Topology-Hiding Communication from Minimal Assumptions

Marshall Ball, Elette Boyle, Ran Cohen, Lisa Kohl,
Tal Malkin, Pierre Meyer, Tal Moran

TCC 2020

Topology-Hiding Computation

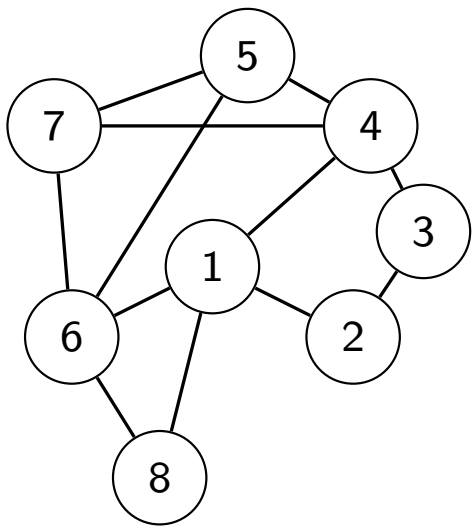
Topology-Hiding Computation:
[Moran-Orlov-Richelson'15]

- (MPC over Incomplete Network)
- (Topology-Hiding) Parties can only see their local view
- (Topology-Hiding) Reveals nothing else about the graph

Topology-Hiding Computation

Topology-Hiding Computation:
[Moran-Orlov-Richelson'15]

- (MPC over Incomplete Network)
- (Topology-Hiding) Parties can only see their local view
- (Topology-Hiding) Reveals nothing else about the graph

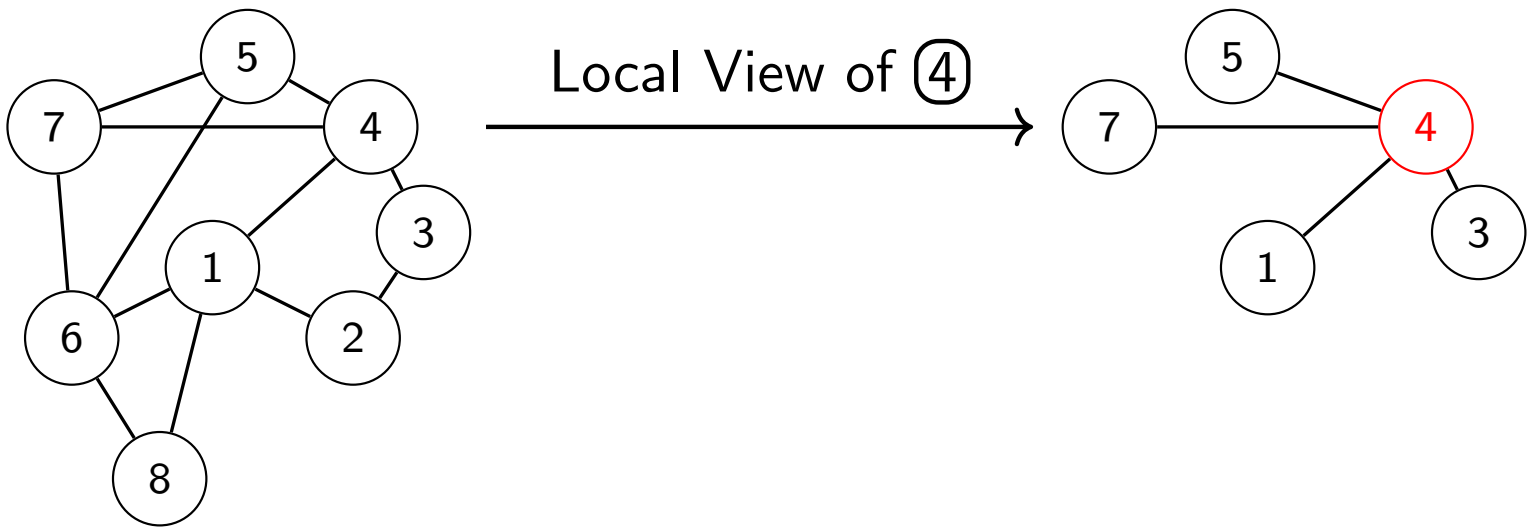


Topology-Hiding Computation

Topology-Hiding Computation:

[Moran-Orlov-Richelson'15]

- (MPC over Incomplete Network)
- (Topology-Hiding) Parties can only see their local view
- (Topology-Hiding) Reveals nothing else about the graph

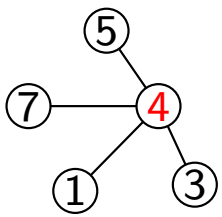


Topology-Hiding Computation

Topology-Hiding Computation:
[Moran-Orlov-Richelson'15]

- (MPC over Incomplete Network)
- (Topology-Hiding) Parties can only see their local view
- (Topology-Hiding) Reveals nothing else about the graph

$$\mathsf{Sim}(\mathcal{G}, \mathsf{LocalView}_4) \quad \simeq \quad \mathsf{View}_4$$



Topology-Hiding Computation

Topology-Hiding Computation:
[Moran-Orlov-Richelson'15]

- (MPC over Incomplete Network)
- (Topology-Hiding) Parties can only see their local view
- (Topology-Hiding) Reveals nothing else about the graph

[MOR'15], [HMTZ'16], [AM'17], [ALM'17],
[BBMM'18], [LLMMMT'18], [BBCMM'19], [LLMMMT'20]

(Please see full version of talk for details)

Our work: The Simplest Setting

- **Broadcast** Only
  (and Anonymous Broadcast)
- **One Semi-Honest** Corruption
- Synchronous Communication

Our work: The Simplest Setting

- **Broadcast** Only
  (and Anonymous Broadcast)
- **One Semi-Honest** Corruption
- Synchronous Communication

1-THB / 1-THAB

Our work: The Simplest Setting

- **Broadcast** Only
  (and Anonymous Broadcast)
- **One Semi-Honest** Corruption
- Synchronous Communication

1-THB / 1-THAB

Trivial without Topology-Hiding
(just flood the graph)

Our work: The Simplest Setting

- **Broadcast** Only
  (and Anonymous Broadcast)
- **One Semi-Honest** Corruption
- Synchronous Communication

1-THB / 1-THAB

Trivial without Topology-Hiding
(just flood the graph)

Very Rich with Topology-Hiding!

For each graph class, what is the minimal (cryptographic) assumption required for 1-THB and 1-THAB?

For each graph class, what is the minimal (cryptographic) assumption required for 1-THB and 1-THAB?

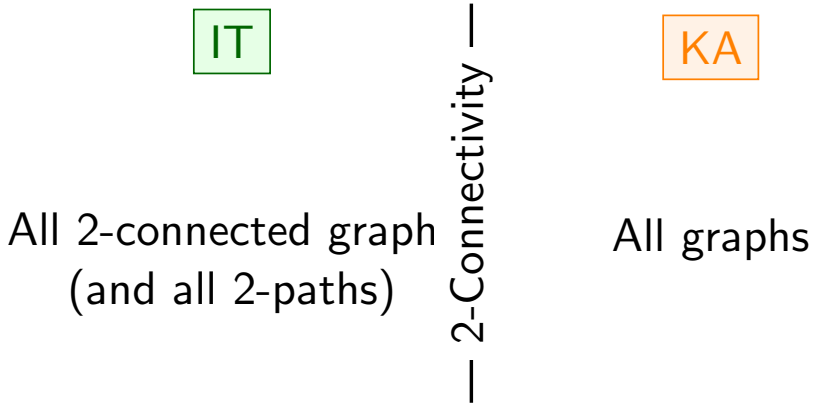
For each graph class, what is the minimal (cryptographic) assumption required for 1-THB and 1-THAB?

