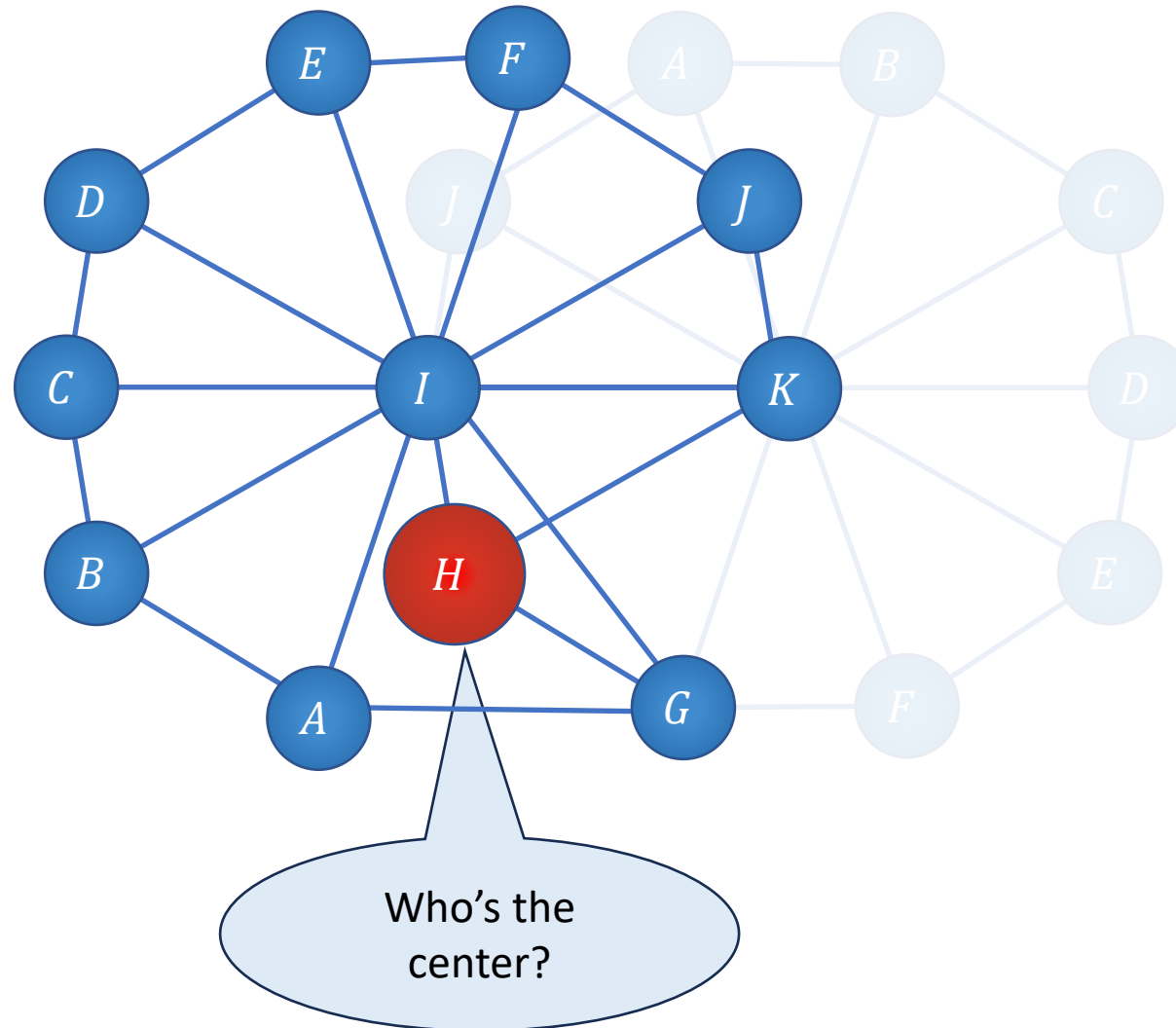
- **Corrupted center**



Wheel graphs

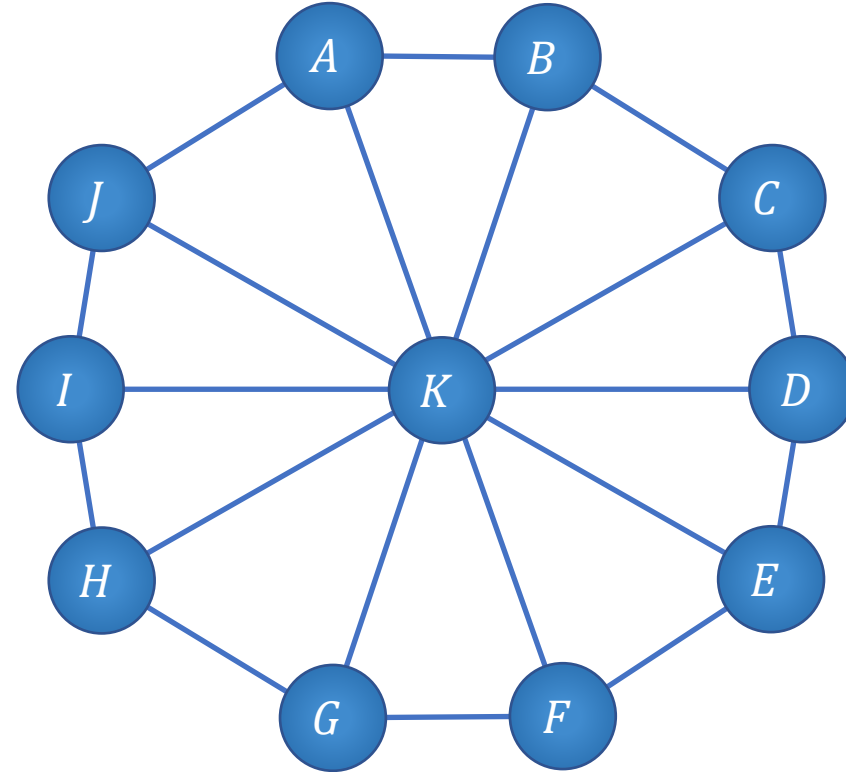
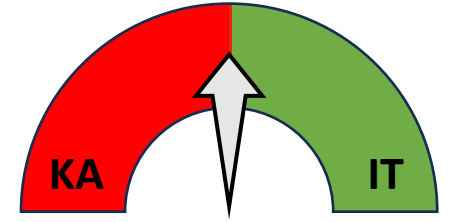
What is there to hide?

- **Corrupted perimeter**



IT-THB for wheel graphs

1-secure perfect IT-THB

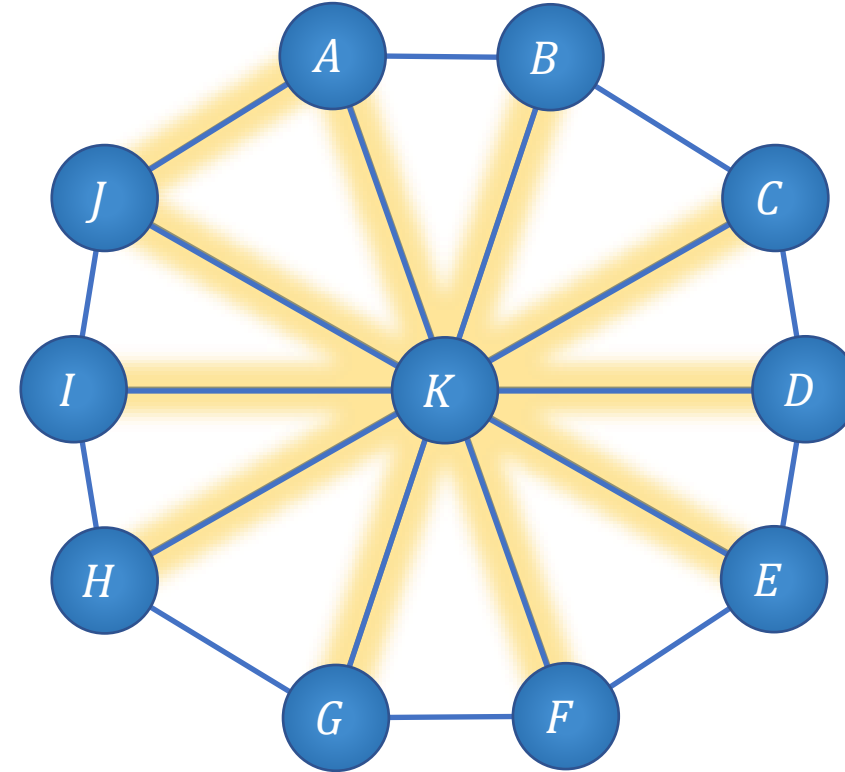
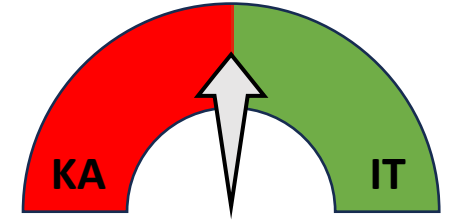


What about sub-graphs of wheels?

Removing edges from a wheel

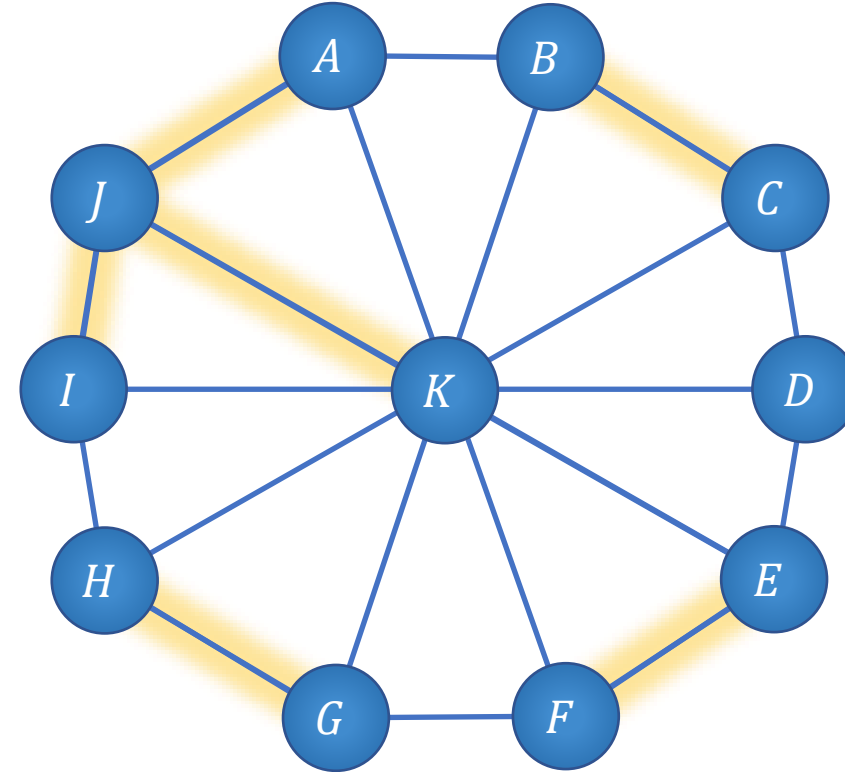
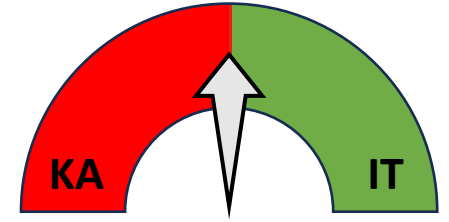
Disconnecting the center:

- Cycle: IT-THB
- Path: require KA



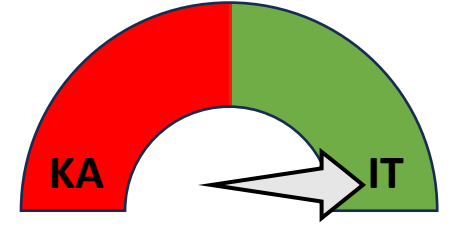
What about sub-graphs of wheels?

