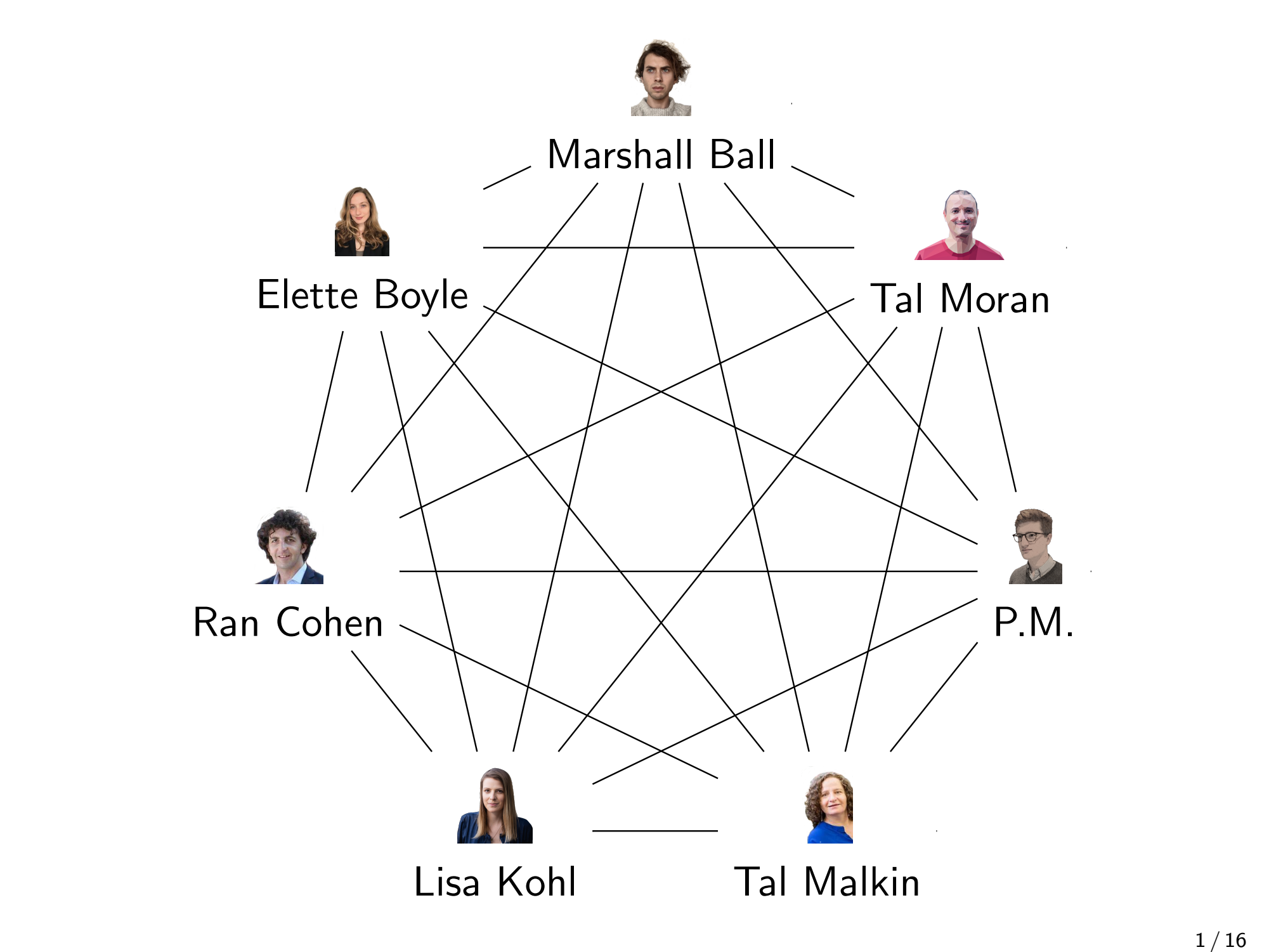
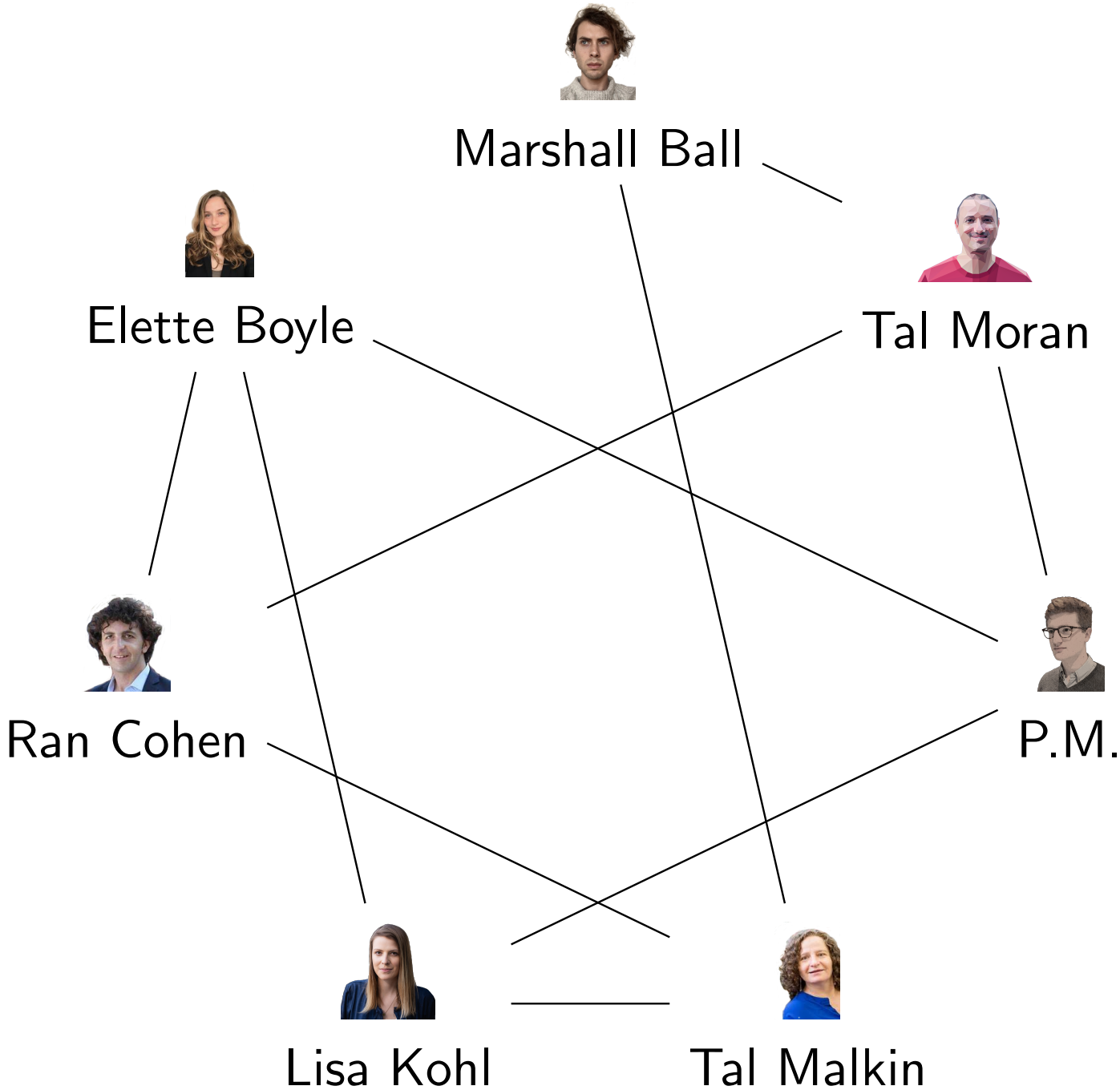
Topology-Hiding Communication from Minimal Assumptions

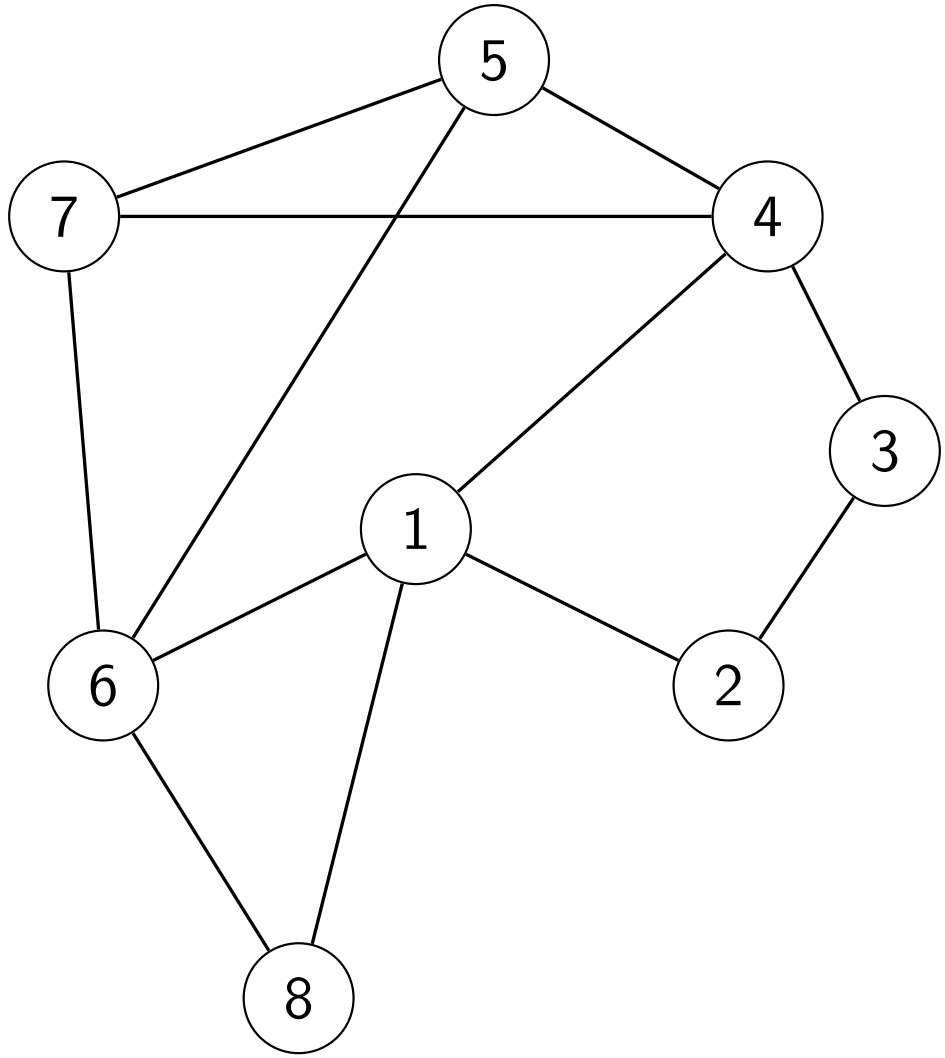
Marshall Ball, Elette Boyle, Ran Cohen, Lisa Kohl,
Tal Malkin, Pierre Meyer, Tal Moran