Information Theoretic (IT) / Key-Agreement (KA) / Oblivious Transfer (OT)

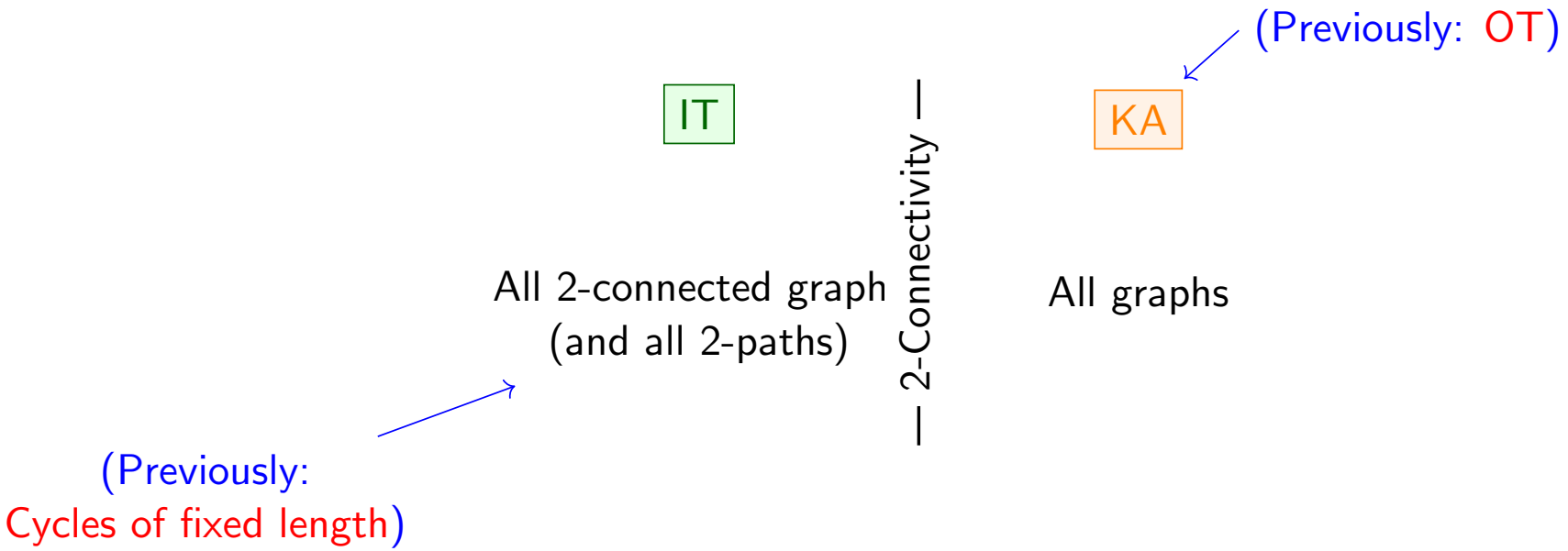
Topology-Hiding Broadcast ($t = 1$)

IT	KA
All 2-connected graphs (and all 2-paths)	All graphs

Topology-Hiding Broadcast ($t = 1$)



Topology-Hiding Broadcast ($t = 1$)



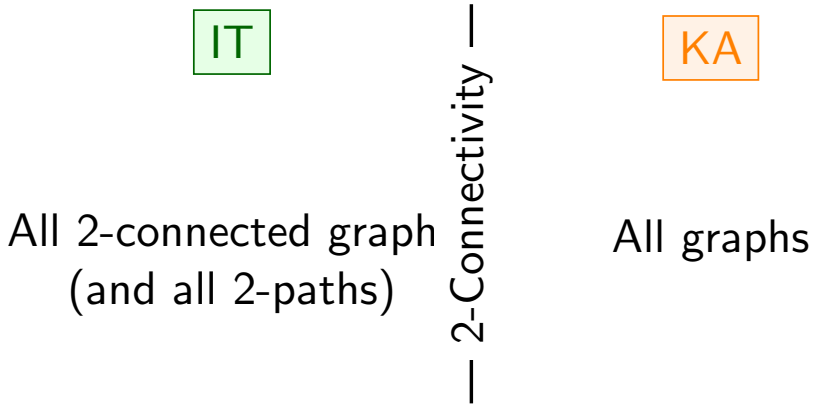
Topology-Hiding Broadcast ($t = 1$)