Remove edges from the perimeter



What about sub-graphs of wheels?

Remove edges from the perimeter

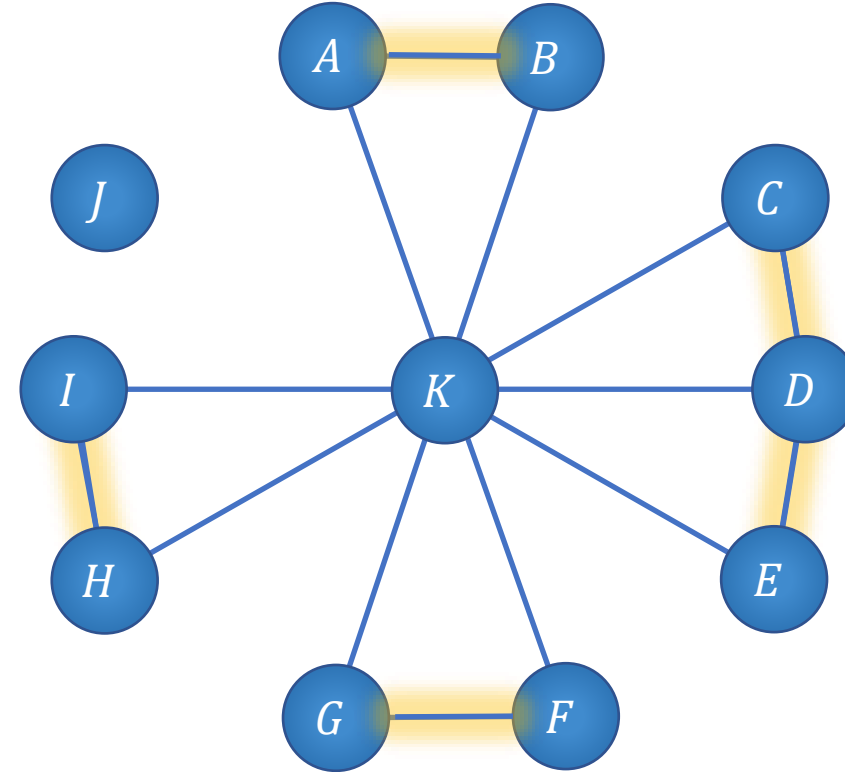


Admissible graph:

a star-embedded graph without tails
(degree of non-center is 0, 2 or 3)

Star:

A center and all tails
(degree of non-center is 0 or 1)

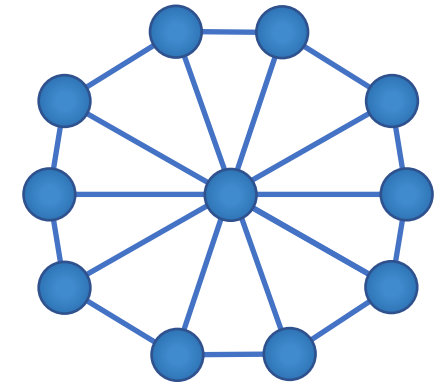
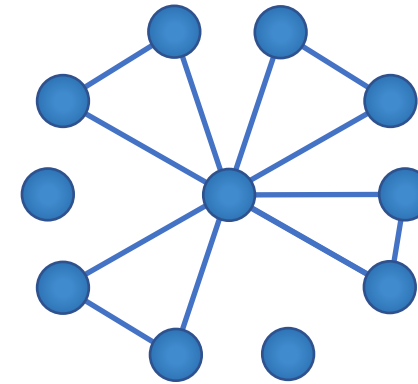
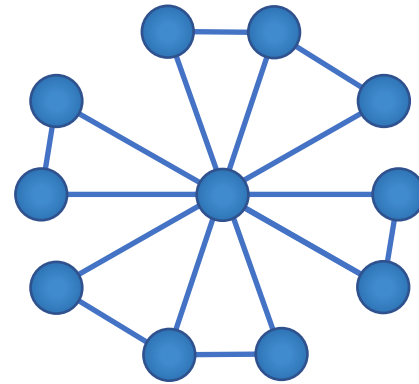


Star-Embedded sub-graphs of wheels

Main connected component

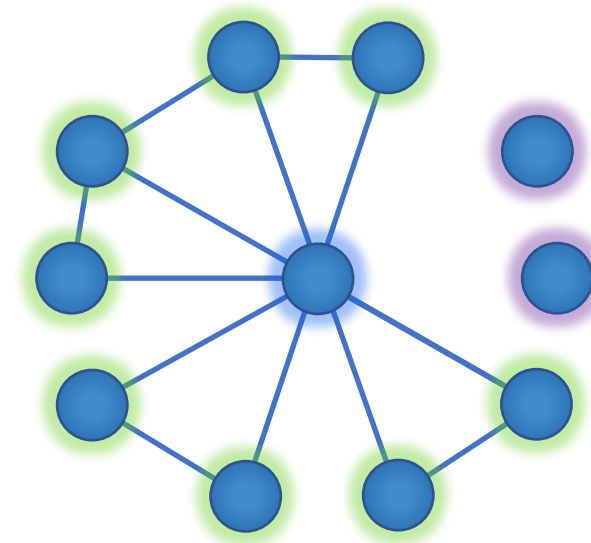
- At least 5 nodes
- Well-defined center

All other nodes are isolated



Three types of nodes:

- Center
- Perimeter
- Isolated nodes

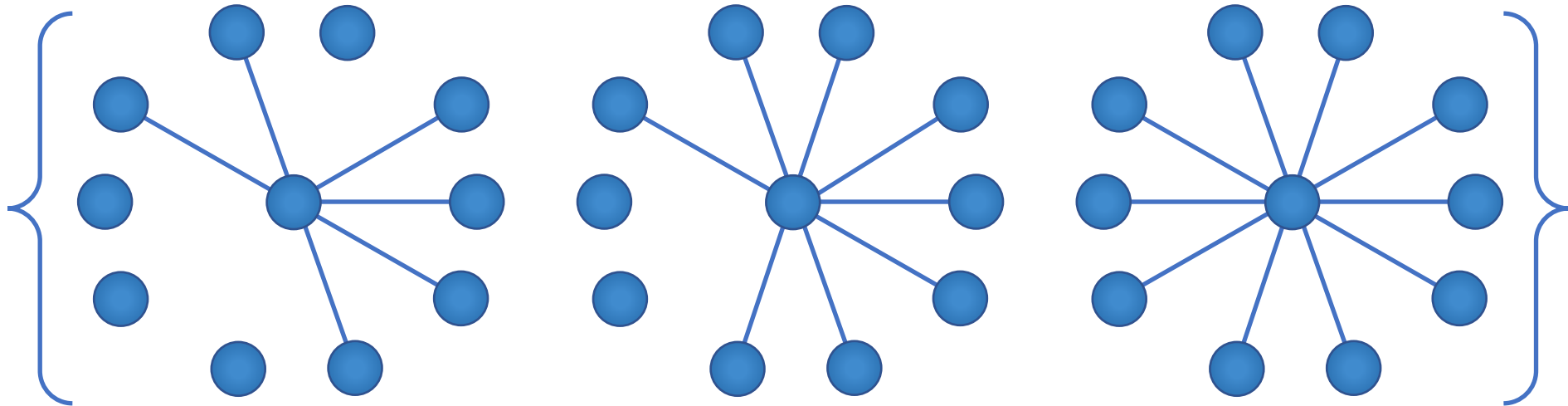


Our theorem

Consider a star-embedded graph-class \mathcal{G} with n nodes

There exists a perfectly 1-secure IT-THB over \mathcal{G} if:

- The maximal degree of perimeter-node is 1 (stars), OR

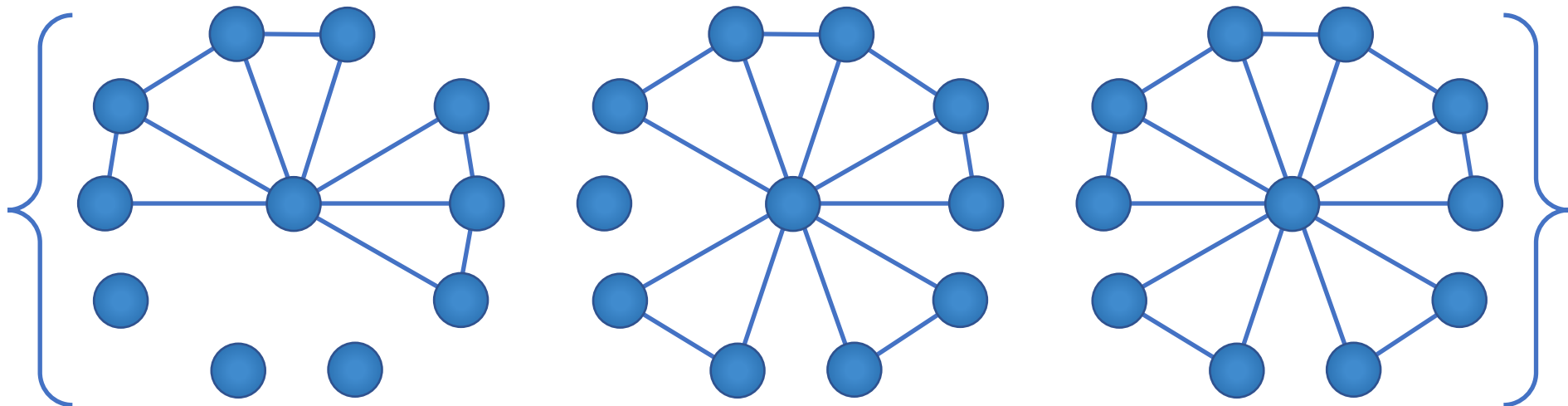


Our theorem

Consider a star-embedded graph-class \mathcal{G} with n nodes

There exists a perfectly 1-secure IT-THB over \mathcal{G} if:

- The **maximal** degree of perimeter-node is **1** (stars), OR
- The **minimal** degree of perimeter-node is **2** or **3** (admissible), OR