TCC 2020

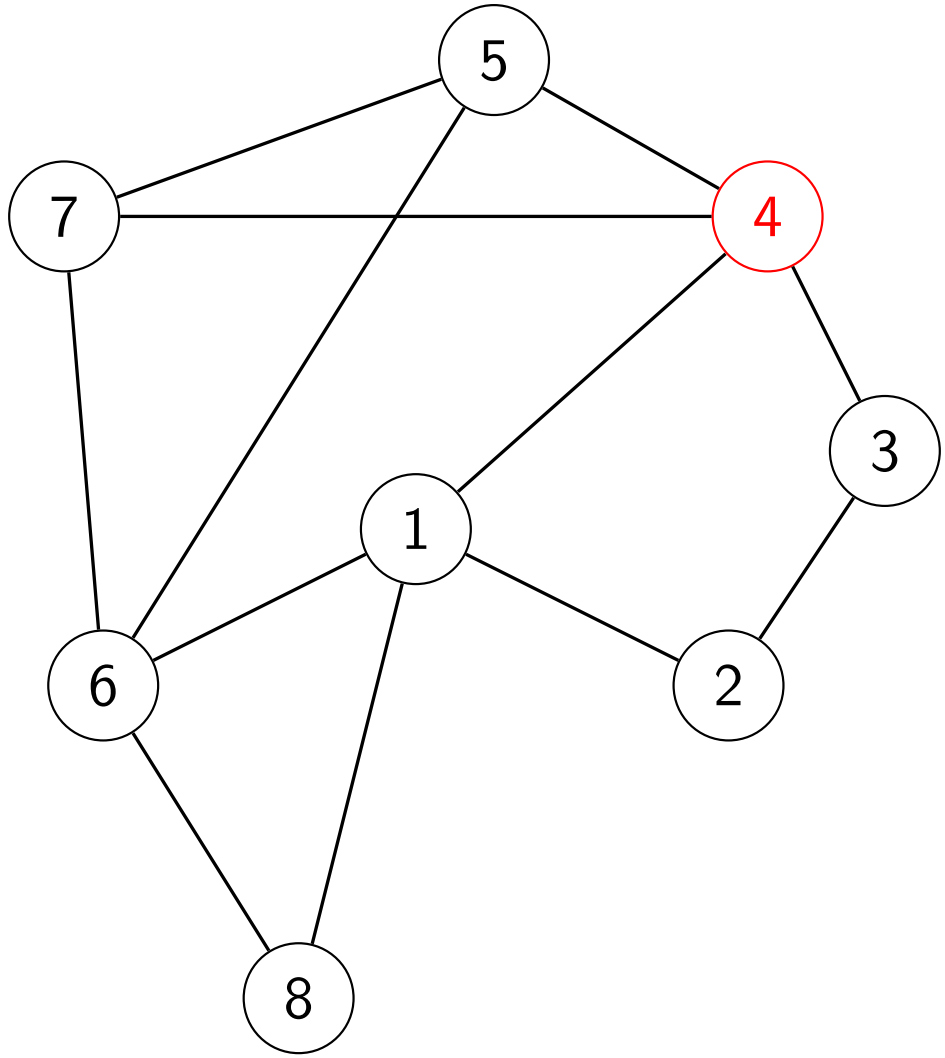

Marshall Ball
Elette Boyle
Tal Moran
Ran Cohen
P.M.
Lisa Kohl
Tal Malkin


Marshall Ball
Elette Boyle
Tal Moran
Ran Cohen
P.M.
Lisa Kohl
Tal Malkin

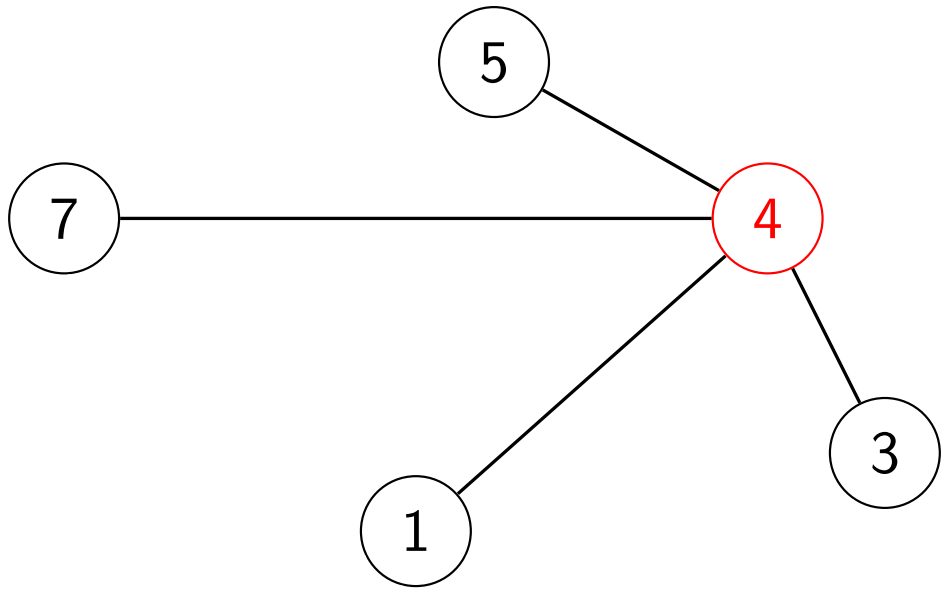
Local View of a Network



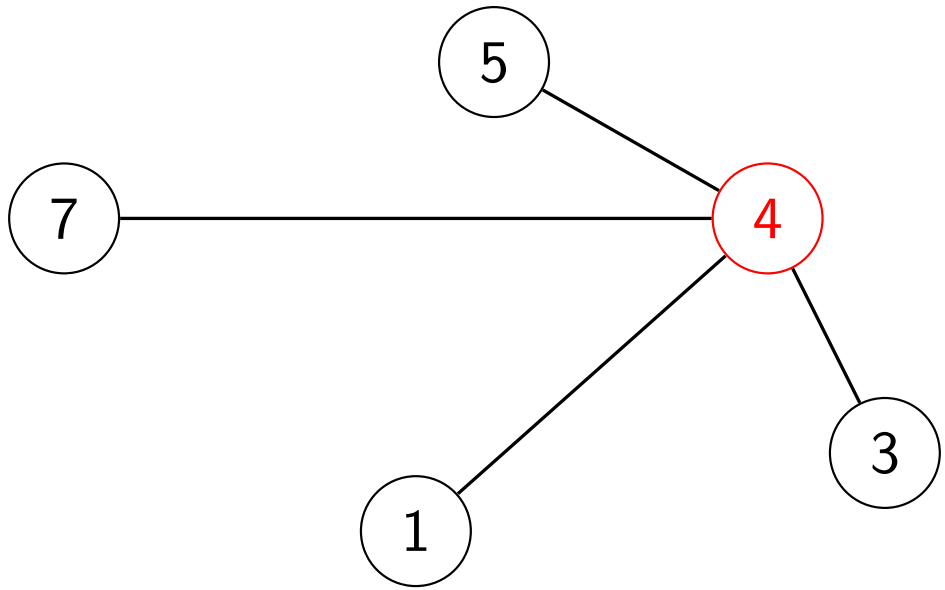
Local View of a Network



Local View of a Network



Local View of a Network



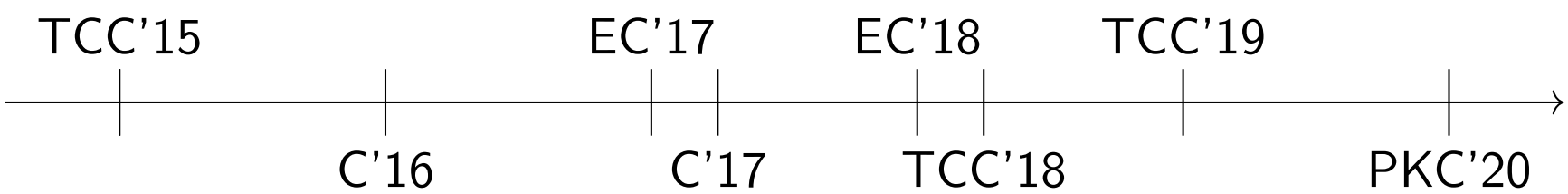
Topology-Hiding Computation:

- Parties can only see their local view
- The MPC reveals nothing else about the graph

Difficulties of Topology-Hiding Computation

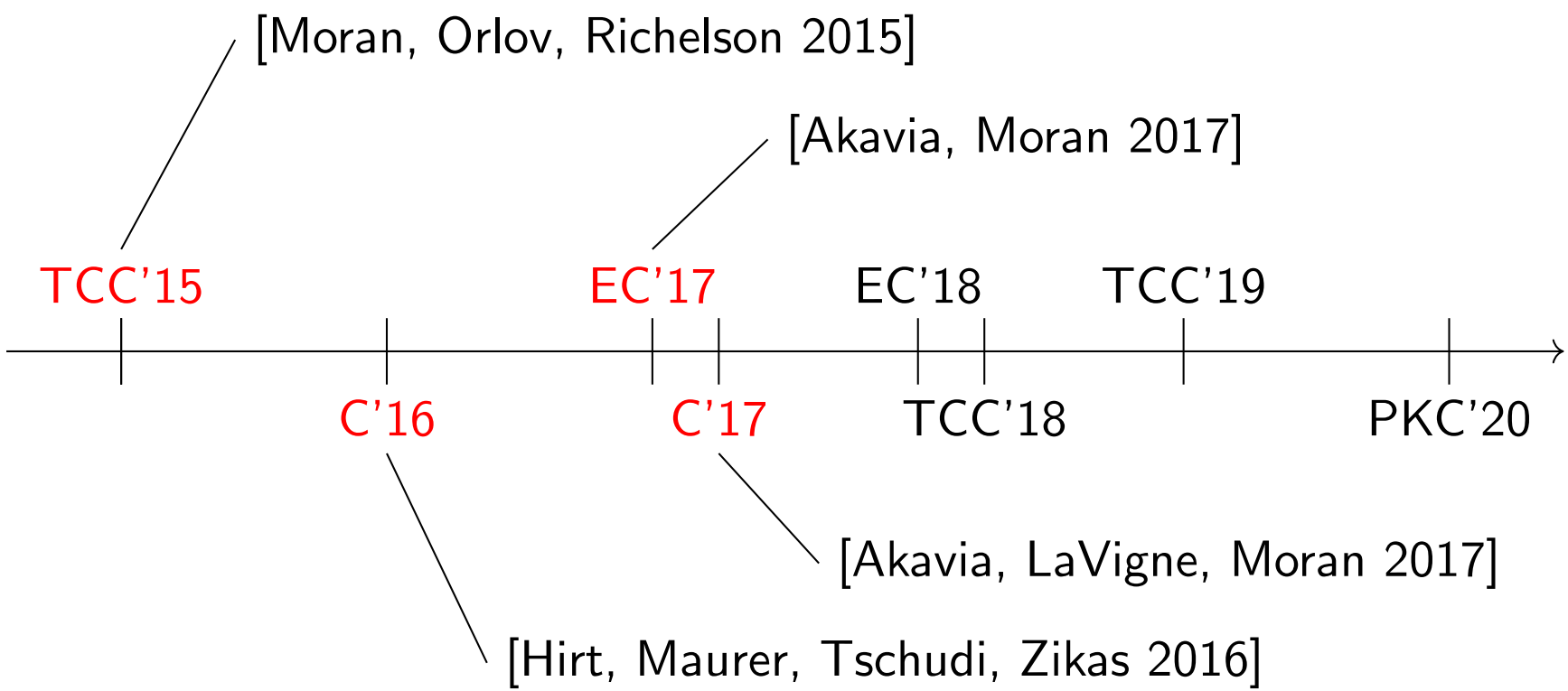
1. Fewer point-to-point secure channels
2. Only local views (and graph class) initially known
3. The topology of the network should not be leaked

Previous Works



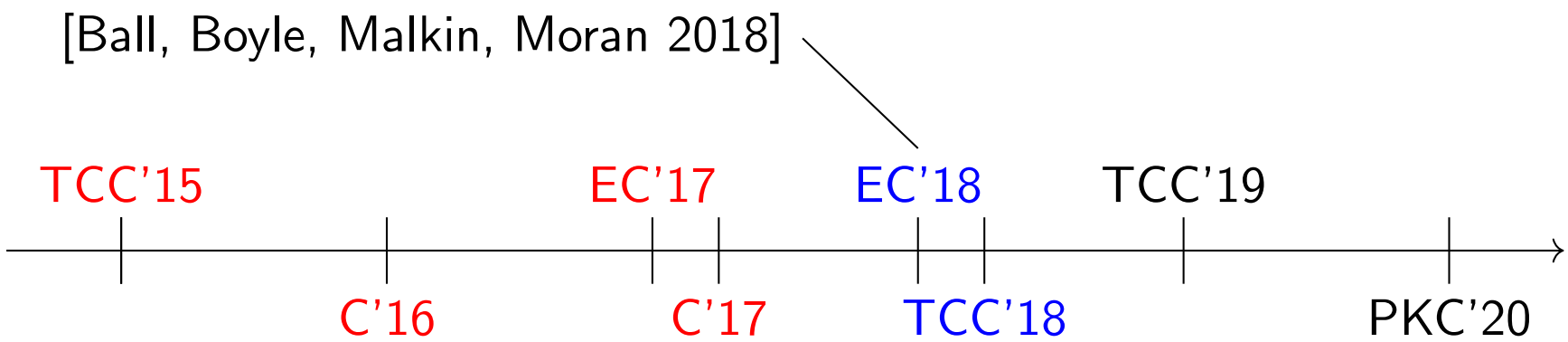
Previous Works

- Computational (DDH, QR, or LWE), ($t = n - 1$) passive



Previous Works

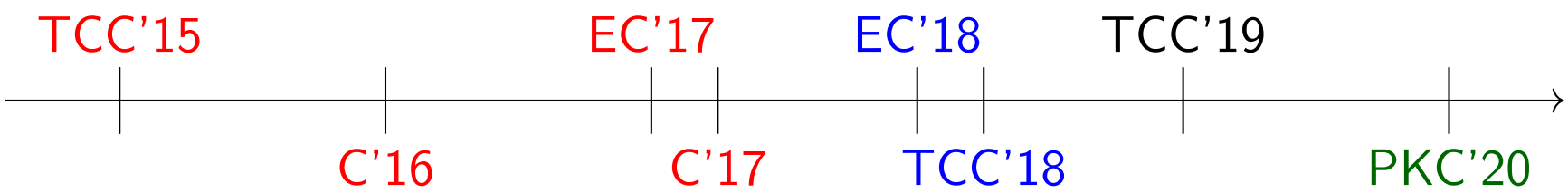
- Computational (DDH, QR, or LWE), ($t = n - 1$) passive
- Computational, ($t = n - 1$) passive + fail-stop



[LaVigne, Liu-Zhang, Maurer, Moran, Mularczyk, Tschudi 2018]

Previous Works

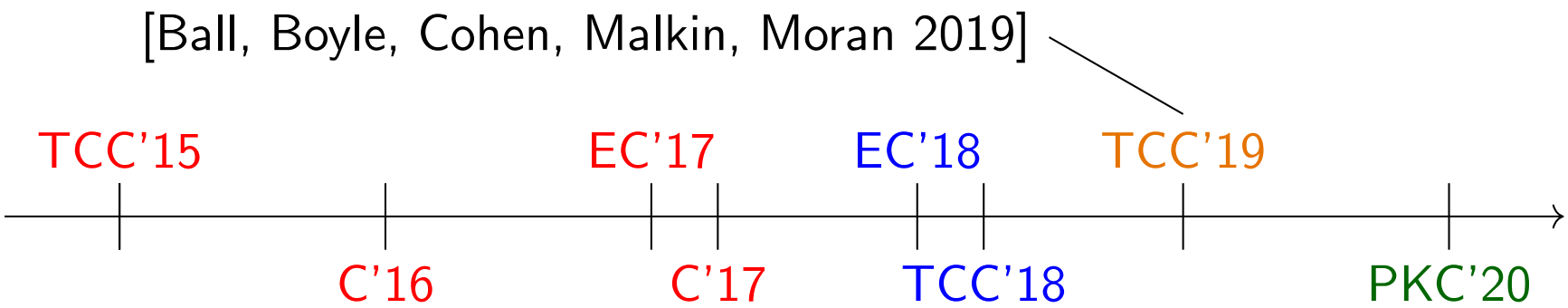
- Computational (DDH, QR, or LWE), ($t = n - 1$) passive
- Computational, ($t = n - 1$) passive + fail-stop
- Asynchronous model, ($t = n - 1$) passive



[LaVigne, Liu-Zhang, Maurer, Moran, Mularczyk, Tschudi 2020]

Previous Works

- Computational (DDH, QR, or LWE), $(t = n - 1)$ passive
- Computational, $(t = n - 1)$ passive + fail-stop
- Asynchronous model, $(t = n - 1)$ passive
- Revisiting information-theoretic setting, $t = 1$ passive



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

Trivial without Topology-Hiding

1-THB

1-THAB

Very Rich with Topology-Hiding!