IT	2-Connectivity	KA
All 2-connected graph (and all 2-paths)		All graphs

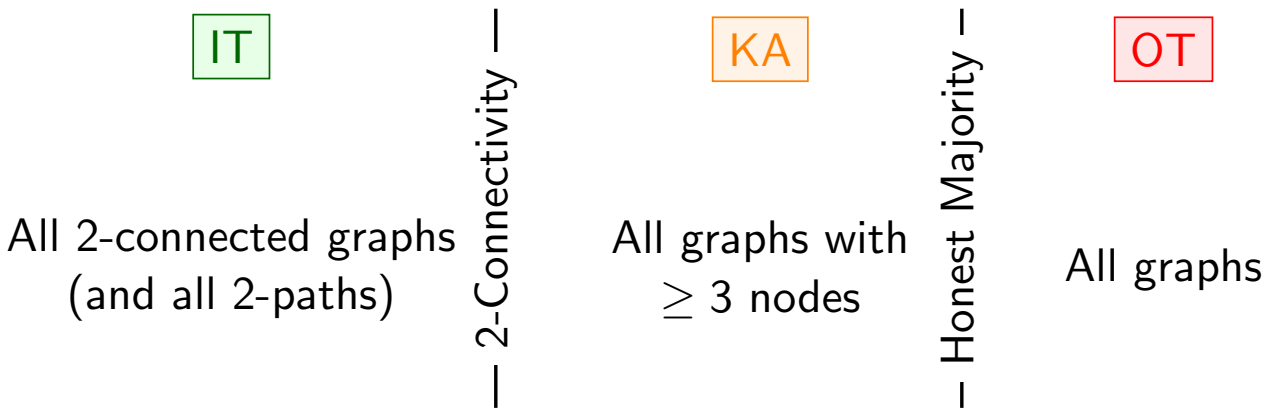
Topology-Hiding Anonymous Broadcast ($t = 1$)

IT	2-Connectivity	KA	OT
All 2-connected graphs (and all 2-paths)		All graphs with ≥ 3 nodes	All graphs

Topology-Hiding Broadcast ($t = 1$)



Topology-Hiding Anonymous Broadcast ($t = 1$)



Topology-Hiding Broadcast ($t = 1$)

IT

All 2-connected graph
(and all 2-paths)

– 2-Connectivity –

KA

All graphs

Topology-Hiding Anonymous Broadcast ($t = 1$)

IT

All 2-connected graphs
(and all 2-paths)