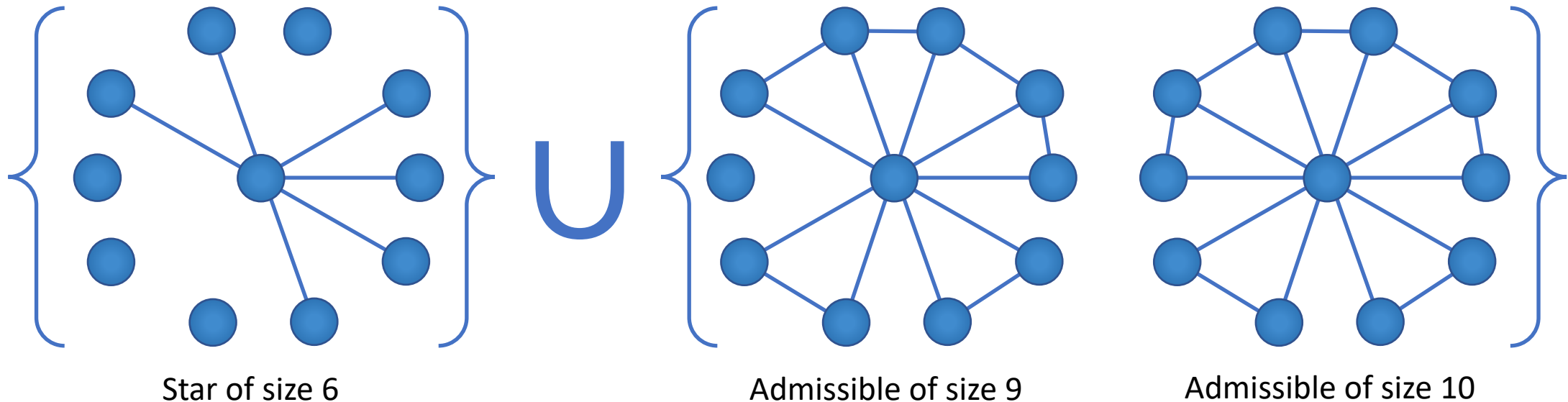


Our theorem

Consider a star-embedded graph-class \mathcal{G} with n nodes

There exists a perfectly 1-secure IT-THB over \mathcal{G} if:

- The **maximal** degree of perimeter-node is **1** (stars), OR
- The **minimal** degree of perimeter-node is **2** or **3** (admissible), OR
- \mathcal{G} consists of **stars** and **admissible** graphs, but of **different** sizes



Our theorem

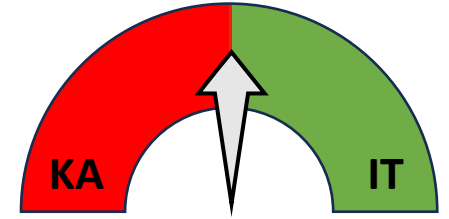
Consider a star-embedded graph-class \mathcal{G} with n nodes

There exists a perfectly 1-secure IT-THB over \mathcal{G} if:

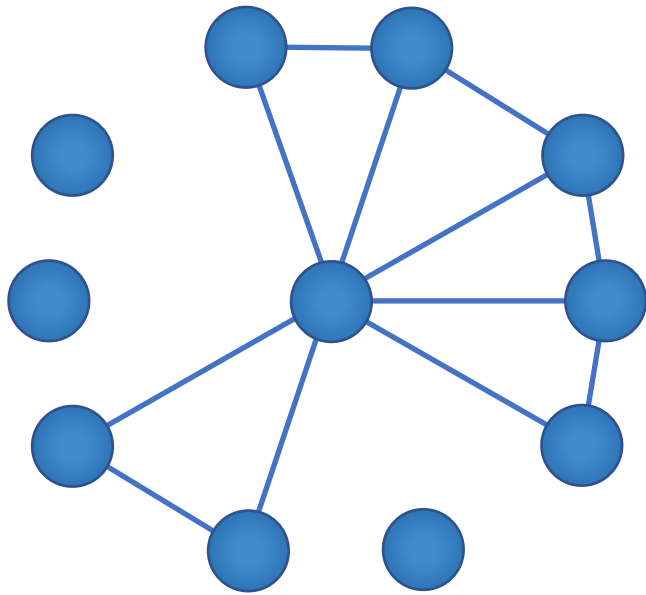
- The **maximal** degree of perimeter-node is **1** (stars), OR
- The **minimal** degree of perimeter-node is **2** or **3** (admissible), OR
- \mathcal{G} consists of **stars** and **admissible** graphs, but of **different** sizes

Otherwise, 1-secure THB over $\mathcal{G} \Leftrightarrow$ KA exists

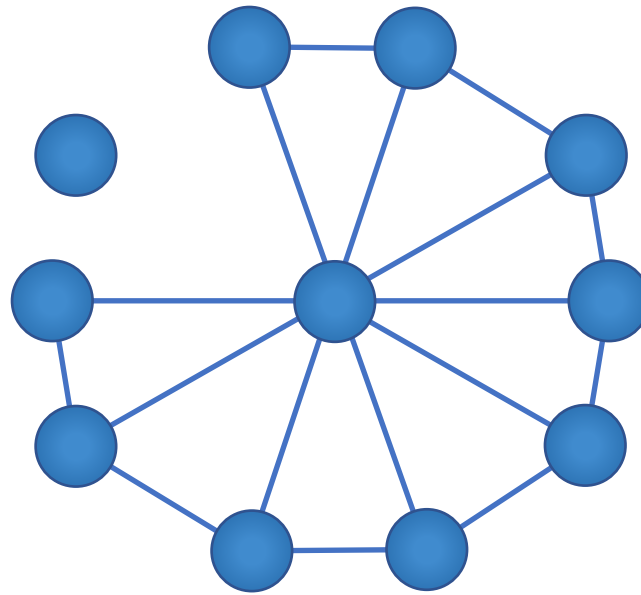
Pop quiz!



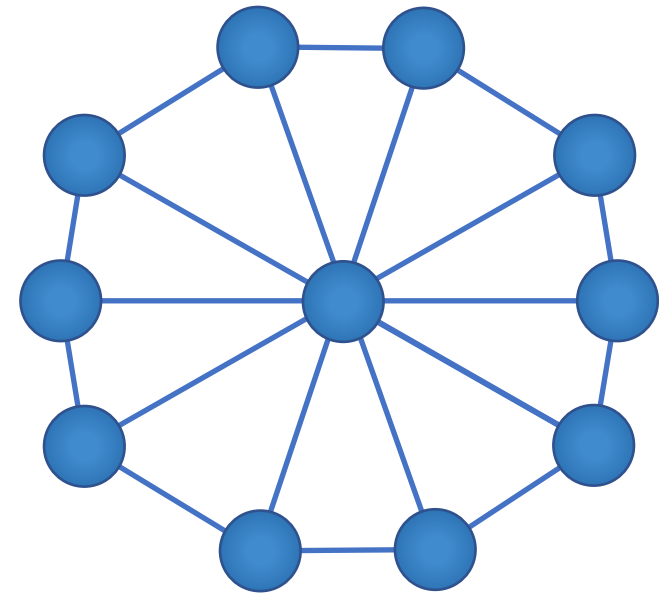
\mathcal{G} consists of **admissible graphs of different sizes**



Admissible of size 7

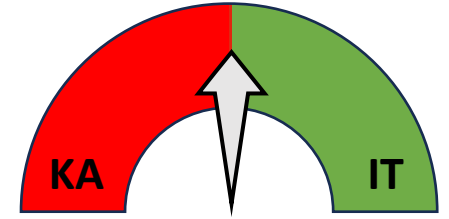


Admissible of size 9

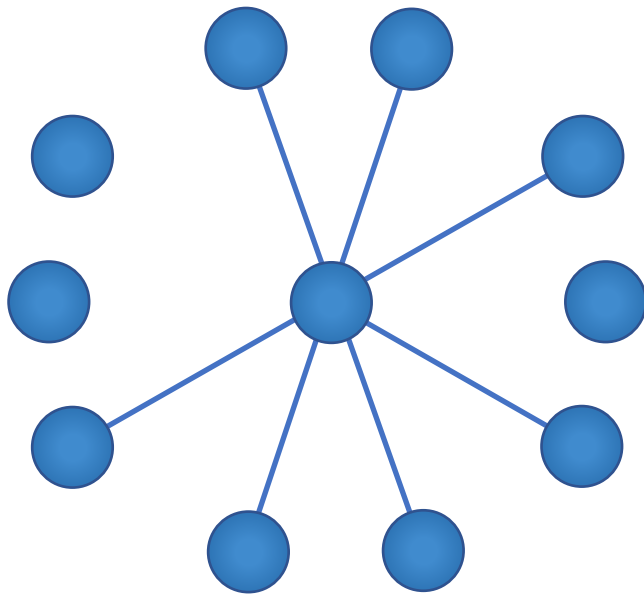


Admissible of size 10

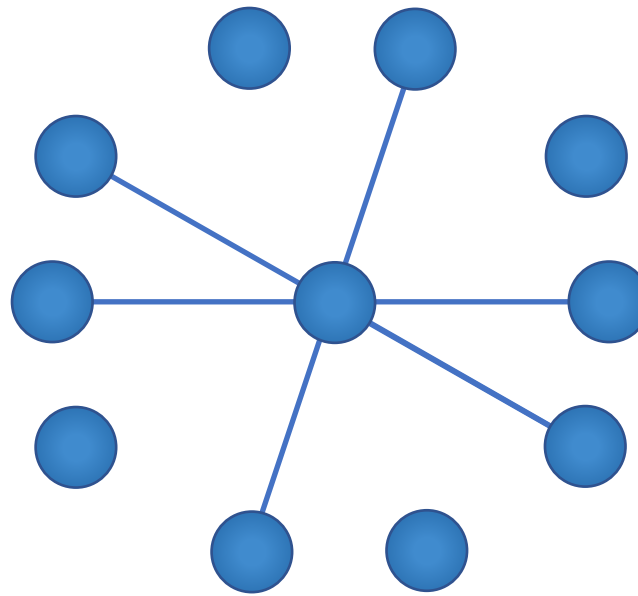
Pop quiz!



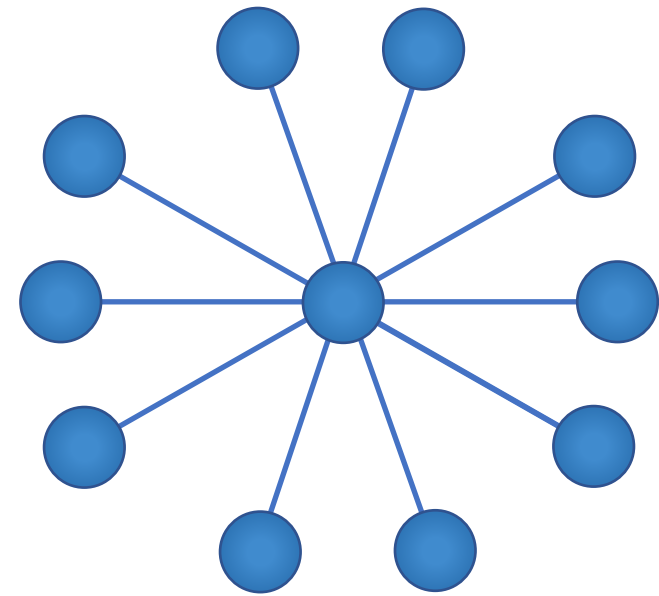
\mathcal{G} consists of **stars of different sizes**