Our work: The Simplest Setting

- **Broadcast** Only
  (and Anonymous Broadcast)

Trivial without

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

Our work: The Simplest Setting

- **Broadcast** Only
  (and Anonymous Broadcast)

Trivial without

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)

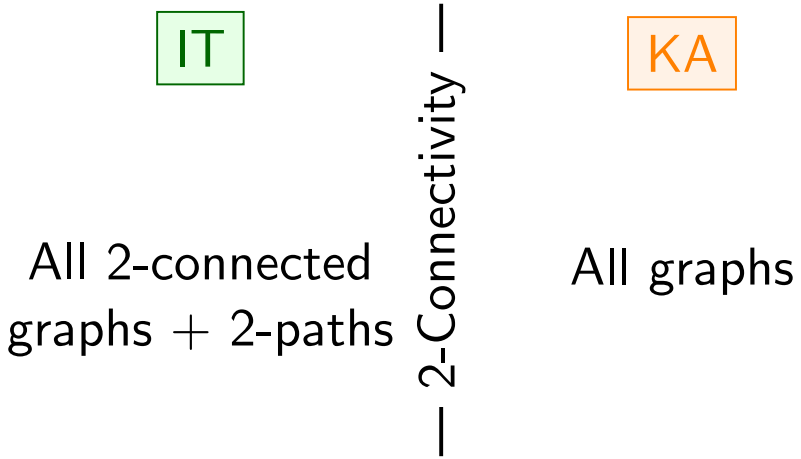
Our Results

Topology-Hiding Broadcast ($t = 1$)

IT	KA
All 2-connected graphs + 2-paths	All graphs

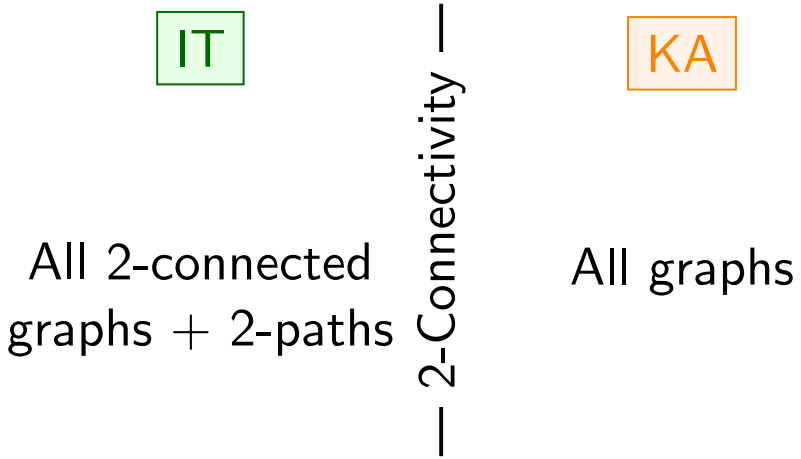
Topology-Hiding Anonymous Broadcast ($t = 1$)

Topology-Hiding Broadcast ($t = 1$)

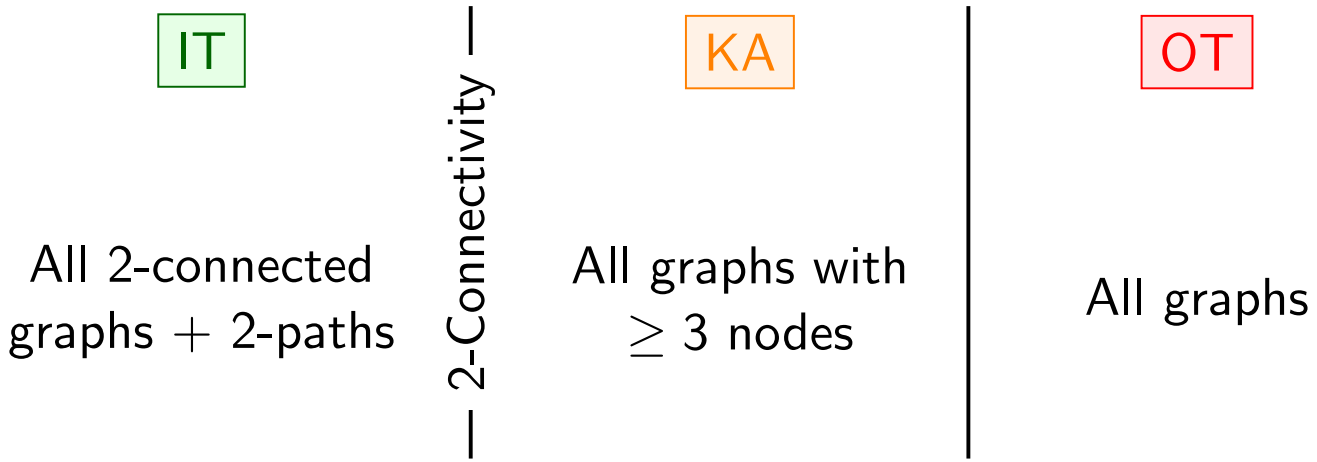


Topology-Hiding Anonymous Broadcast ($t = 1$)

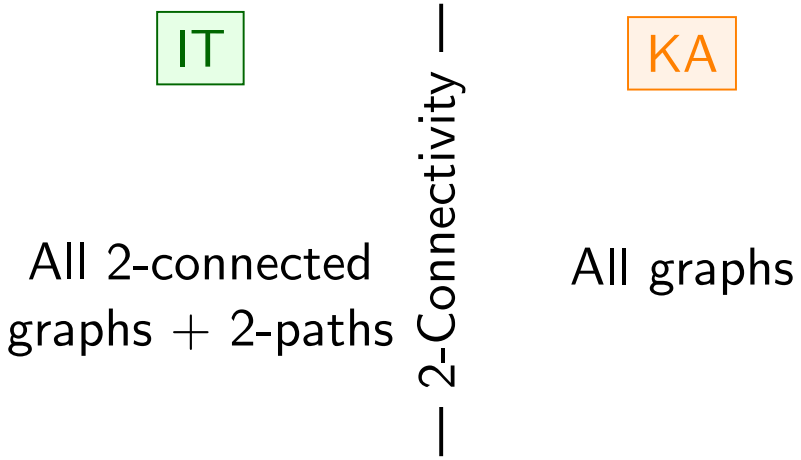
Topology-Hiding Broadcast ($t = 1$)



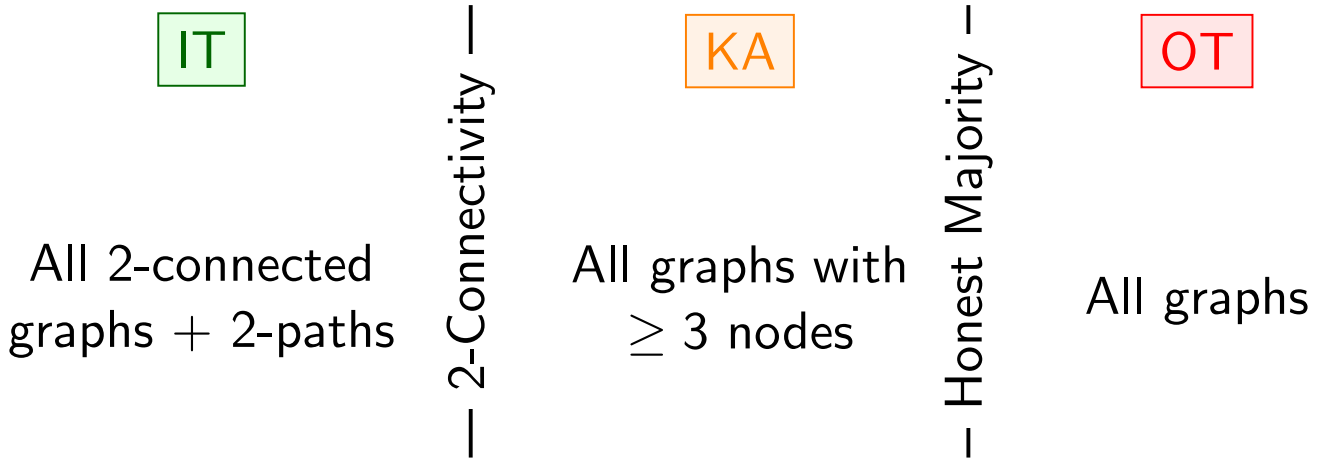
Topology-Hiding Anonymous Broadcast ($t = 1$)



Topology-Hiding Broadcast ($t = 1$)

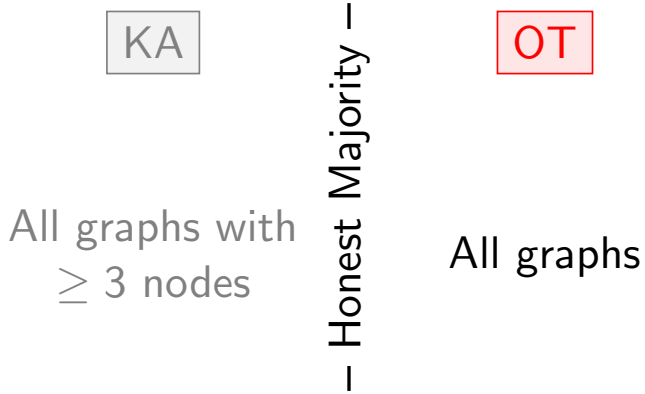


Topology-Hiding Anonymous Broadcast ($t = 1$)

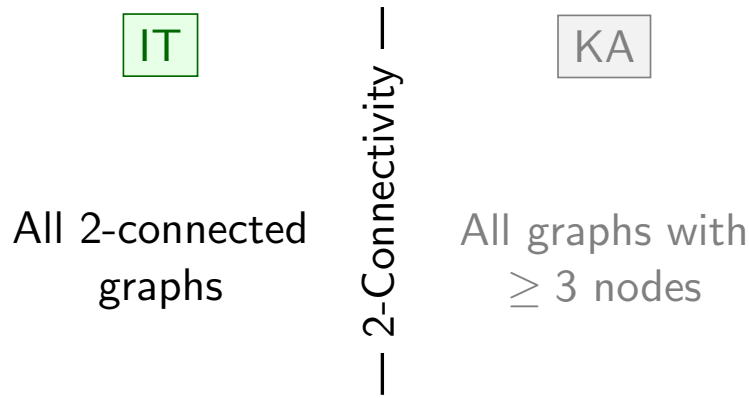


This Talk

1. 'Paths of Length Two and Three': 1-THAB requires OT



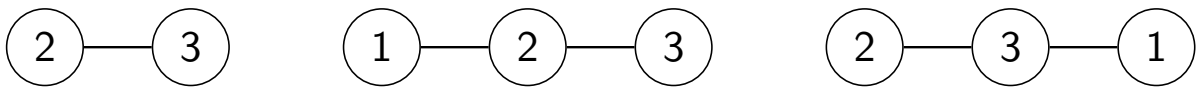
2. 'All 2-connected Graphs': 1-THAB is possible Information-Theoretically



‘Paths of Length Two and Three’: 1-THAB requires OT

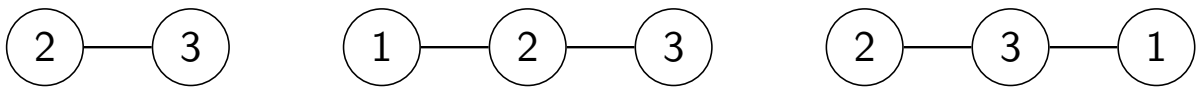
‘Paths of Length Two and Three’: 1-THAB requires OT

- *Functionality:* Anonymous Broadcast
- *Player Pool:* $\{①, ②, ③\}$
- *Graph Class:* $\mathcal{G}_{P_2\text{-}vs\text{-}P_3}$



‘Paths of Length Two and Three’: 1-THAB requires OT

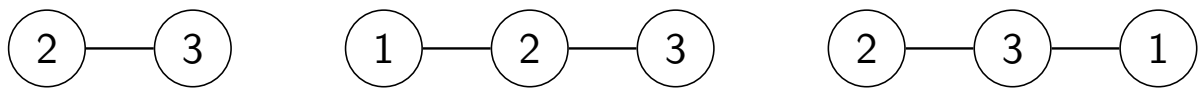
- *Functionality:* Anonymous Broadcast
- *Player Pool:* $\{①, ②, ③\}$
- *Graph Class:* $\mathcal{G}_{P_2\text{-}vs\text{-}P_3}$



$$\text{1-THAB}(\mathcal{G}_{P_2\text{-}vs\text{-}P_3}) \Rightarrow \text{OT}$$

‘Paths of Length Two and Three’: 1-THAB requires OT

- *Functionality:* Anonymous Broadcast in 2 Rounds
- *Player Pool:* $\{①, ②, ③\}$
- *Graph Class:*