– 2-Connectivity –

KA

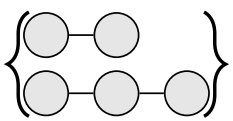
All graphs with
≥ 3 nodes

– Honest Majority –

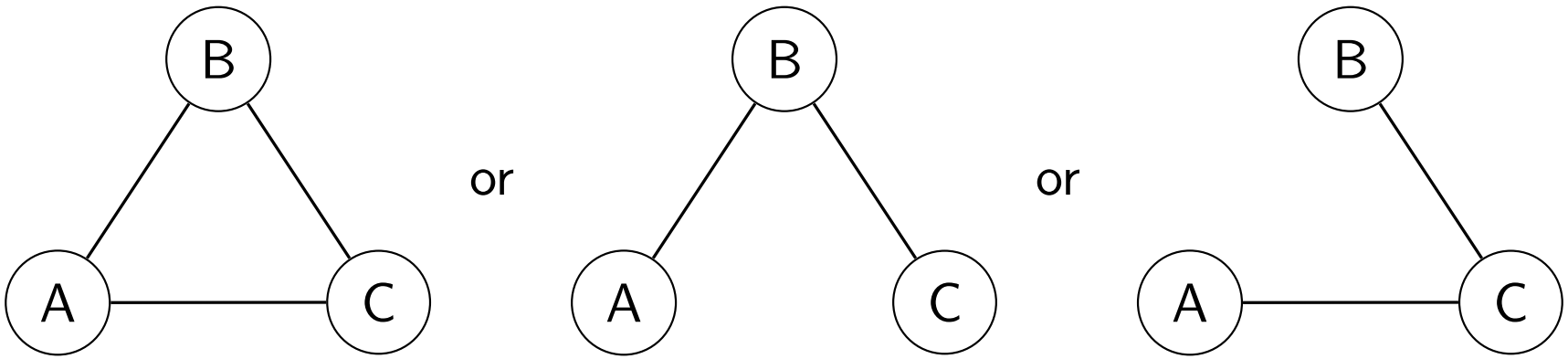
OT

~~All graphs~~

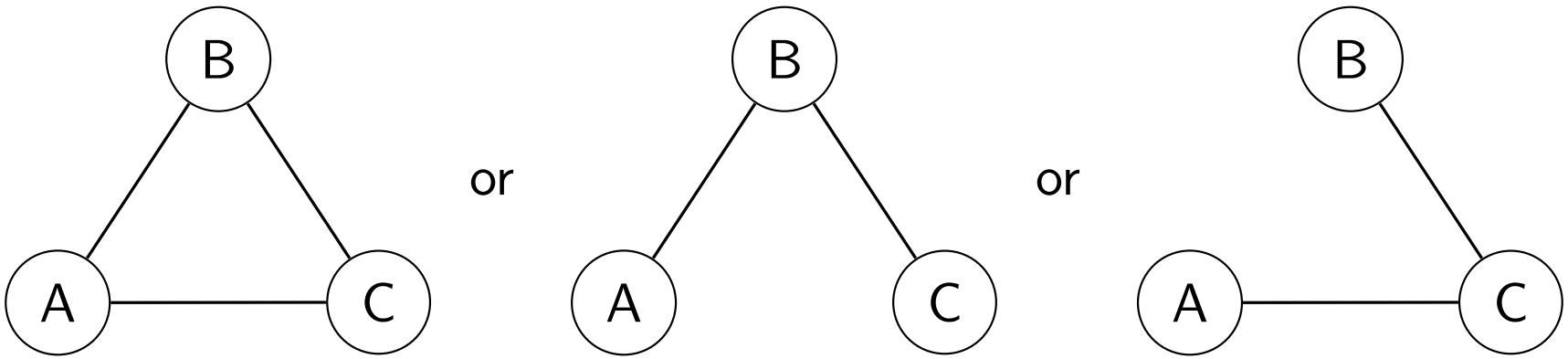
$\{2, 3\}$-Paths
are enough!

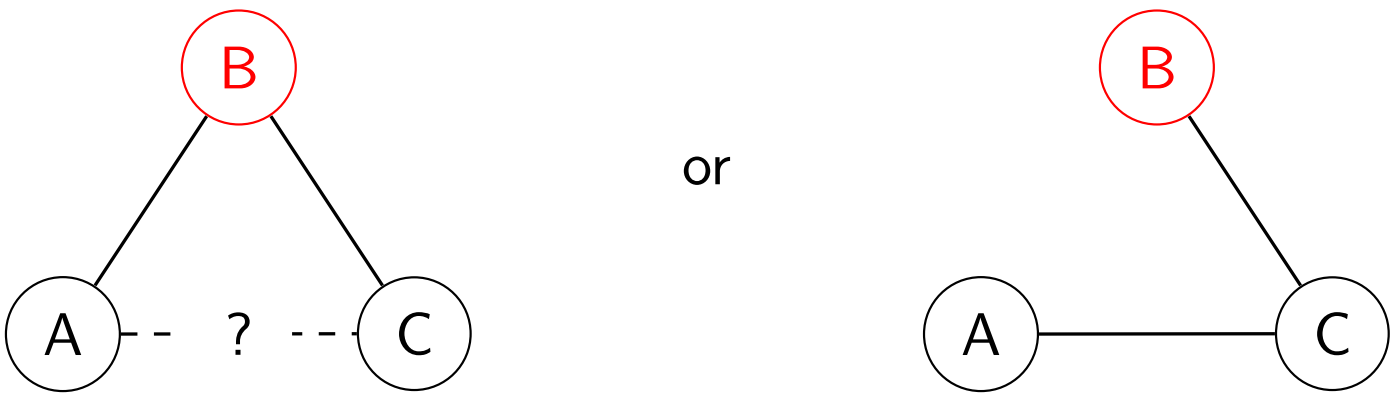


Topology-Hiding Broadcast on 'The Triangle'