Star of size 6

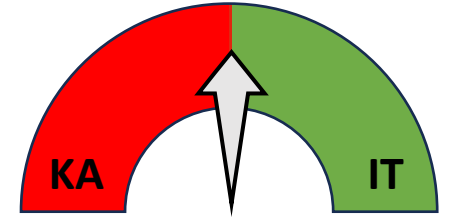


Star of size 6

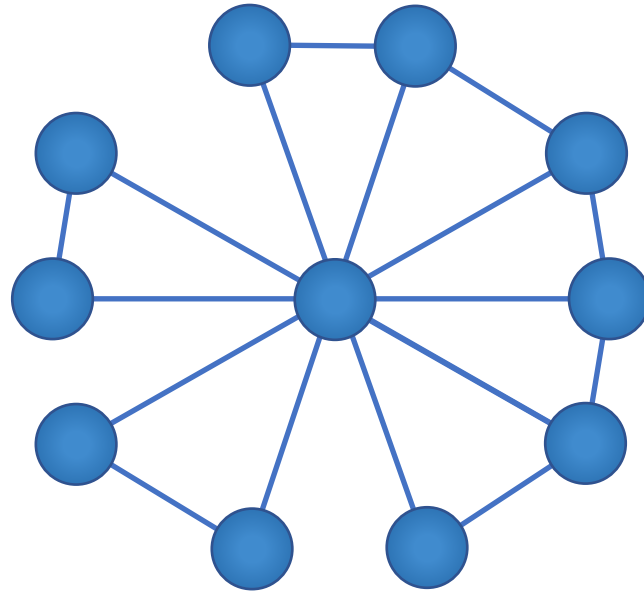


Star of size 10

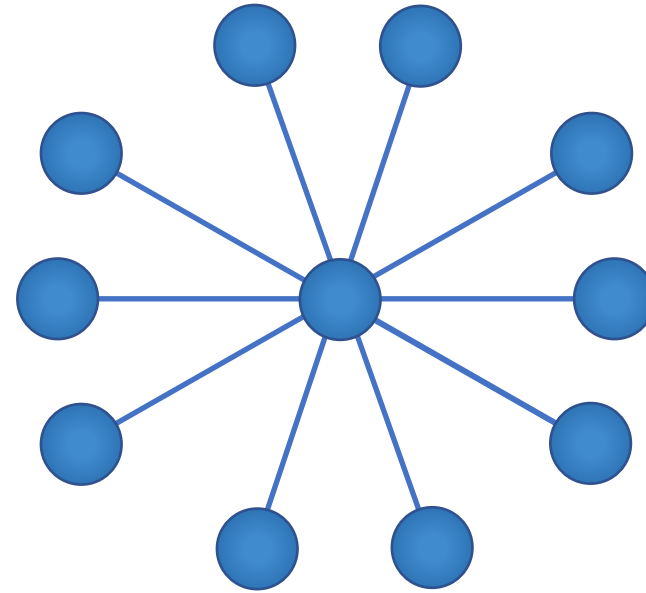
Pop quiz!



\mathcal{G} consists of **admissible** and **star of the same size**

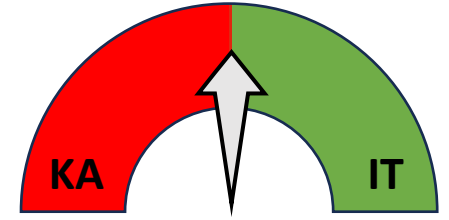


Admissible of size 10

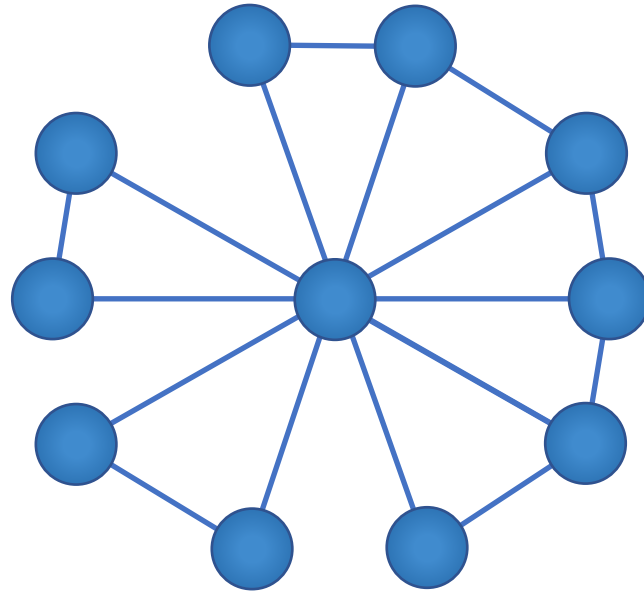


Star of size 10

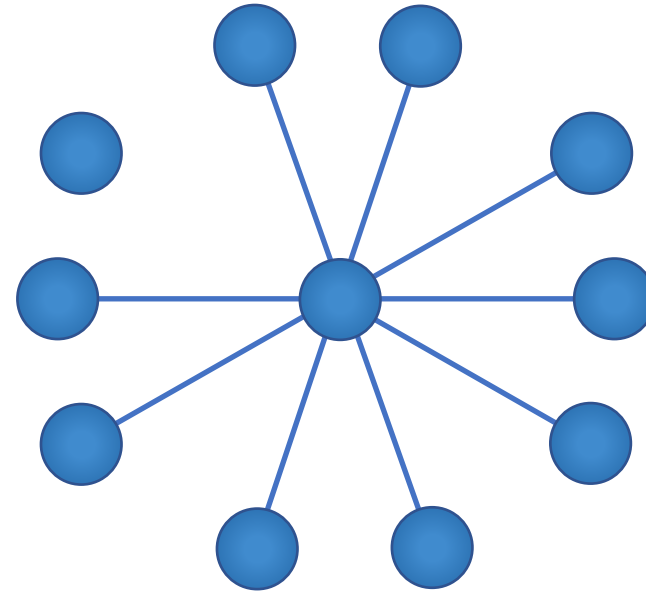
Pop quiz!



\mathcal{G} consists of **admissible** and **star of different sizes**



Admissible of size 10



Star of size 9

Agenda

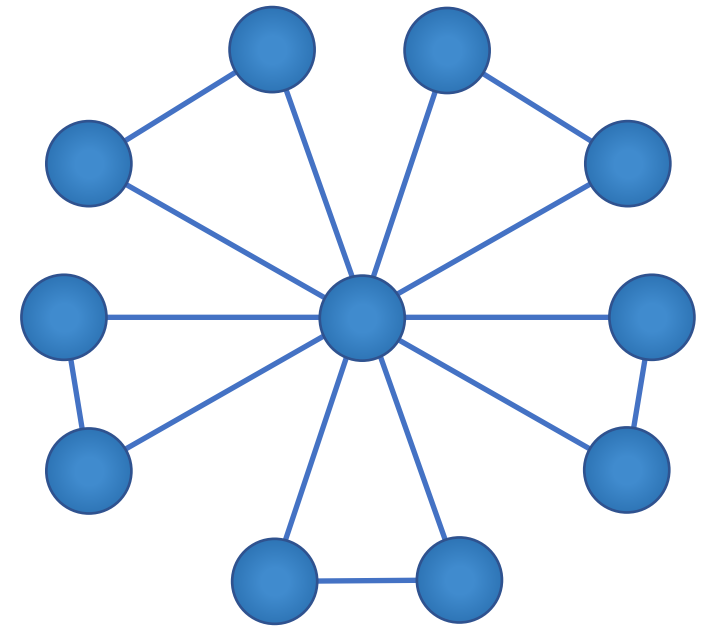
- Our results in a nutshell
- Characterization of wheel subgraphs
- Friendship graphs
- Lower bound



Friendship graphs

The friendship theorem [Erdős, Rényi, Sós '66]

If each pair of parties have one common friend
 $\Rightarrow \exists$ someone who's friend with everyone



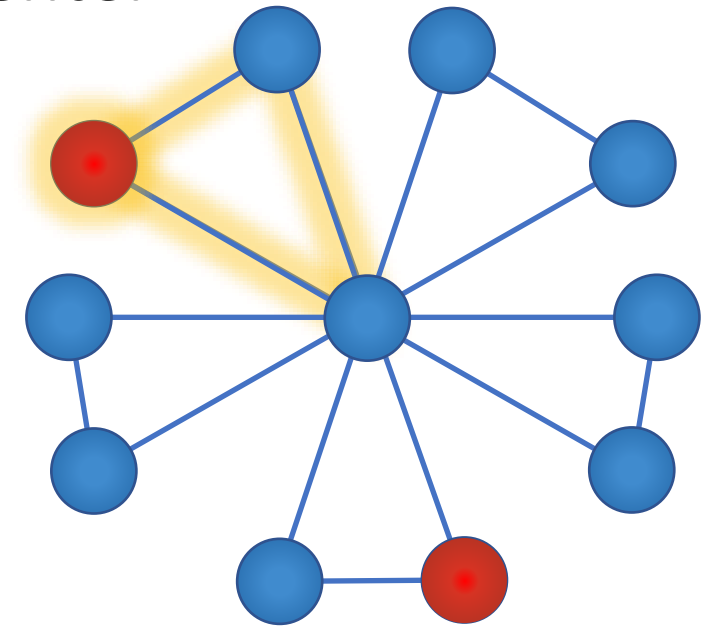
What's so special about friendship graphs?

Can enforce local behavior in each triangle

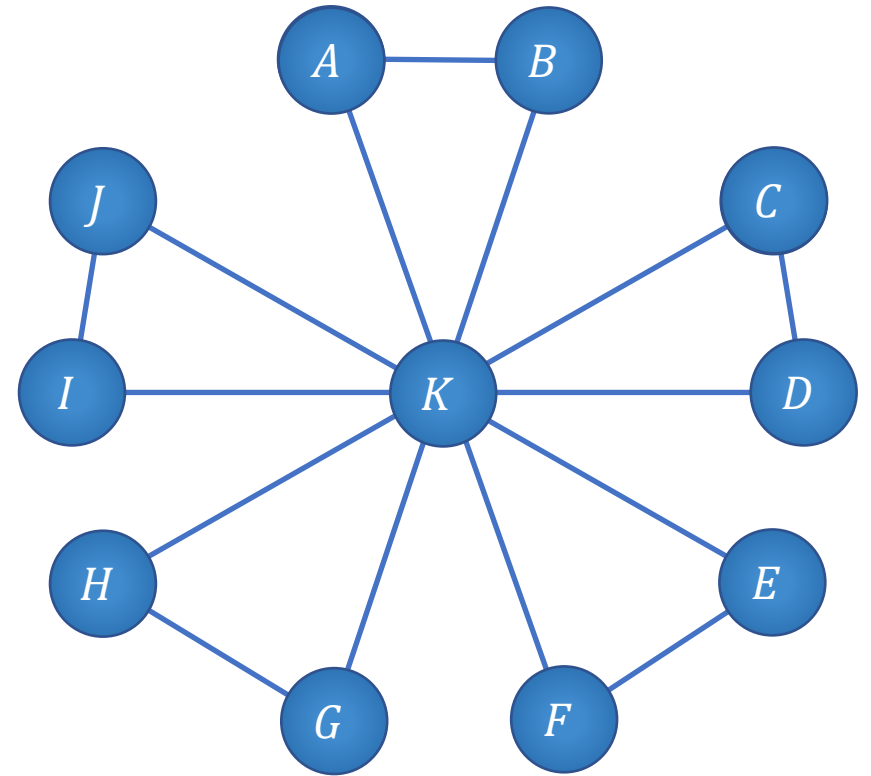
All information about each triangle is through the center