[2-round 1-THAB($\mathcal{G}_{P_2\text{-}vs\text{-}P_3}$)] $\Rightarrow$ Semi-honest AND $\Rightarrow$ OT

[2-round 1-THAB($\mathcal{G}_{P_2\text{-}vs\text{-}P_3}$)] $\Rightarrow$ OT (Correctness)

Alice | Bob

If $x = 0$

If $x = 1$

If $y = 0$

If $y = 1$

$[\text{2-round 1-THAB}(\mathcal{G}_{P_2\text{-vs-}P_3})] \Rightarrow \text{OT}$ (Correctness)

Alice | Bob

$r \xleftarrow{\$} \{0,1\}^\lambda \longrightarrow$

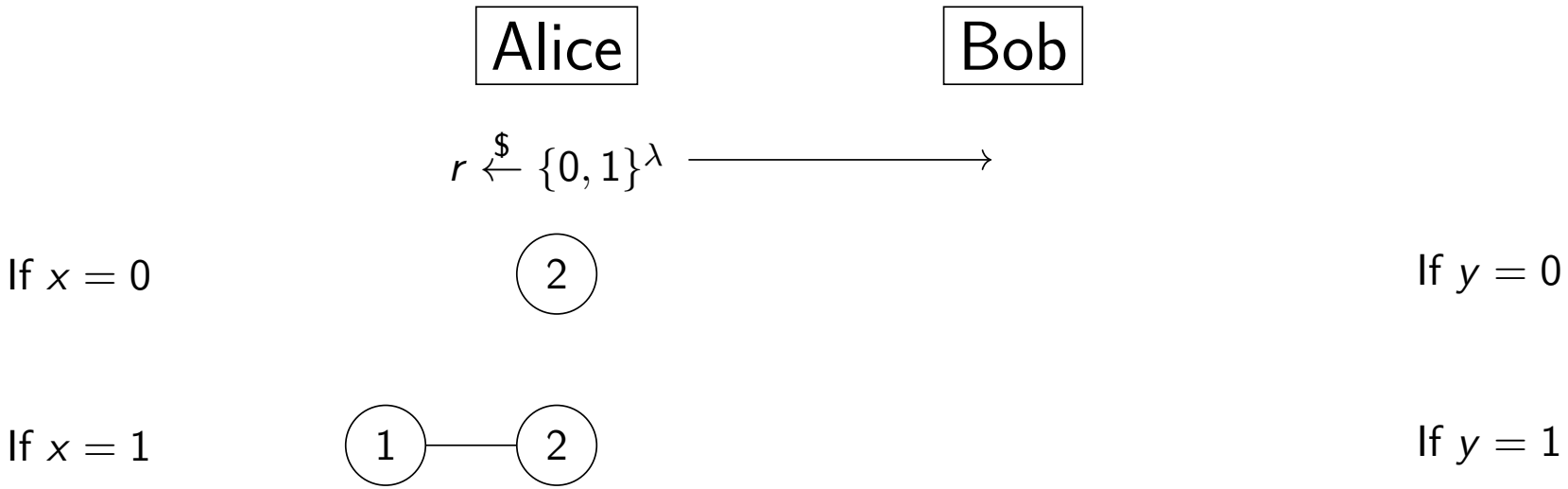
If $x = 0$

If $y = 0$

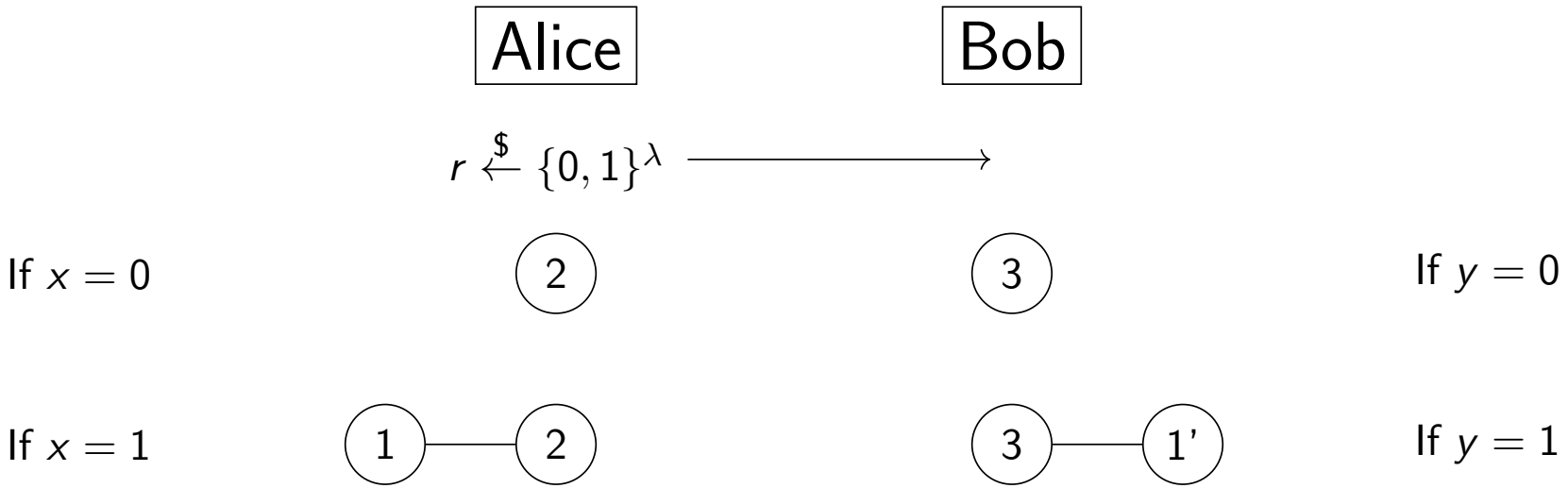
If $x = 1$

If $y = 1$

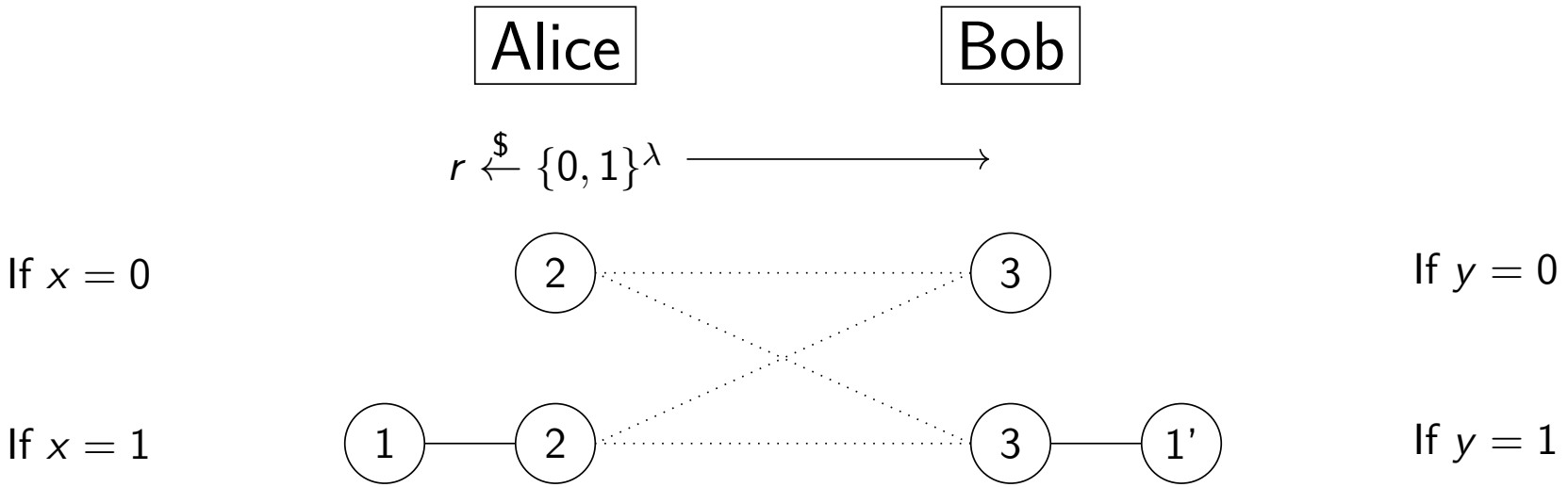
$[\text{2-round 1-THAB}(\mathcal{G}_{P_2\text{-vs-}P_3})] \Rightarrow \text{OT}$ (Correctness)



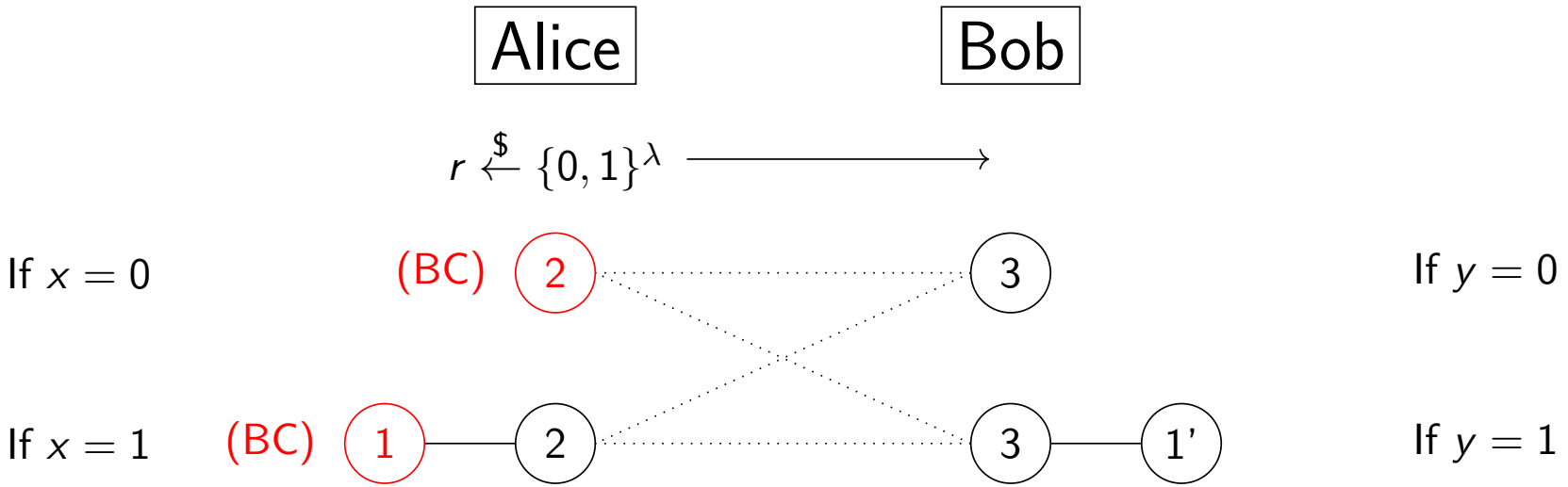
$[\text{2-round 1-THAB}(\mathcal{G}_{P_2\text{-vs-}P_3})] \Rightarrow \text{OT}$ (Correctness)



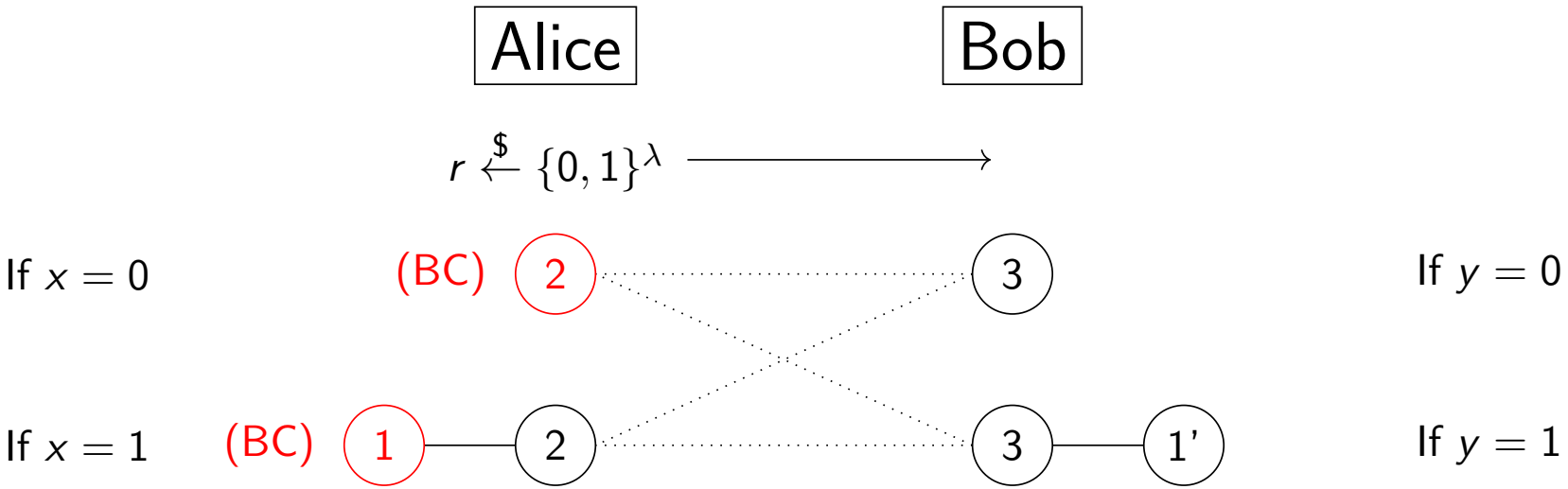
[2-round 1-THAB($\mathcal{G}_{P_2\text{-vs-}P_3}$)] $\Rightarrow$ OT (Correctness)