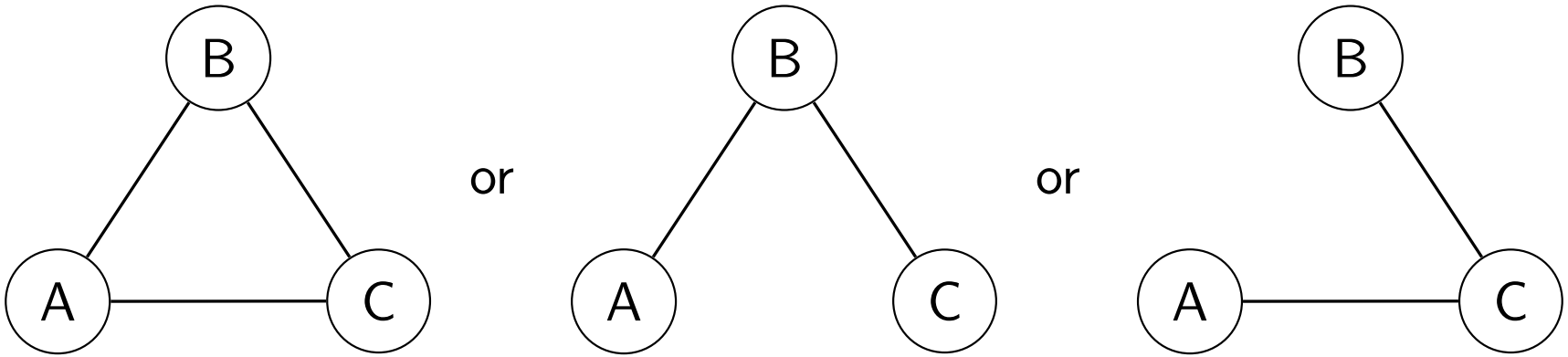


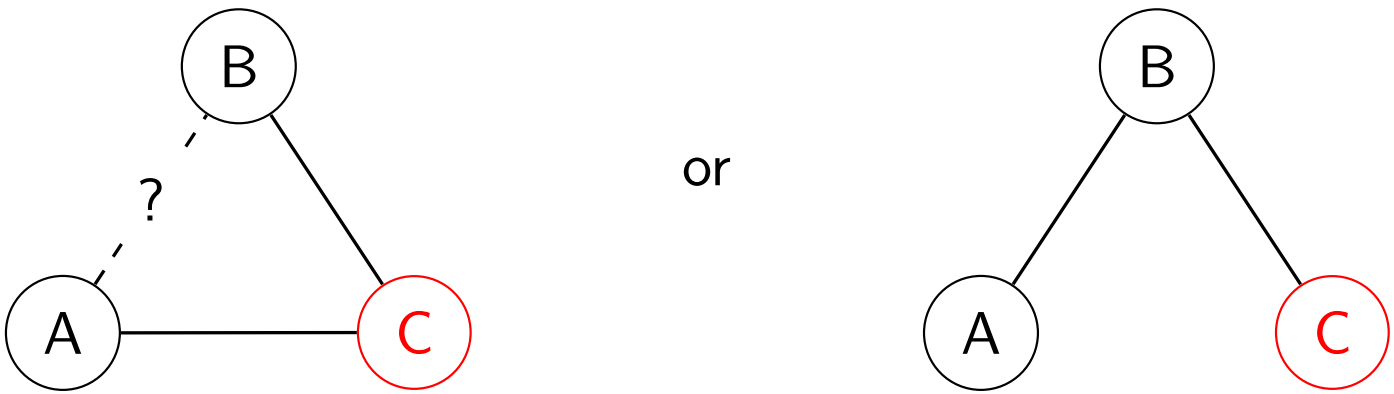
Topology-Hiding Broadcast on 'The Triangle'