⇒ Can “decompose” the protocol to triangles

⇒ We obtain perfect security for $t < n$

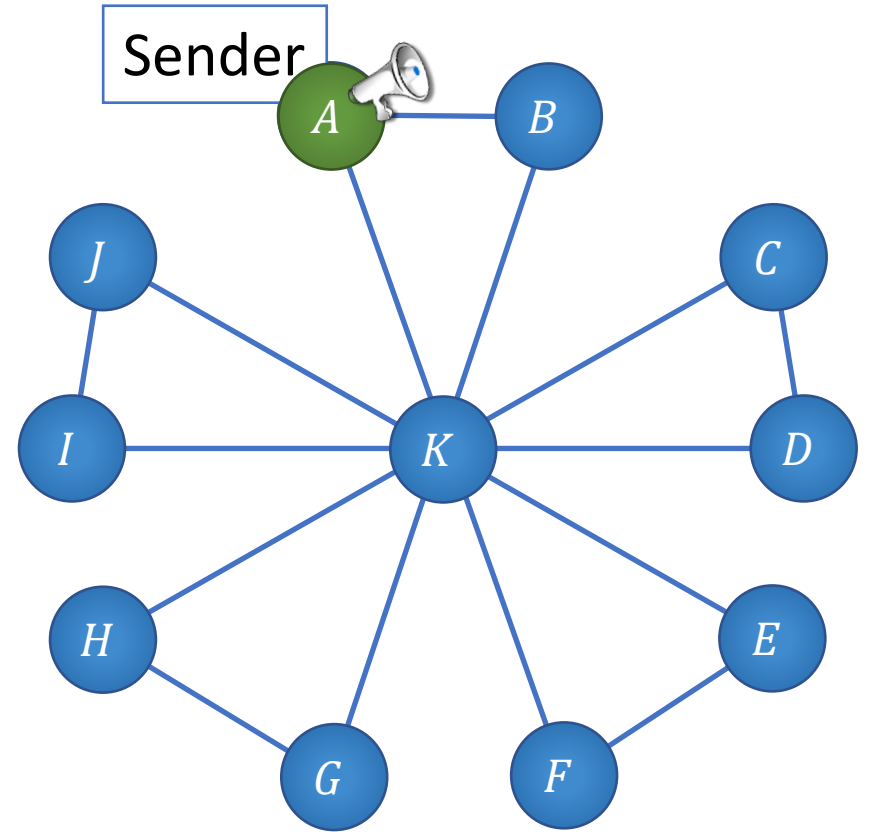


The friendship protocol



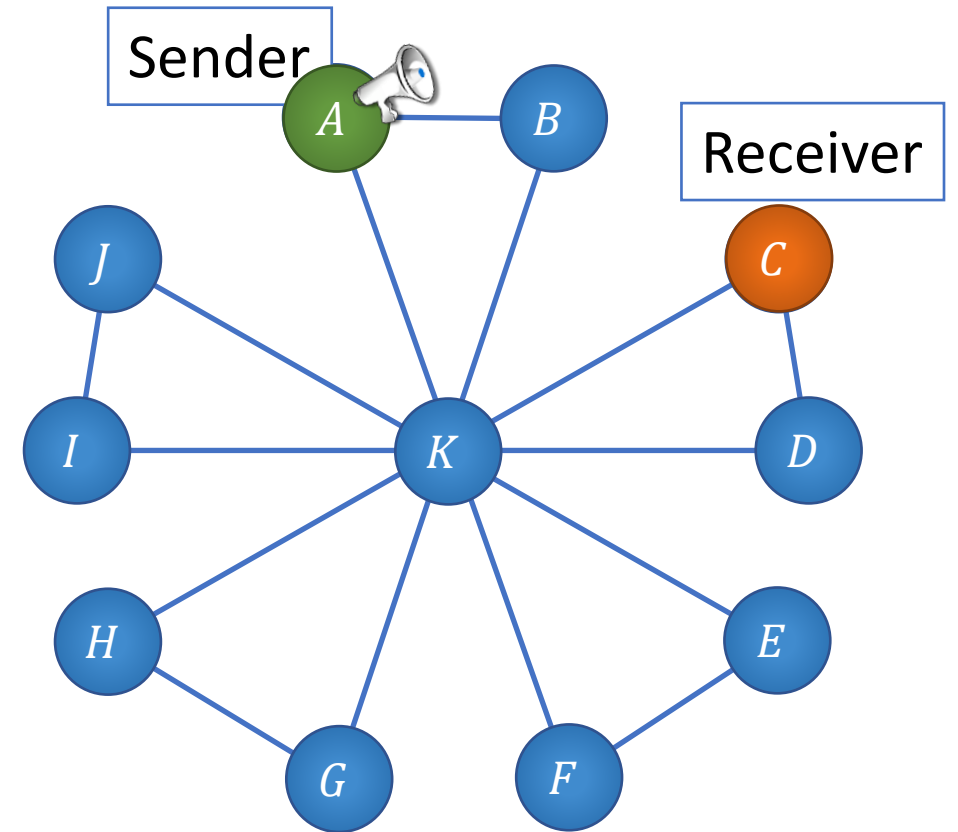
The friendship protocol

- Sender with input m



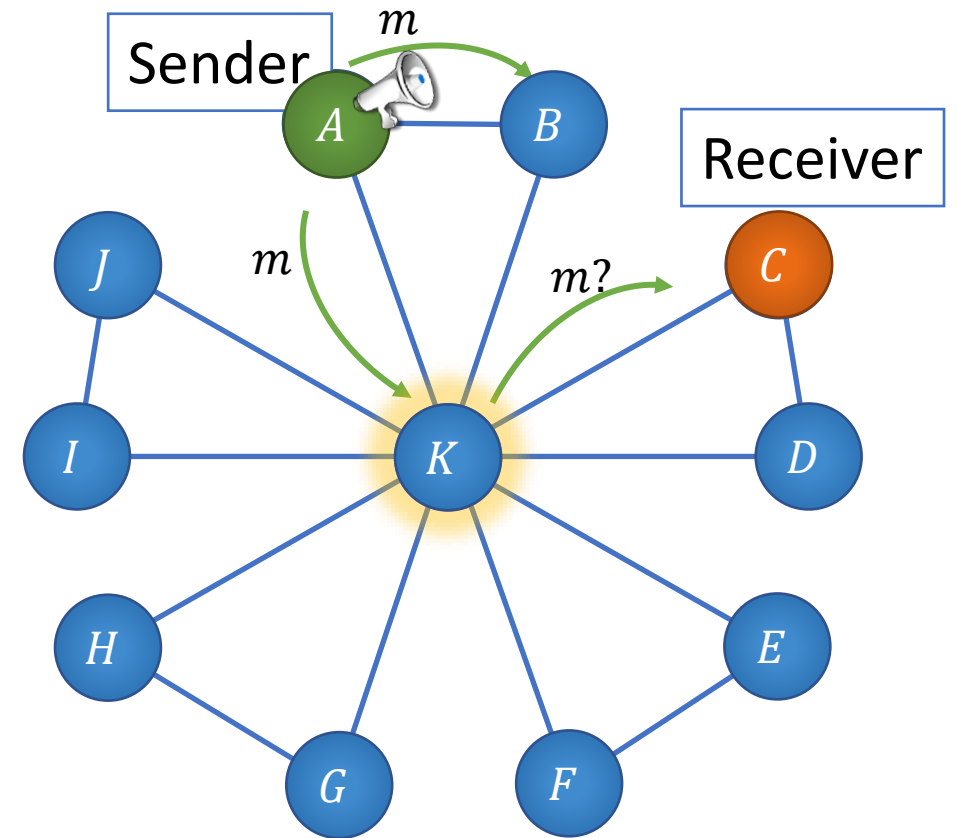
The friendship protocol

- Sender with input m
- Send to one receiver at a time
- Important: sender & receiver are known



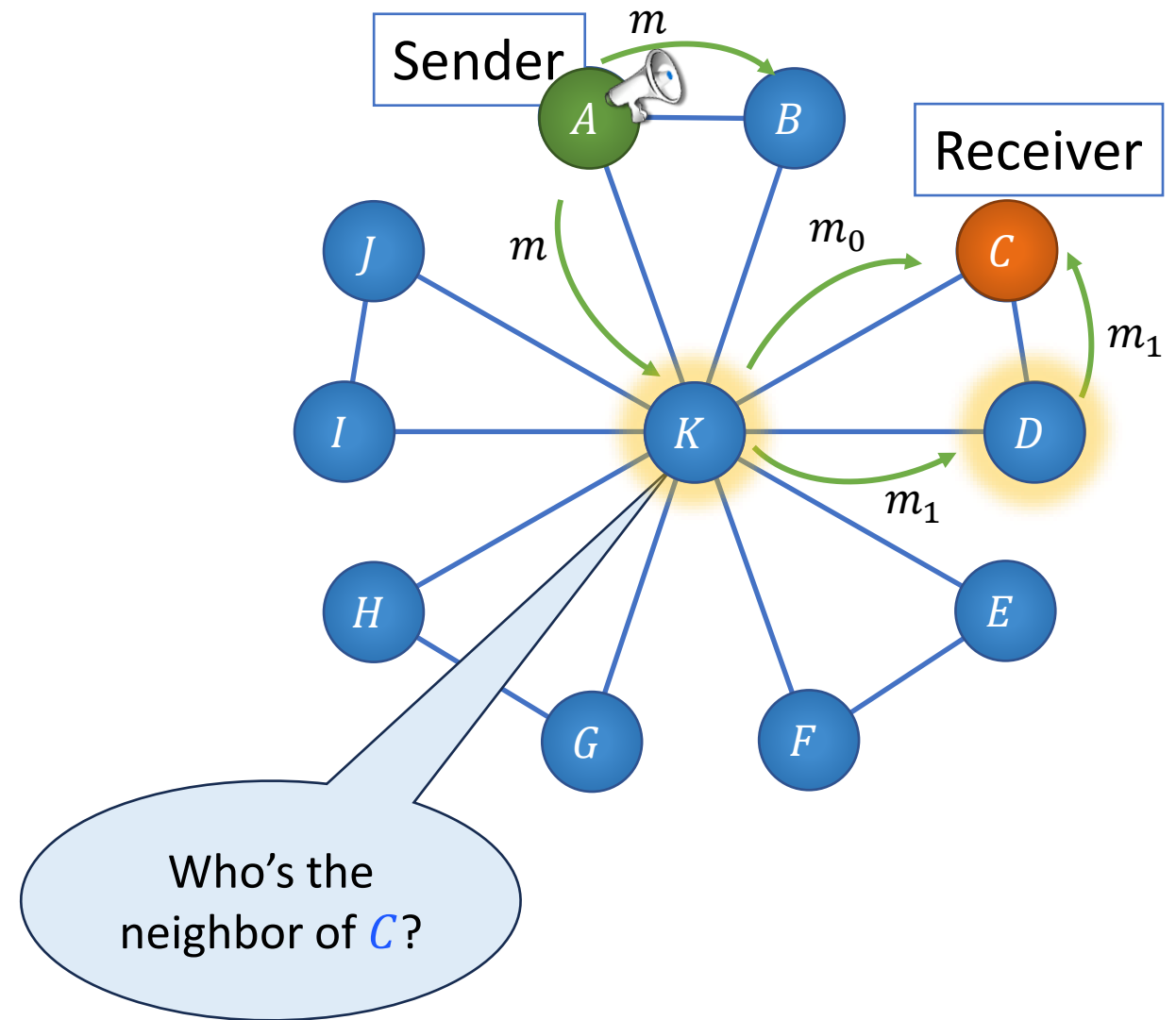
The friendship protocol

- Sender sends m to its neighbors
- Can the center forward m to receiver?
- No! Receiver will learn who's the center