[2-round 1-THAB($\mathcal{G}_{P_2\text{-vs-}P_3}$)] $\Rightarrow$ OT (Correctness)



$[\text{2-round 1-THAB}(\mathcal{G}_{P_2\text{-vs-}P_3})] \Rightarrow \text{OT}$ (Correctness)



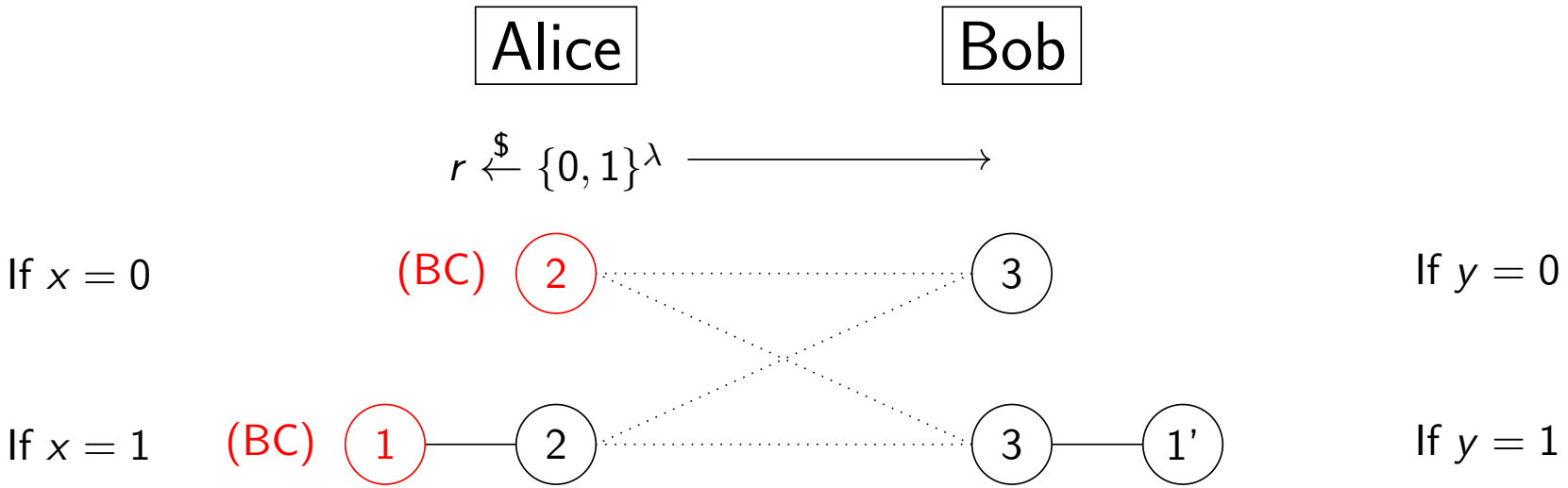
If $(x, y) = (0, 0)$:

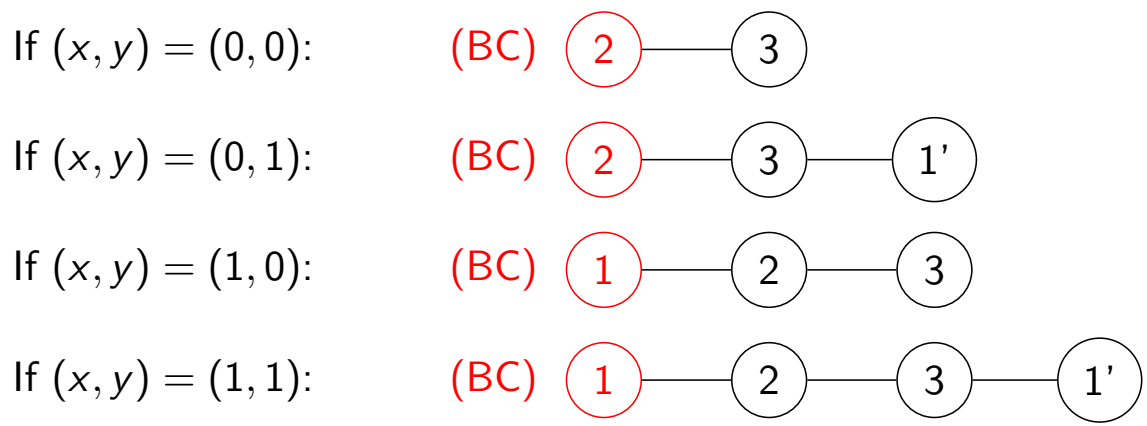
If $(x, y) = (0, 1)$:

If $(x, y) = (1, 0)$:

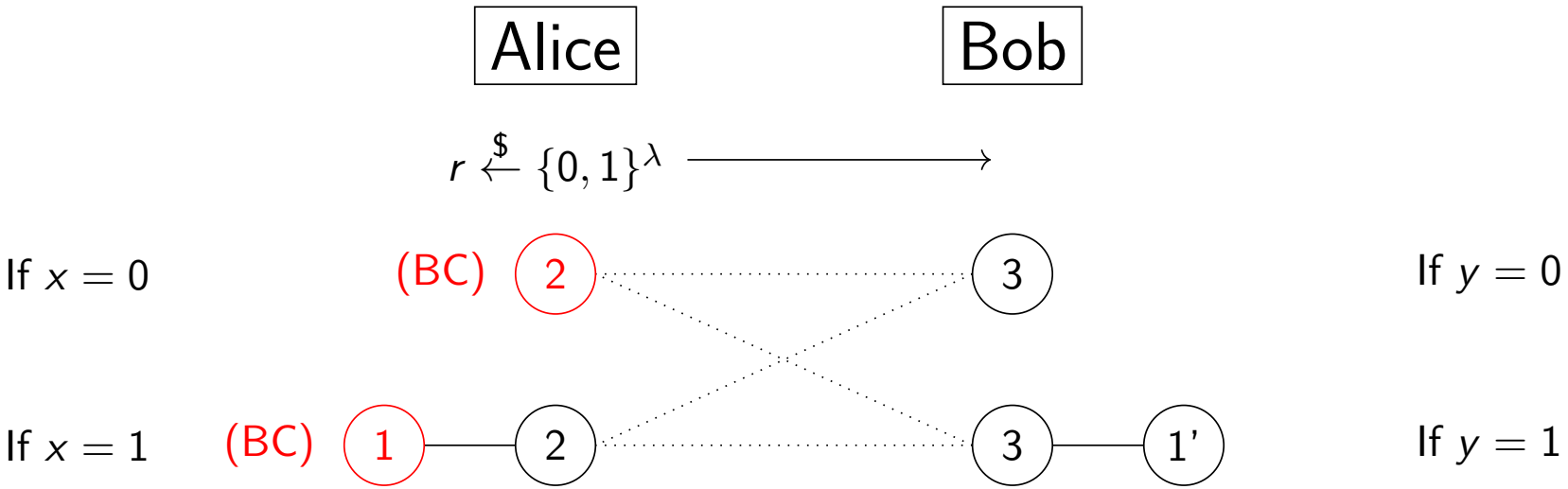
If $(x, y) = (1, 1)$:

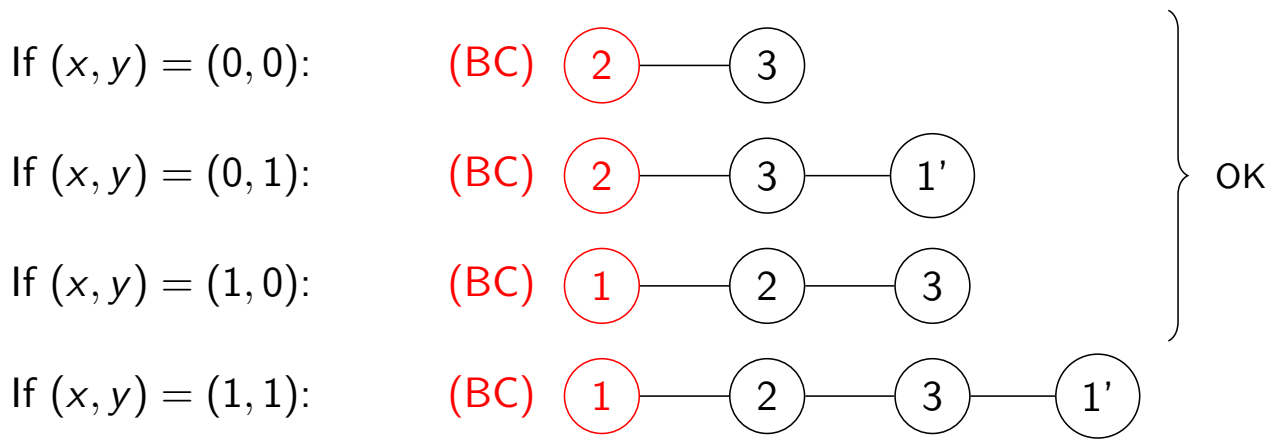
$[\text{2-round 1-THAB}(\mathcal{G}_{P_2\text{-vs-}P_3})] \Rightarrow \text{OT}$ (Correctness)



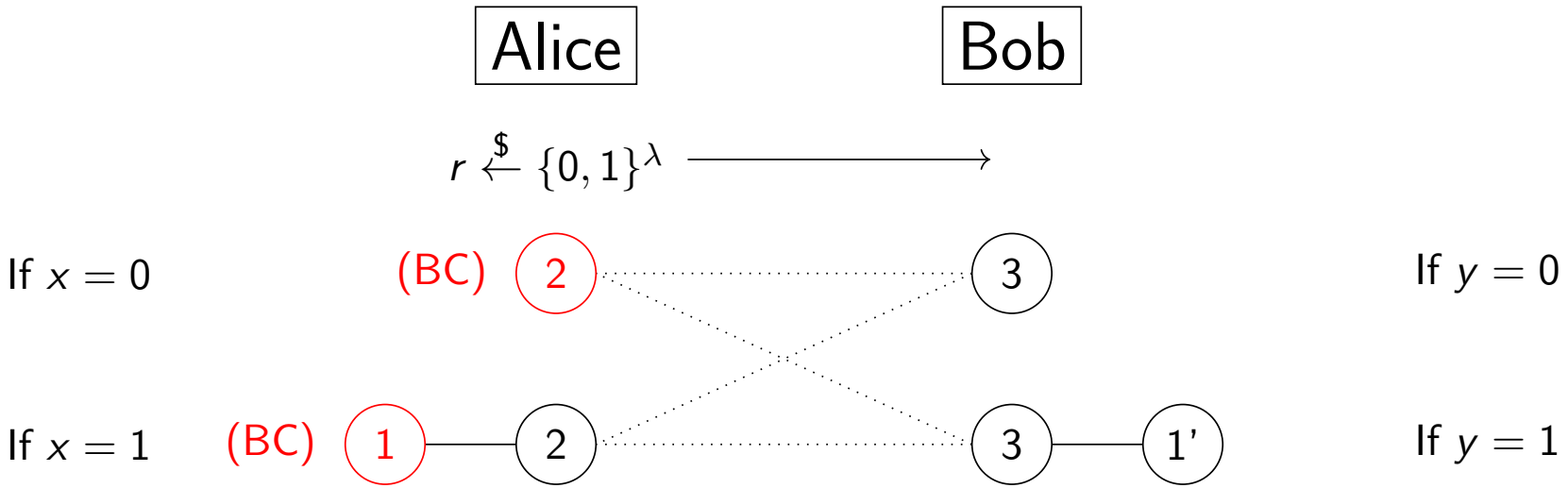


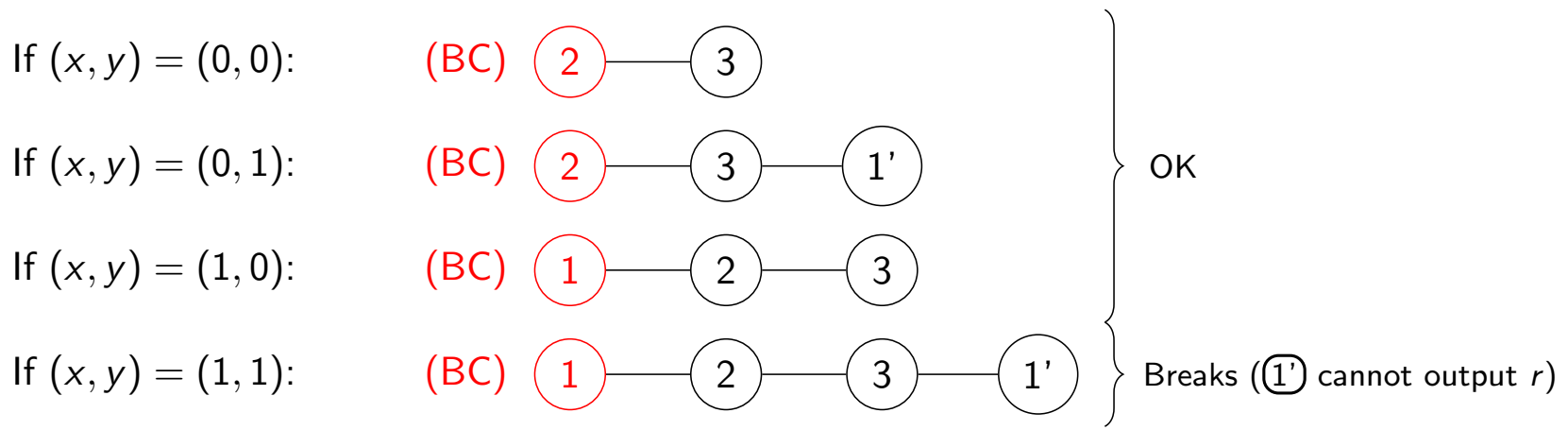
$[\text{2-round 1-THAB}(\mathcal{G}_{P_2\text{-vs-}P_3})] \Rightarrow \text{OT}$ (Correctness)