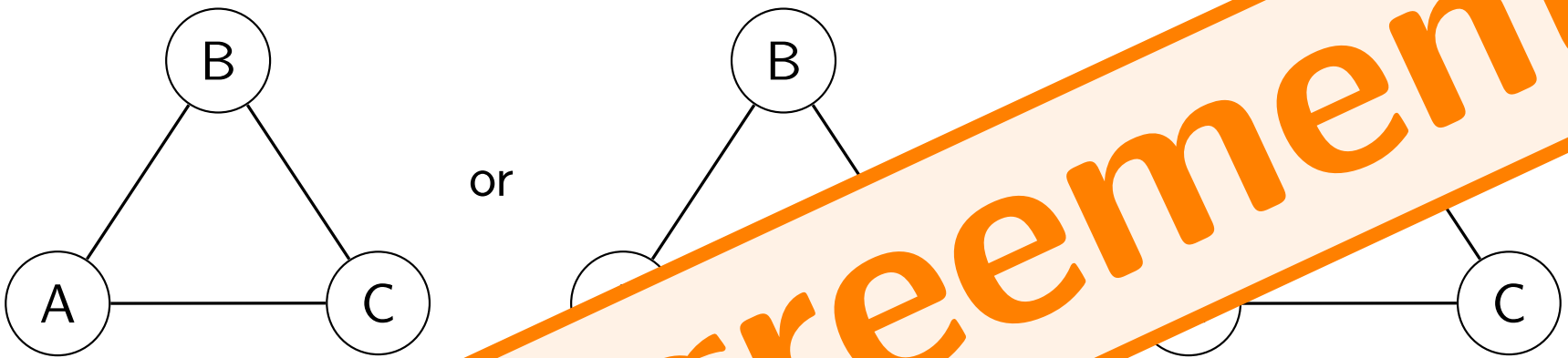


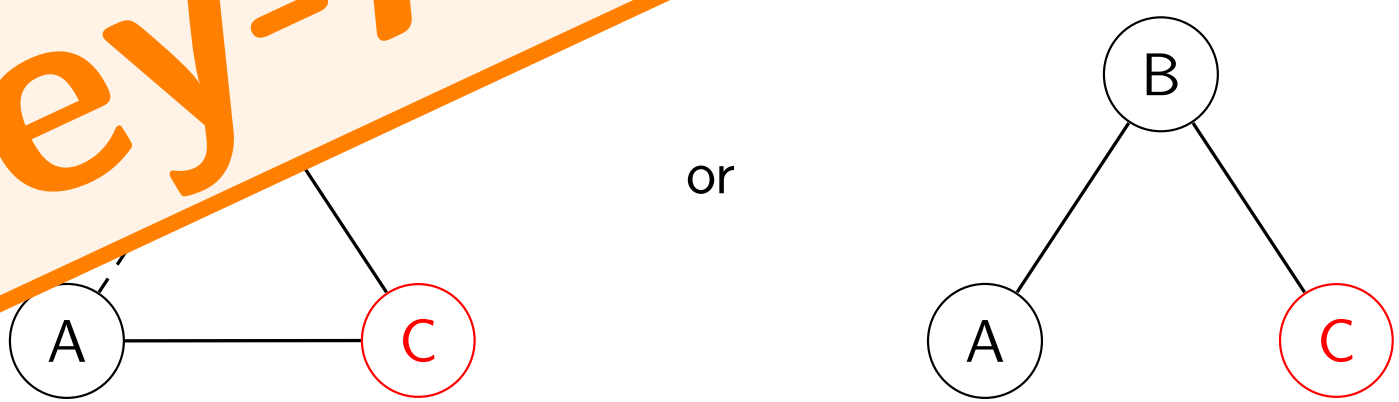
Topology-Hiding Broadcast on 'The Triangle'





Topology-Hiding Broadcast on 'The Triangle'





Key-Agreement

Thank You!