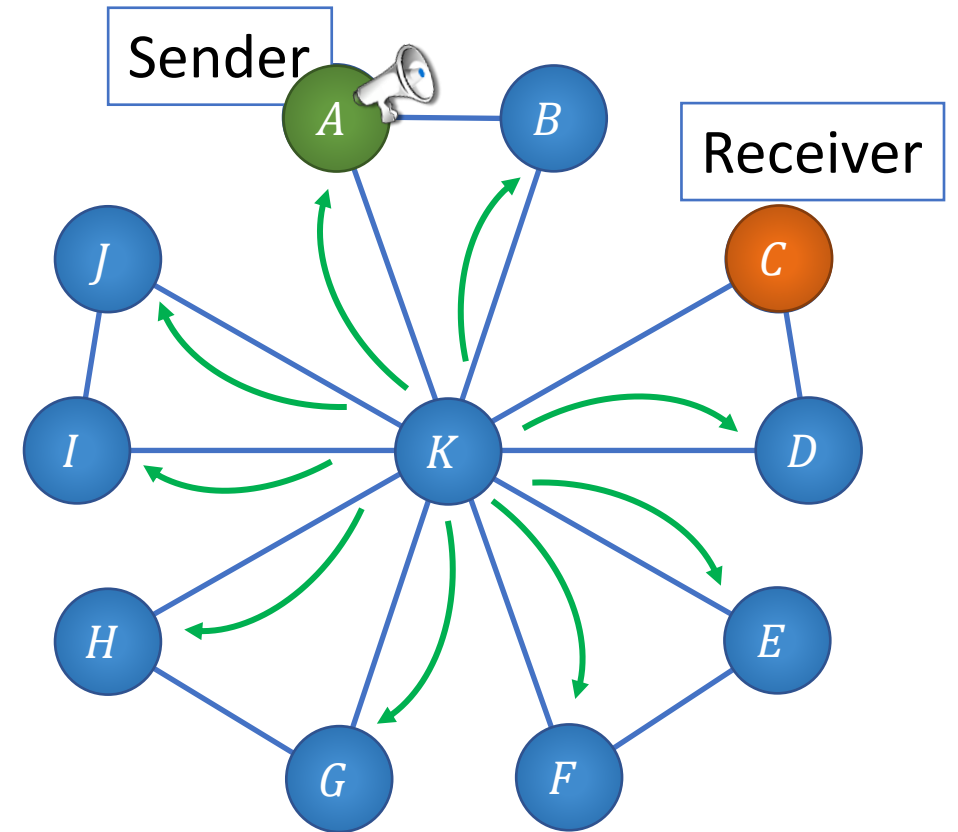
The friendship protocol

- Say the center knows that D is the third node in the triangle
 - Set $m = m_0 \oplus m_1$
 - Send m_1 to D
 - Each send their share to C
- But who is it?



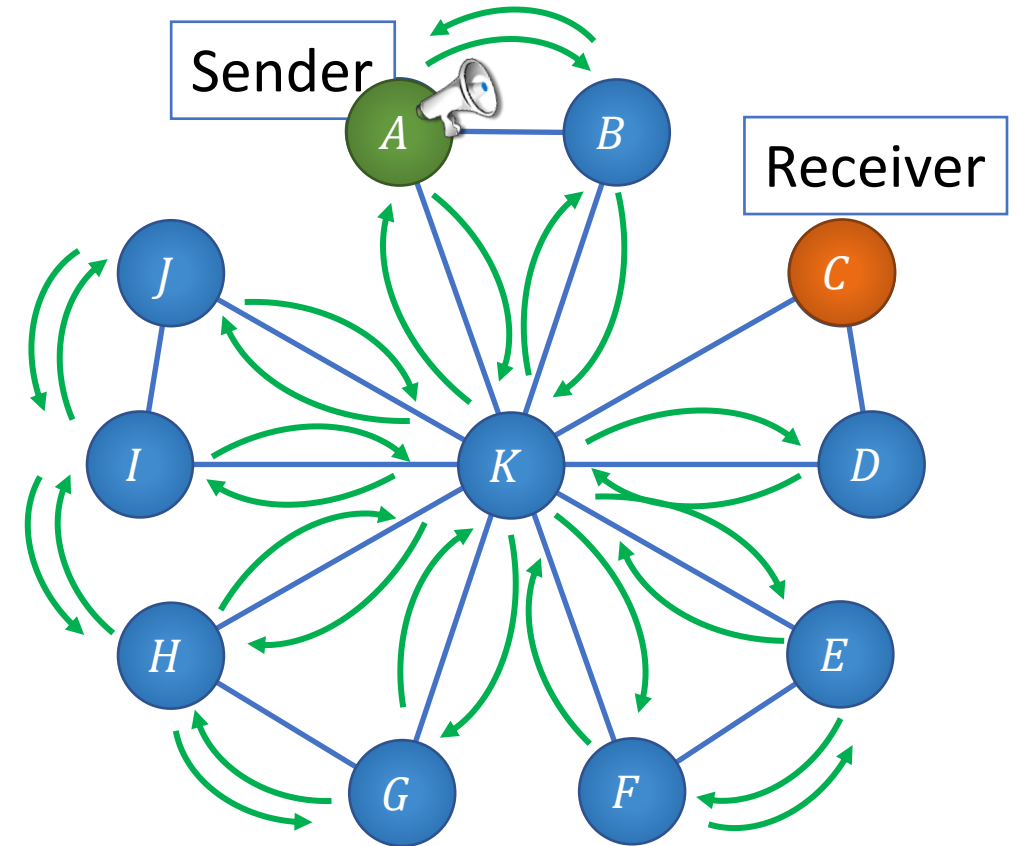
The friendship protocol

- Say the center knows that D is the third node in the triangle
 - Set $m = m_0 \oplus m_1$
 - Send m_1 to D
 - Each send their share to C
- But who is it?
- Center plays towards everyone as if they're the neighbor of C



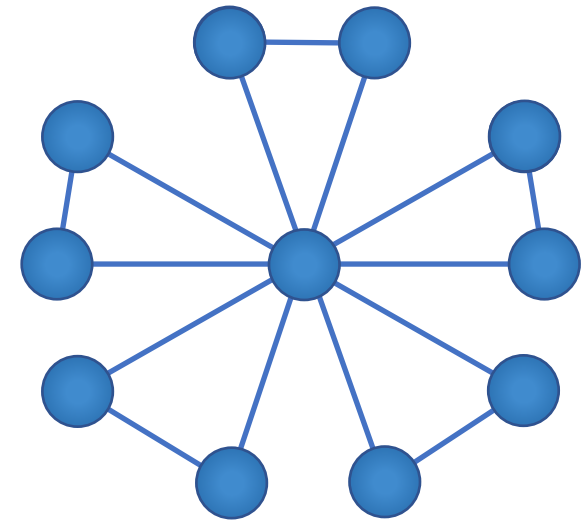
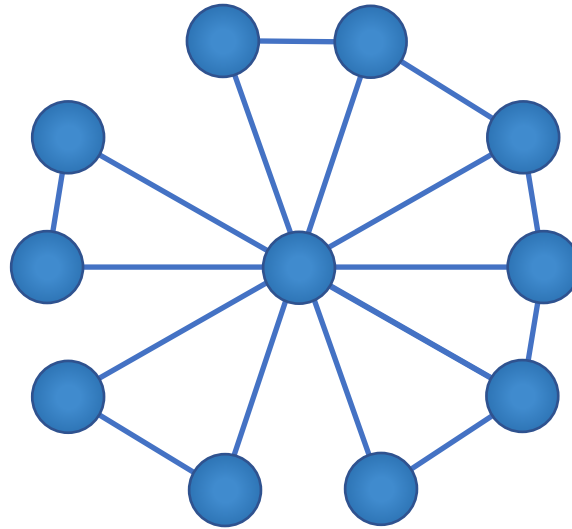
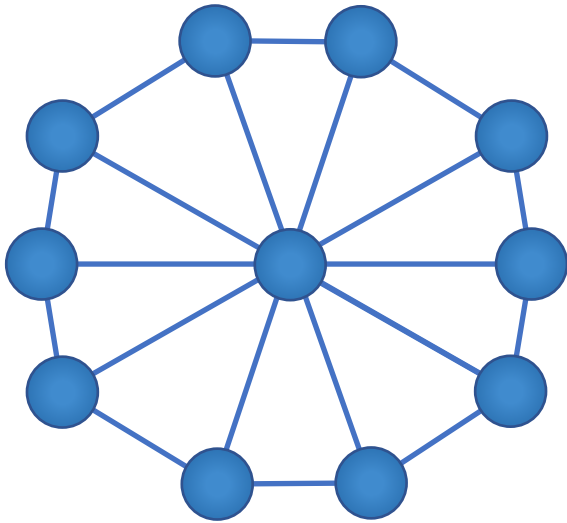
The friendship protocol

- Say the center knows that D is the third node in the triangle
 - Set $m = m_0 \oplus m_1$
 - Send m_1 to D
 - Each send their share to C
 - But who is it?
 - Center plays towards everyone as if they're the neighbor of C
- ⇒ every node plays as if it's the center towards their neighbors (sharing 0)
- More subtle if the receiver is the center



1-secure IT-THB beyond friendship

- Extend to arbitrary admissible graphs (non-center degree is 0, 2 or 3)
 - Careful: graphs no longer have the local behavior
- ⇒ Many subtle attacks to address (see paper for details)
- ⇒ Supports only 1 corruption

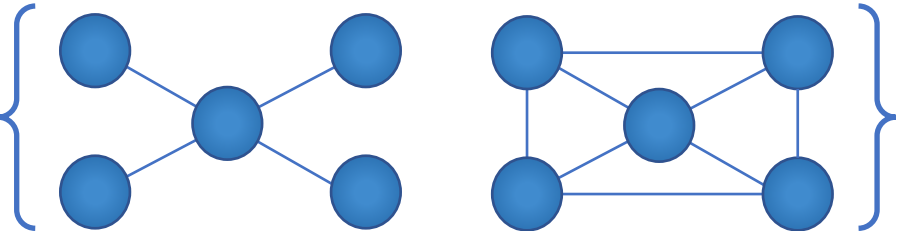


Agenda

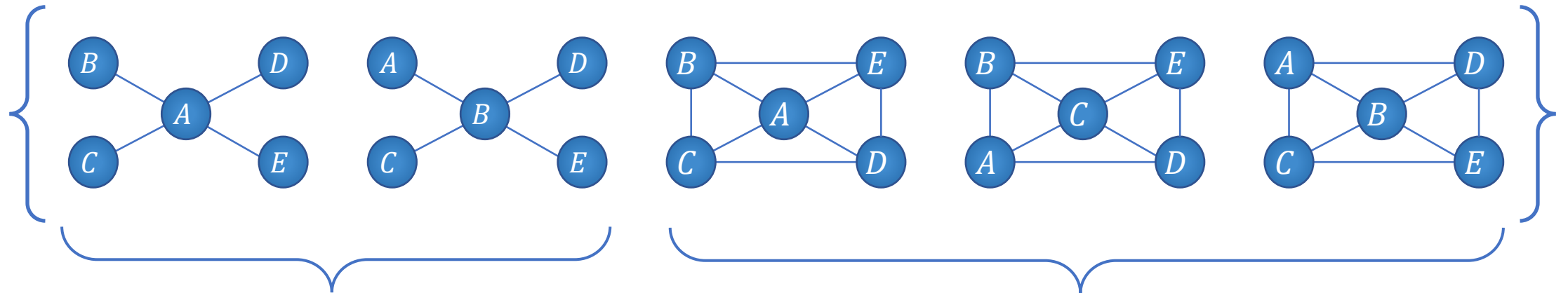
- Our results in a nutshell
- Characterization of wheel subgraphs
- Friendship graphs
- Lower bound