$[\text{2-round 1-THAB}(\mathcal{G}_{P_2\text{-vs-}P_3})] \Rightarrow \text{OT}$ (Correctness)





[2-round 1-THAB($\mathcal{G}_{P_2\text{-vs-}P_3}$)] $\Rightarrow$ OT (Security)

Alice

Bob

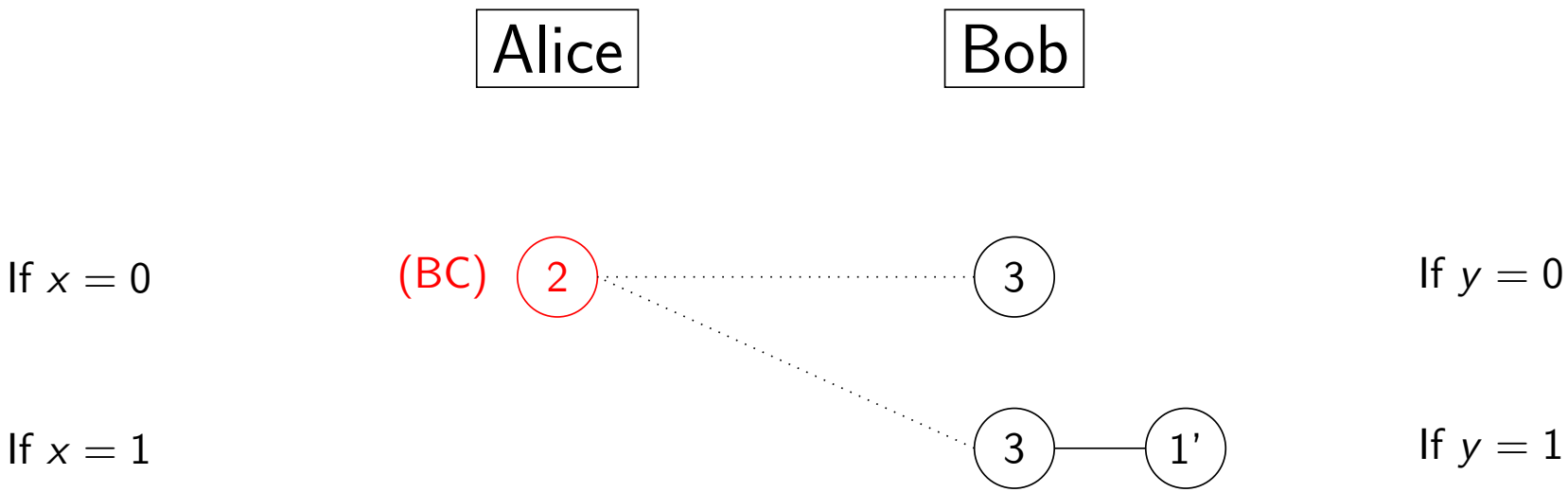
If $x = 0$

If $y = 0$

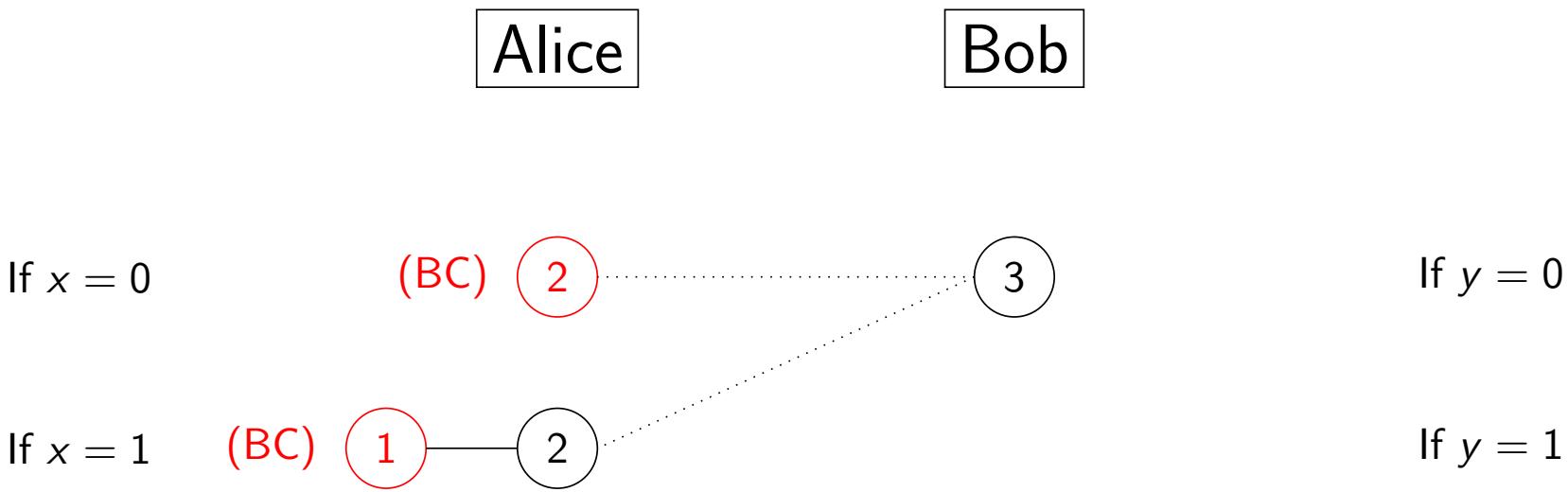
If $x = 1$

If $y = 1$

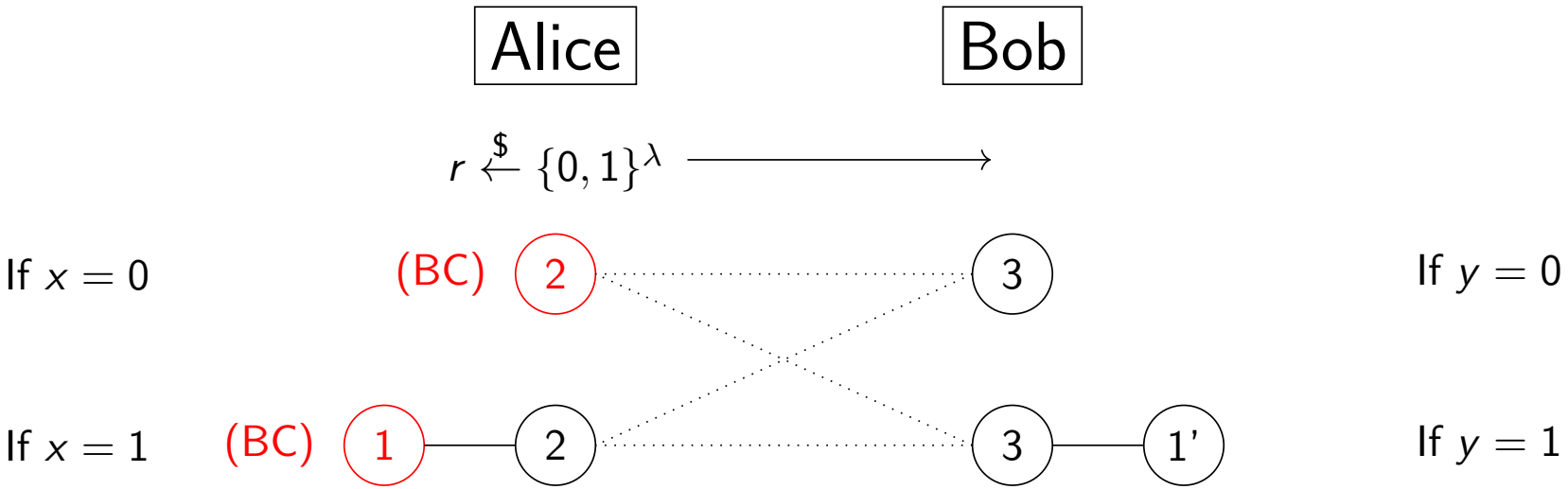
[2-round 1-THAB($\mathcal{G}_{P_2\text{-}vs\text{-}P_3}$)] $\Rightarrow$ OT (Security)

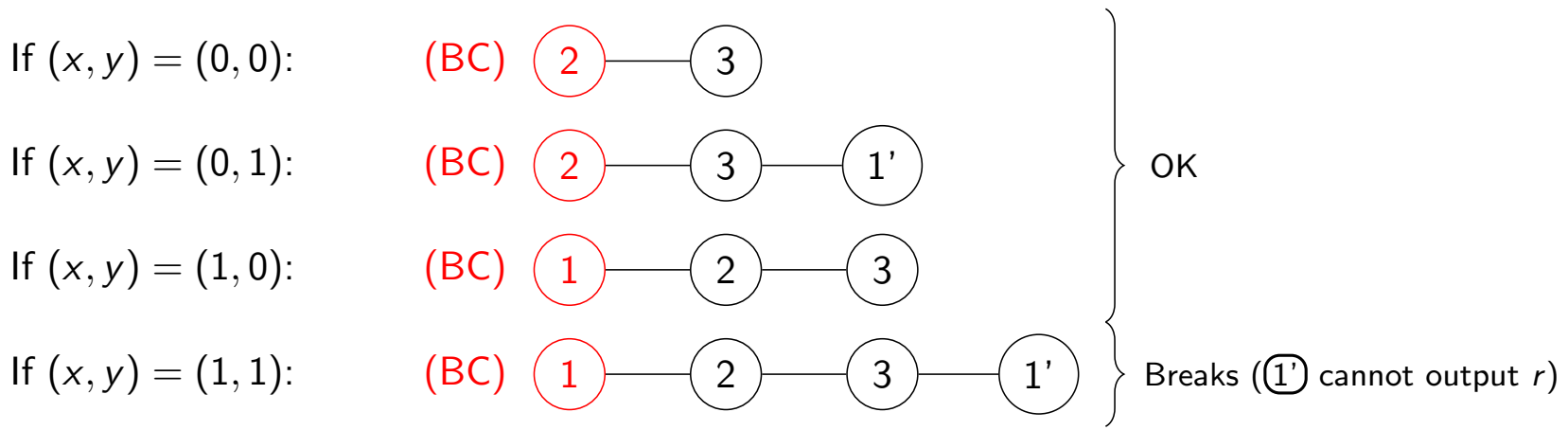


[2-round 1-THAB($\mathcal{G}_{P_2\text{-vs-}P_3}$)] $\Rightarrow$ OT (Security)



1-THAB($\mathcal{G}_{P_2\text{-vs-}P_3}$) $\Rightarrow$ OT





‘All 2-connected Graphs’: 1-THAB is possible Information-Theoretically

‘All 2-connected Graphs’: 1-THAB is possible IT

- *Functionality:* Anonymous Broadcast
- *Player Pool:* $\left\{\boxed{P_1}, \ldots, \boxed{P_N}\right\}$
- *Graph Class:* All two-connected graphs

1-THAB($\mathcal{G}_{2\text{-}conn}$) is possible

- *Functionality:* Anonymous Broadcast
- *Player Pool:* $\{\boxed{P_1}, \ldots, \boxed{P_N}\}$
- *Graph Class:* All two-connected graphs with all the players

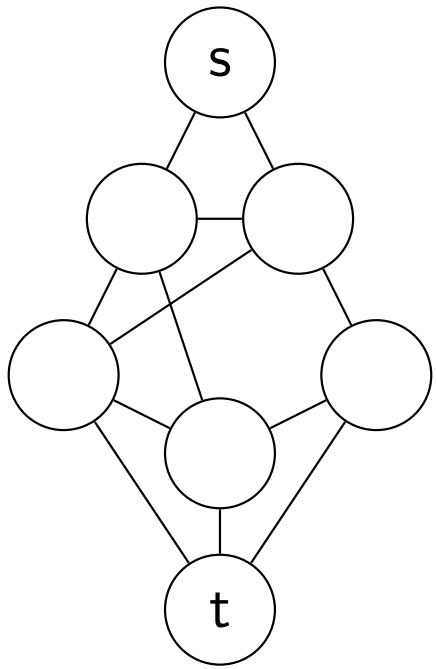
1-THAB($\mathcal{G}_{2\text{-}conn}$) is possible Unconditionally

1-THAB($\mathcal{G}_{2\text{-}conn}$) is possible

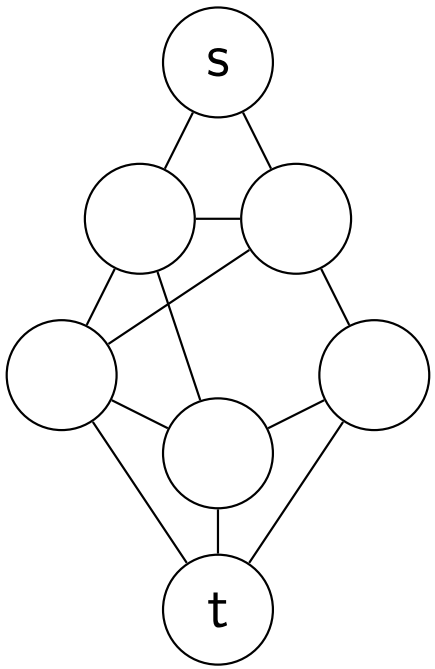
- *Functionality:* Secure Message Transmission from Ⓢ to Ⓣ
- *Player Pool:* $\left\{\boxed{P_1}, \ldots, \boxed{P_N}\right\}$
- *Graph Class:* All two-connected graphs with all the players