1-secure THB on Wheel & Star \Rightarrow KA

- Assume a 1-secure THB for 

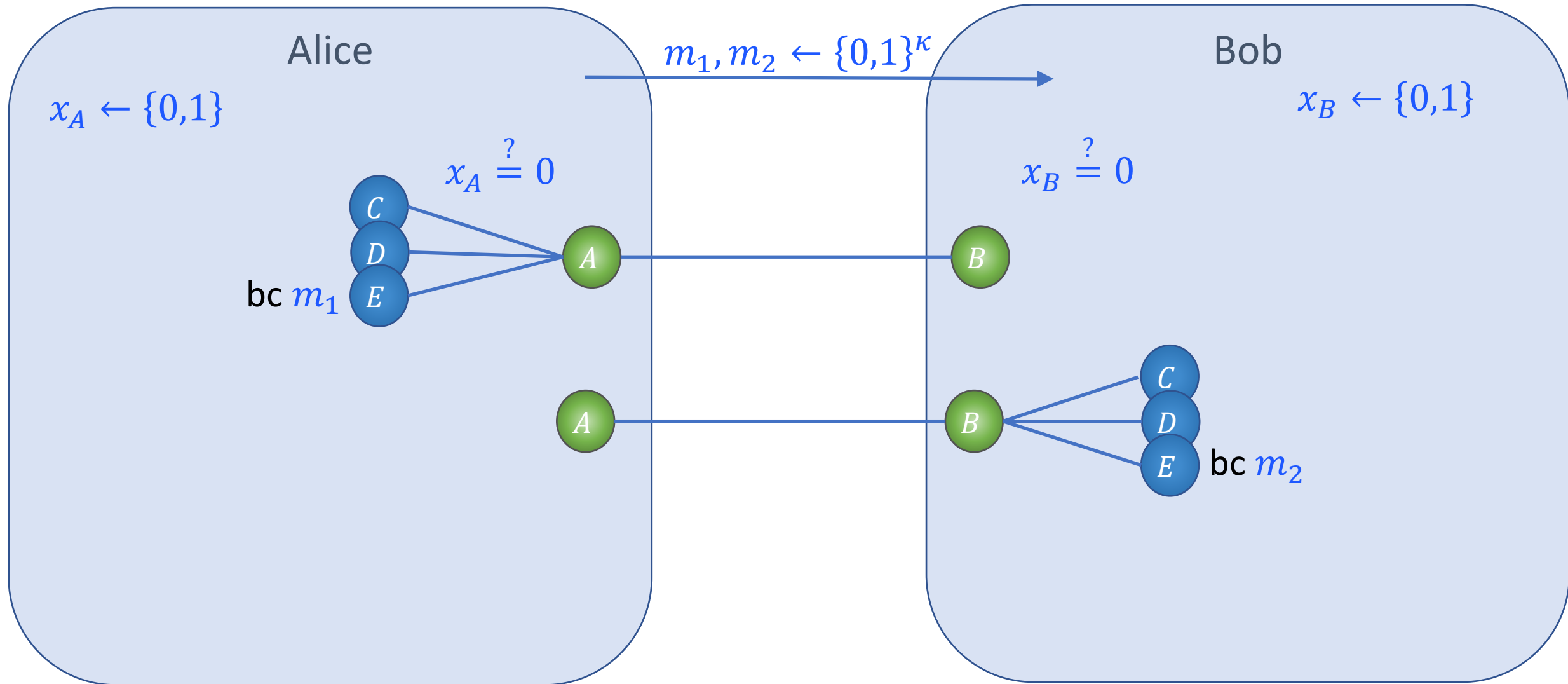
- Proof will use the following labeled graphs:



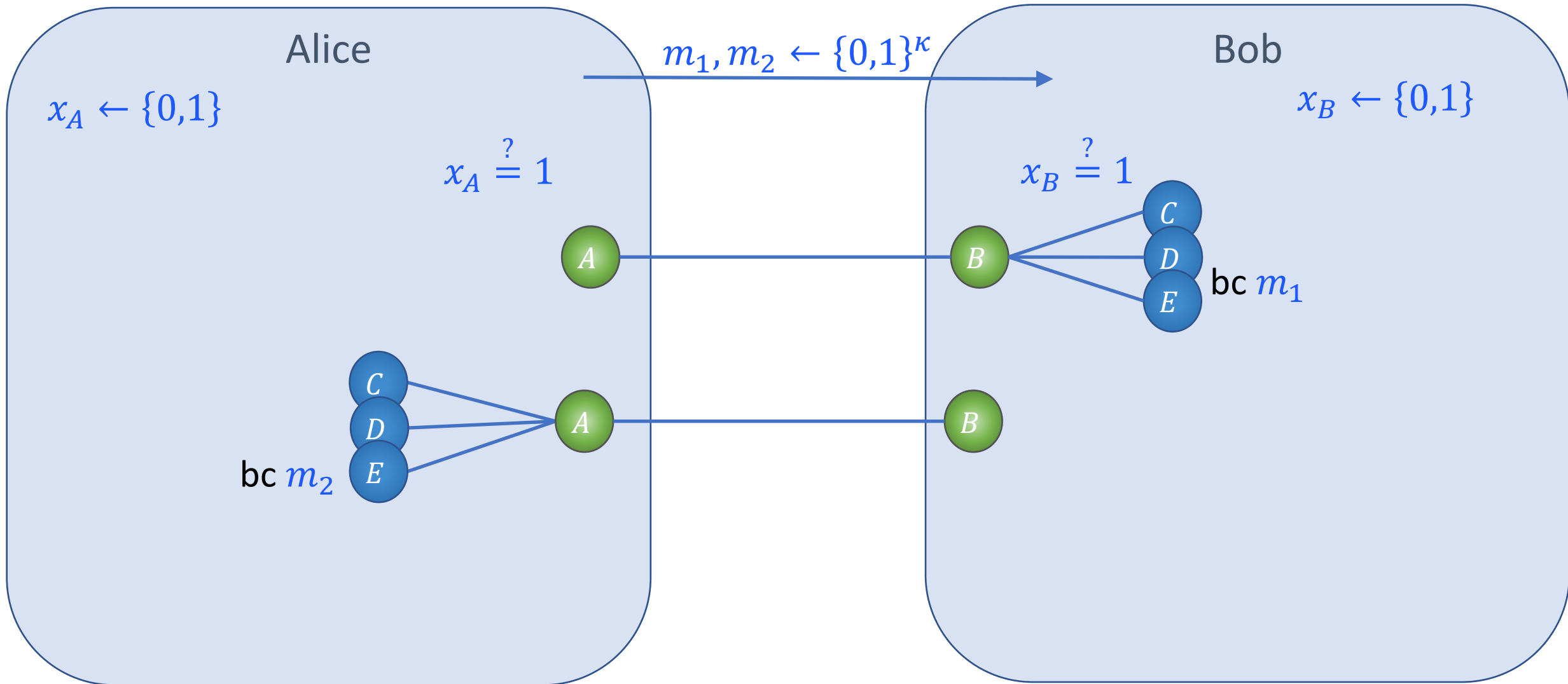
Used to construct KA

Required by security proof

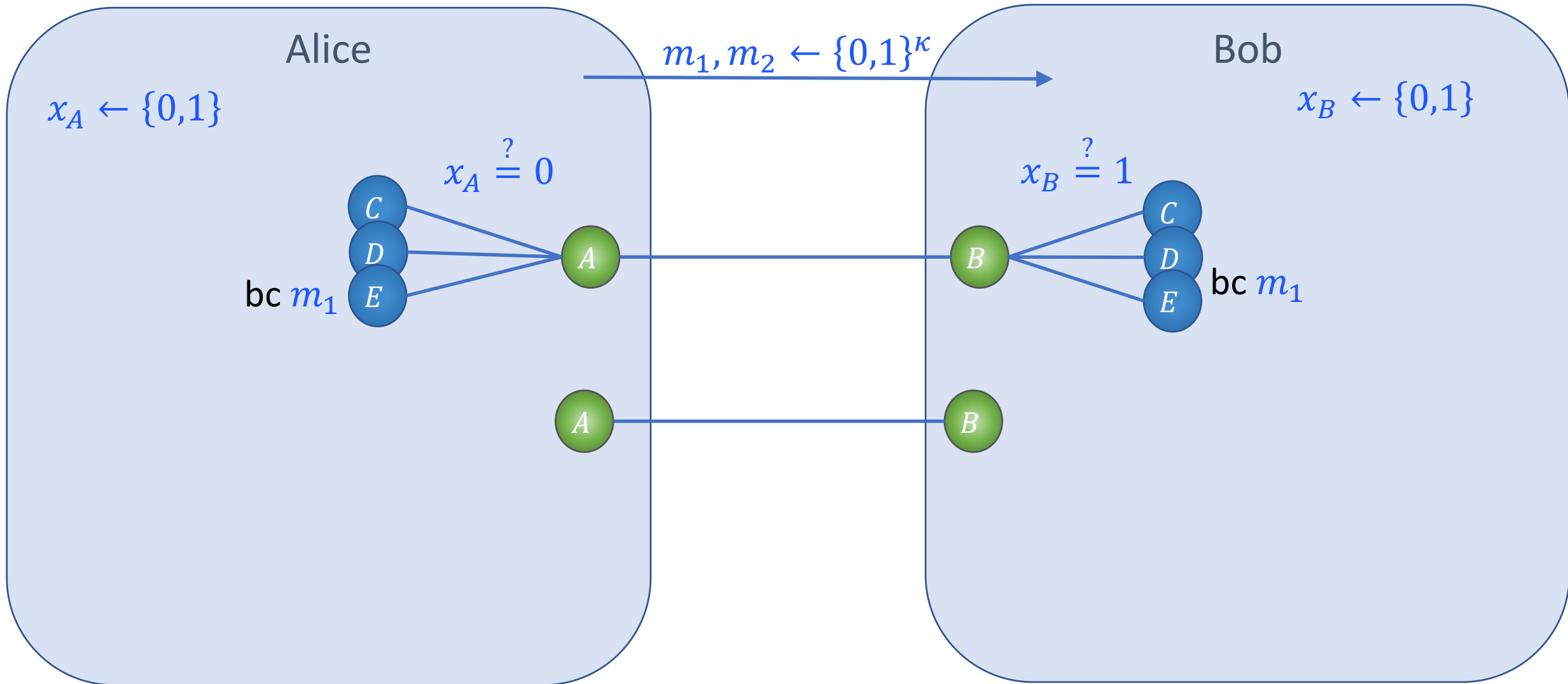
Constructing KA from THB



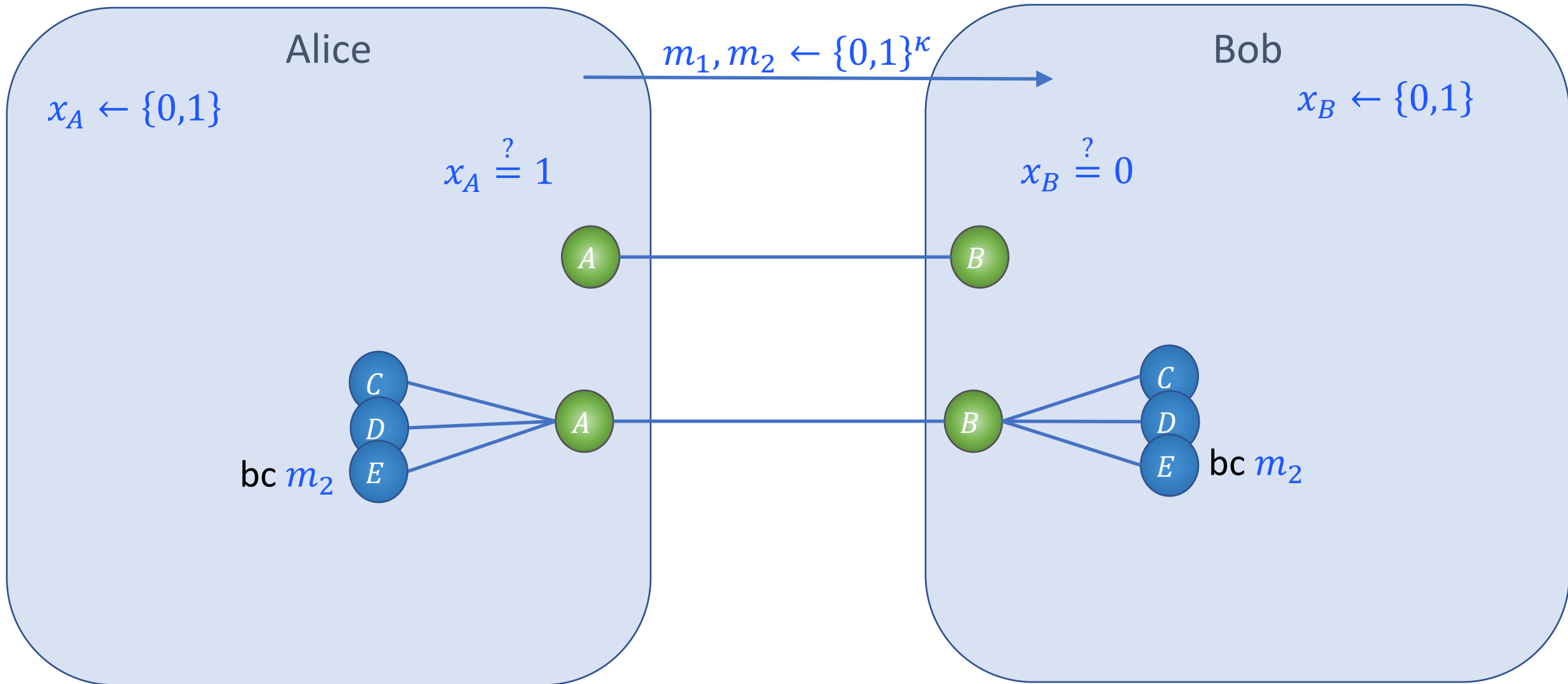
Constructing KA from THB



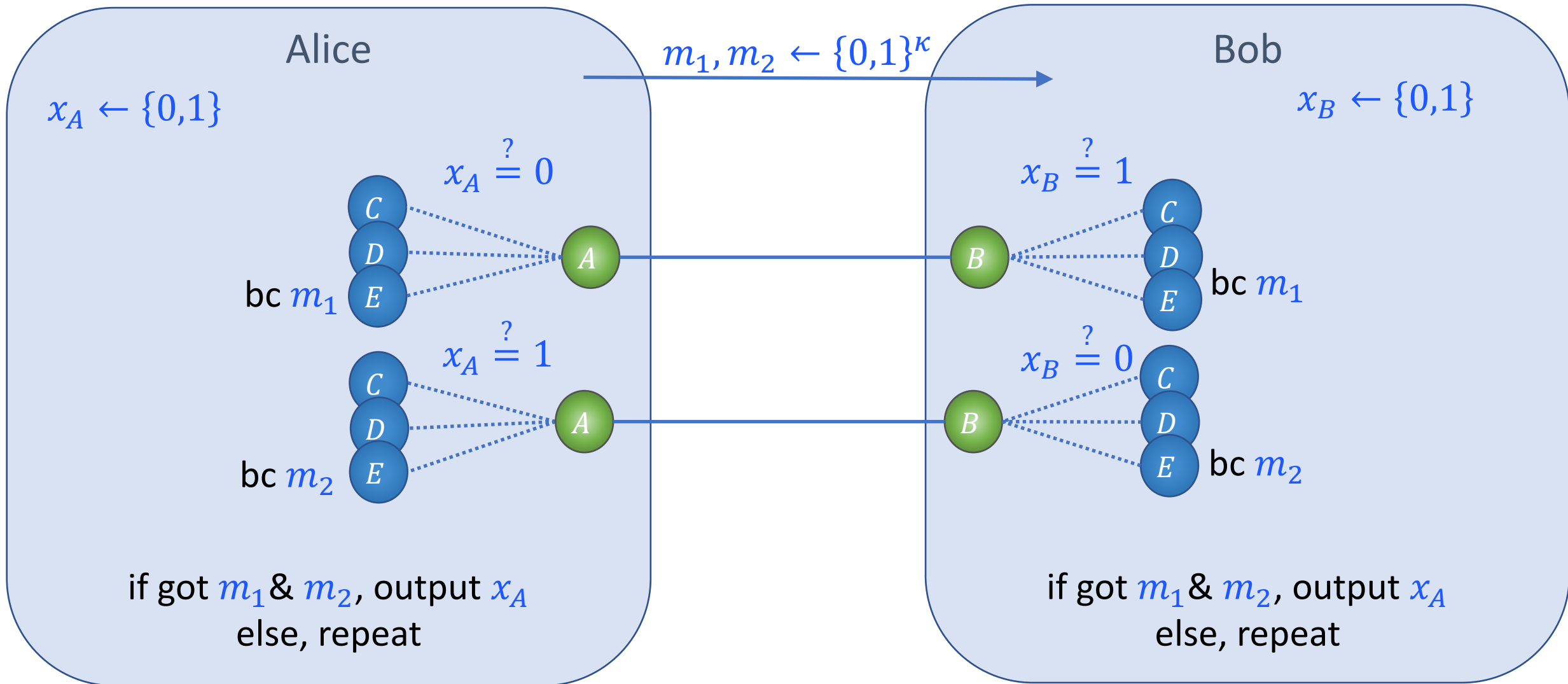
Constructing KA from THB



Constructing KA from THB

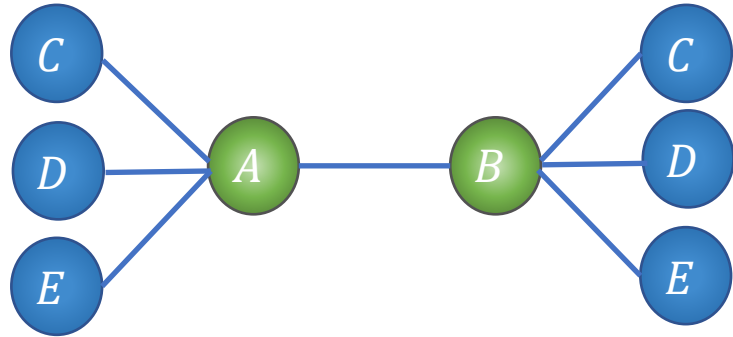


Constructing KA from THB



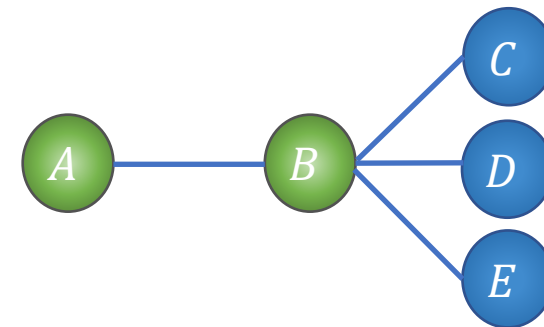
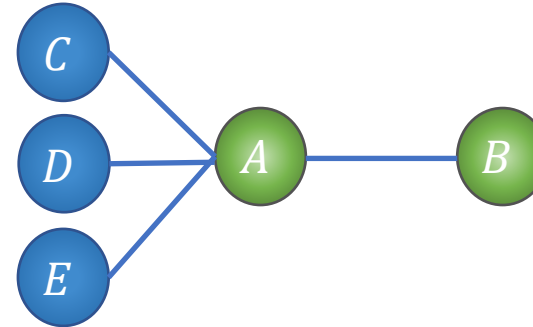
Protocol analysis

If $x_A \neq x_B$ then THB runs are



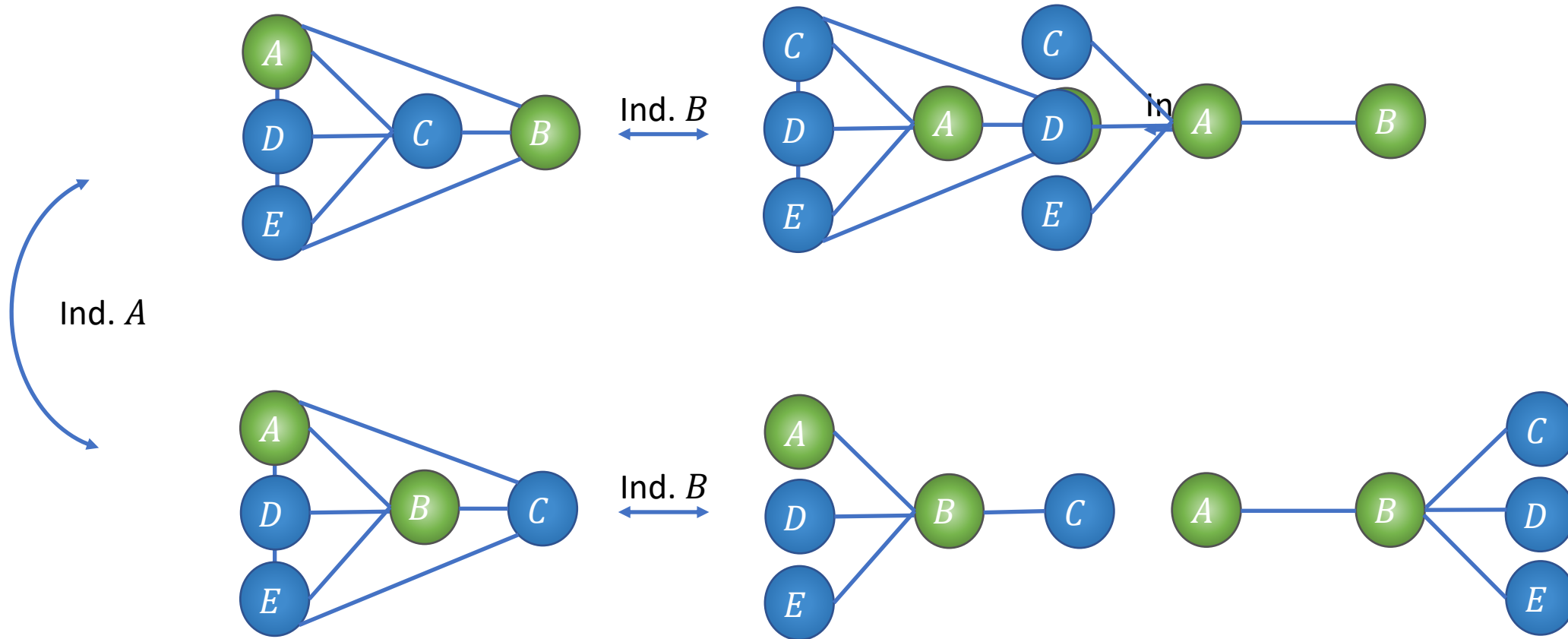
Output is m_1, m_2 wp $2^{-\kappa}$

If $x_A = x_B$ then THB runs are



THB security \Rightarrow KA security

Protocol analysis



Summary

- Characterizing 1-secure IT-THB for wheels & star-embedded subgraphs
- First feasibility of **perfect** 1-secure IT-THB beyond cycles
- First feasibility of IT-THB with $t < n$

Many open questions

- Which graph properties enable IT-THB?
- Which graph properties enable $t > 1$ corruptions?
- Malicious security?

Thank you for listening 😊