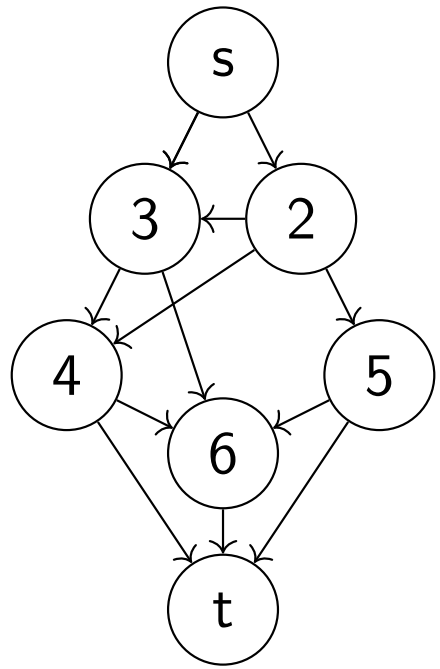
1-SMT$_{s \to t}(\mathcal{G}_{P_2\text{-}vs\text{-}P_3})$ is possible Unconditionally

1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible



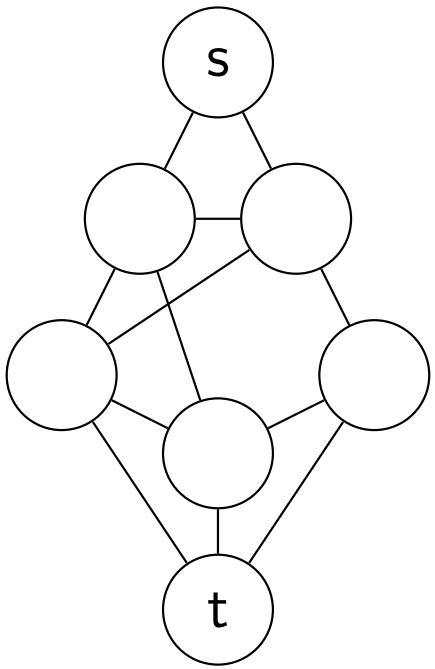
1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible

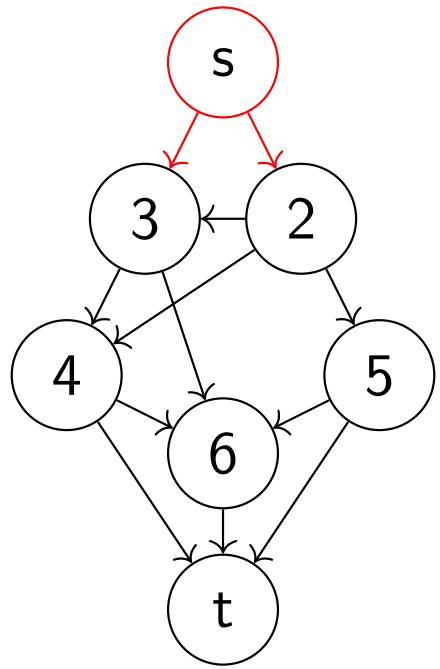




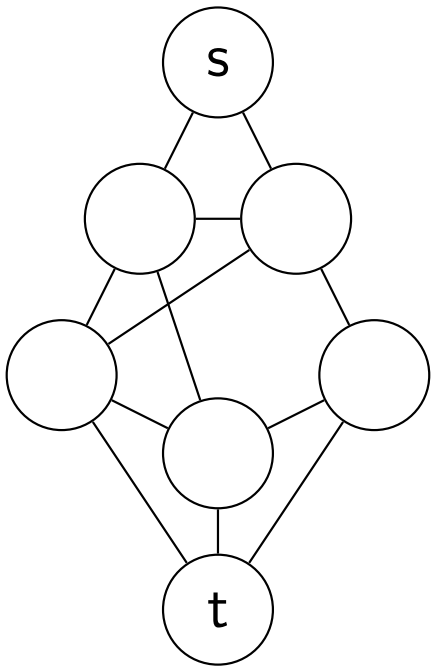
bipolar orientation from s to t:
orientation as D.A.G. with single source s and single sink t

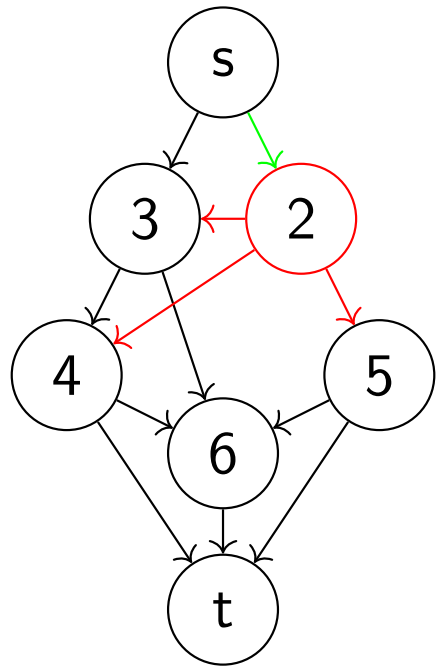
1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible



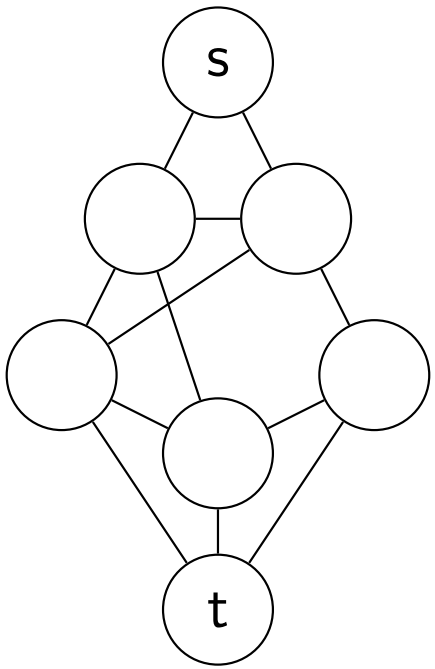


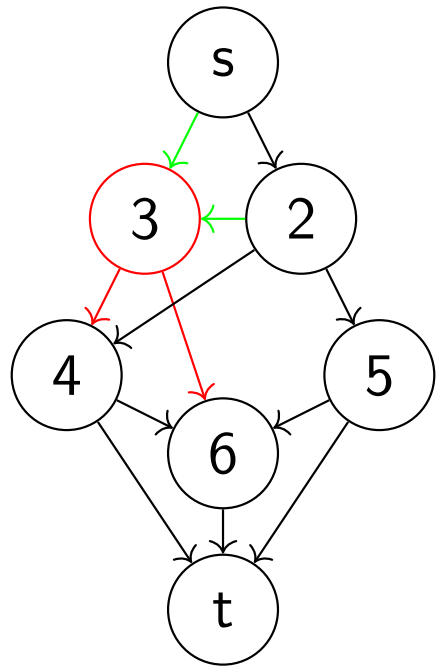
1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible



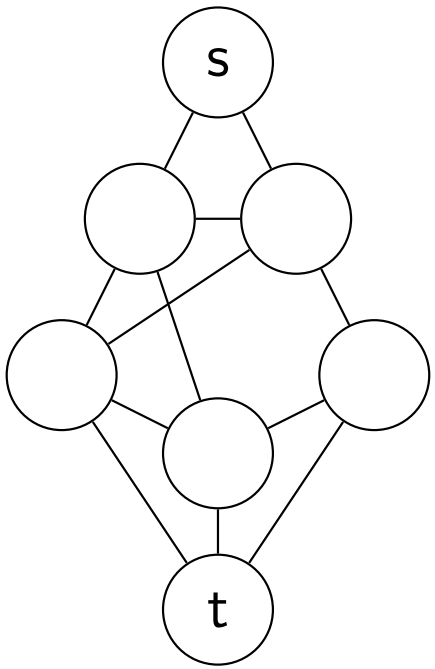


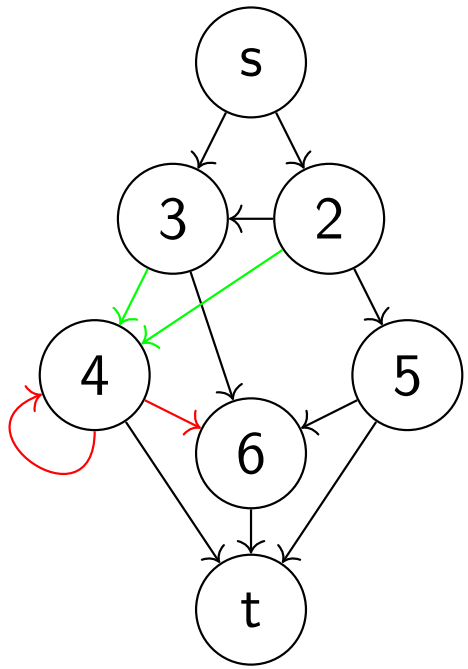
1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible



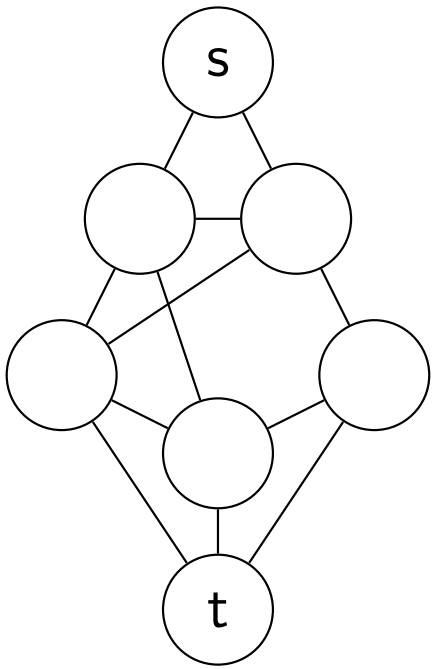


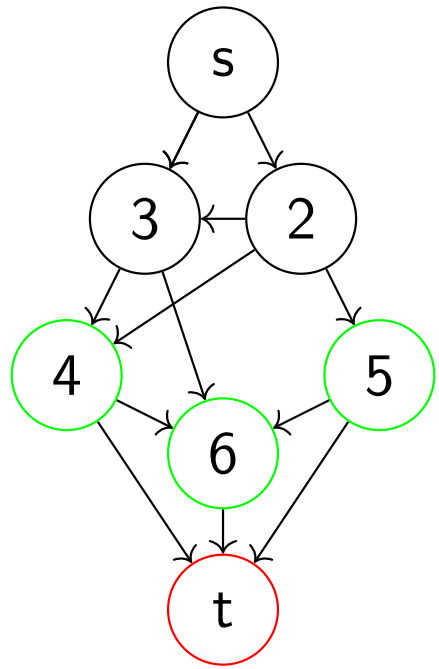
1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible





1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible





1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible

Public:

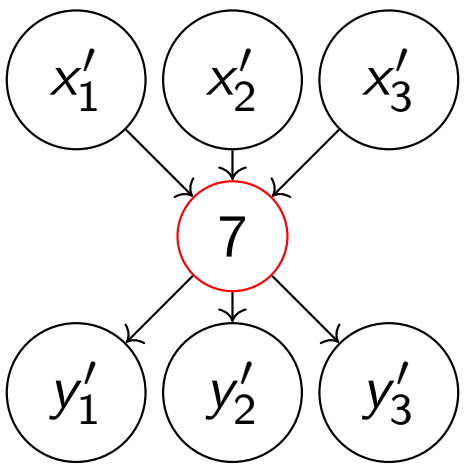
- $\mathcal{G} = \{G_1, G_2, \ldots, G_k\}$ on $V = [N]$
- st-orientations $s \to t$: $H_1, H_2, \ldots H_k$

1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible

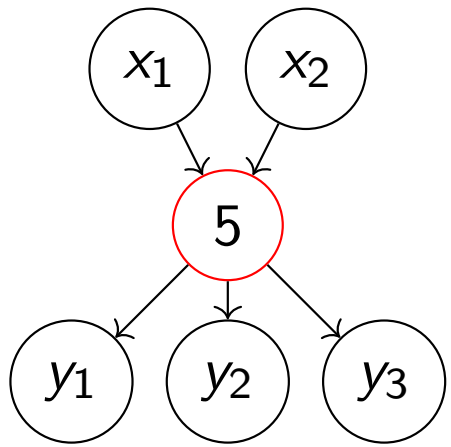
Public:

- $\mathcal{G} = \{G_1, G_2, \ldots, G_k\}$ on $V = [N]$
- st-orientations $s \to t$: $H_1, H_2, \ldots H_k$

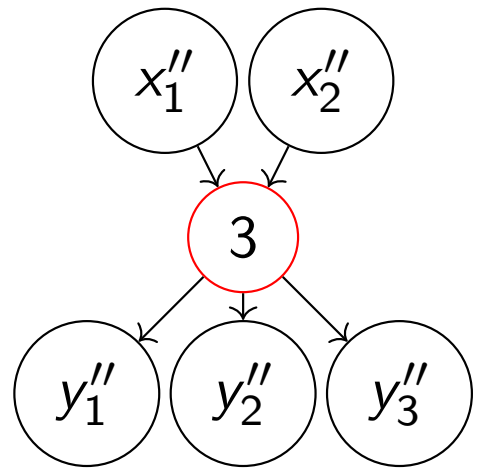
$(H_{i'})$



(H_i)



$(H_{i''})$

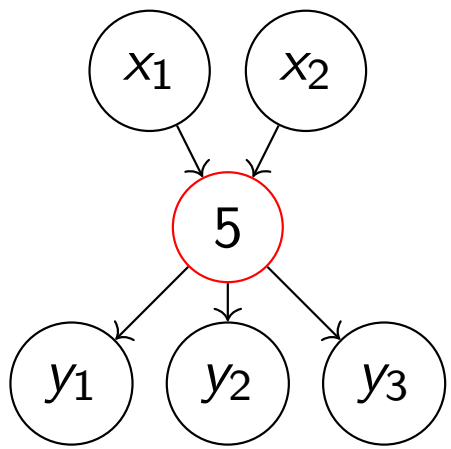


1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible

Public:

- $\mathcal{G} = \{G_1, G_2, \ldots, G_k\}$ on $V = [N]$
- st-orientations $s \to t : H_1, H_2, \ldots H_k$

(H_i)



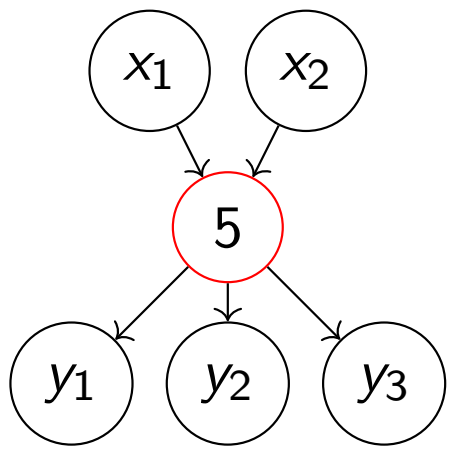
1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible

Public:

- $\mathcal{G} = \{G_1, G_2, \ldots, G_k\}$ on $V = [N]$
- st-orientations $s \to t$: $H_1, H_2, \ldots H_k$

If $N_G = N_{G_i}$

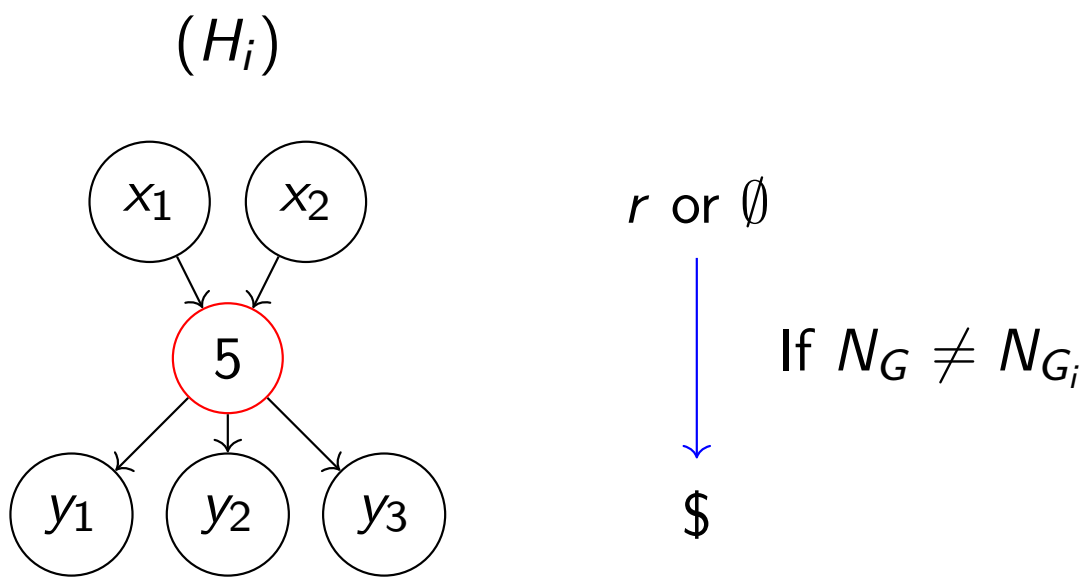
(H_i)



1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible

Public:

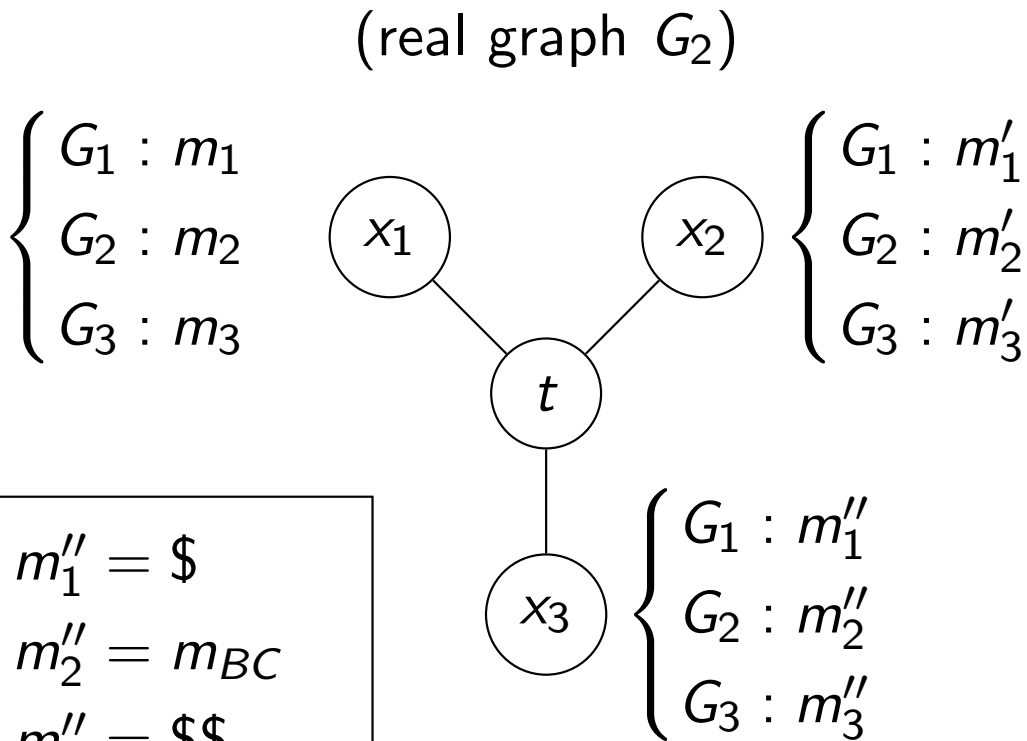
- $\mathcal{G} = \{G_1, G_2, \ldots, G_k\}$ on $V = [N]$
- st-orientations $s \to t$: $H_1, H_2, \ldots H_k$



1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible

Public:

- $\mathcal{G} = \{G_1, G_2, \ldots, G_k\}$
- st-orientations $s \to t : H_1, H_2, \ldots H_k$

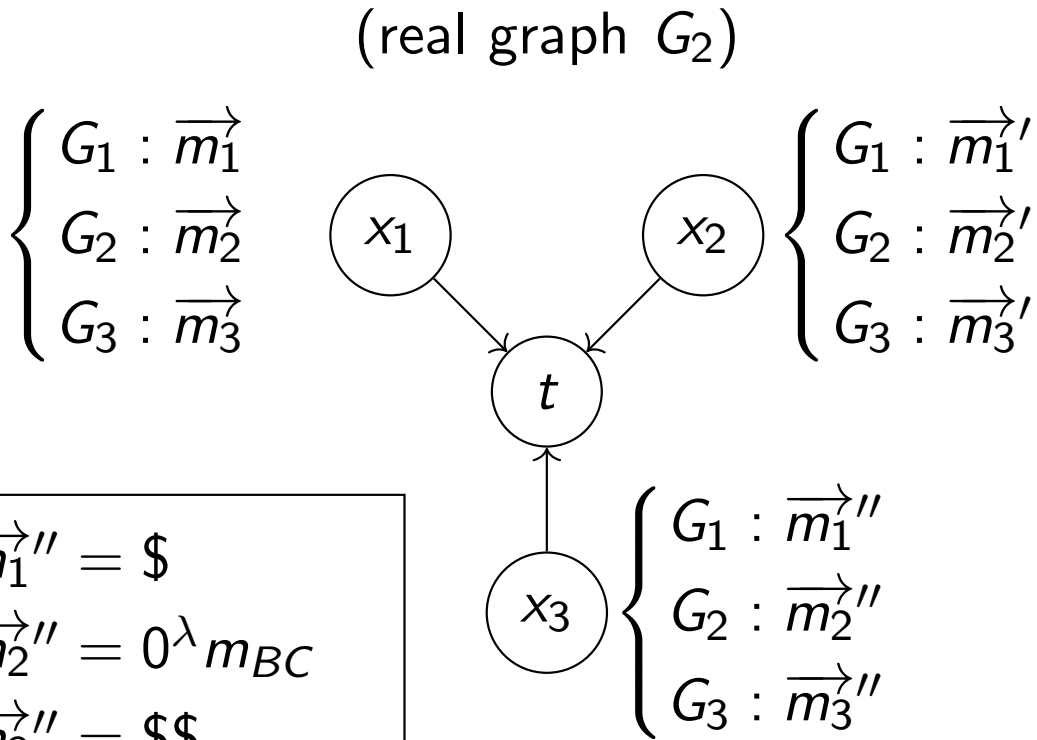


$$\begin{cases} m_1 + m'_1 + m''_1 = \$ \\ m_2 + m'_2 + m''_2 = m_{BC} \\ m_3 + m'_3 + m''_3 = \$\$ \end{cases}$$

1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible

Public:

- $\mathcal{G} = \{G_1, G_2, \ldots, G_k\}$
- st-orientations $s \to t$: $H_1, H_2, \ldots H_k$



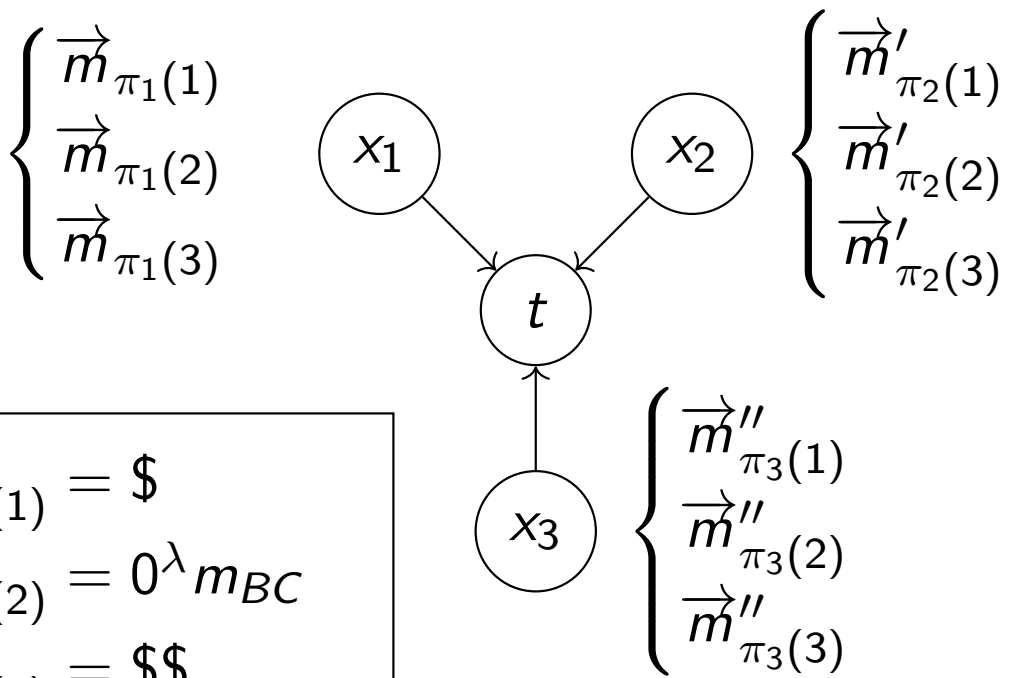
$$\begin{cases} \overrightarrow{m_1} + \overrightarrow{m_1}' + \overrightarrow{m_1}'' = \$ \\ \overrightarrow{m_2} + \overrightarrow{m_2}' + \overrightarrow{m_2}'' = 0^{\lambda} m_{BC} \\ \overrightarrow{m_3} + \overrightarrow{m_3}' + \overrightarrow{m_3}'' = \$\$ \end{cases}$$

1-SMT$_{s\to t}(\mathcal{G}_{2\text{-}conn})$ is possible

Public:

- $\mathcal{G} = \{G_1, G_2, \ldots, G_k\}$
- st-orientations $s \to t$: $H_1, H_2, \ldots H_k$

(real graph G_2)



$$\begin{cases} \overrightarrow{m}_{\pi_1(1)} + \overrightarrow{m}'_{\pi_2(1)} + \overrightarrow{m}''_{\pi_3(1)} = \$ \\ \overrightarrow{m}_{\pi_1(2)} + \overrightarrow{m}'_{\pi_2(2)} + \overrightarrow{m}''_{\pi_3(2)} = 0^{\lambda} m_{BC} \\ \overrightarrow{m}_{\pi_1(3)} + \overrightarrow{m}'_{\pi_2(3)} + \overrightarrow{m}''_{\pi_3(3)} = \$\$ \end{cases}$$

Our Results (Extended)

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

IT	KA	OT
All 2-connected graphs + 2-paths	All graphs with ≥ 3 nodes	All graphs

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

IT	KA	OT
Only 2-connected graphs + 2-paths	Only graphs with ≥ 3 nodes	Contains paths of length 2 and 3

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

IT	KA	???	OT
Only 2-connected graphs + 2-paths	Only graphs with ≥ 3 nodes	Contains a path of length 2 and a graph with ≥ 3 nodes not 2-connected	Contains paths of length 2 and 3

Thank You!