Is Information-Theoretic Topology-Hiding Computation Possible?

Marshall Ball — Columbia University

Elette Boyle — IDC Herzliya

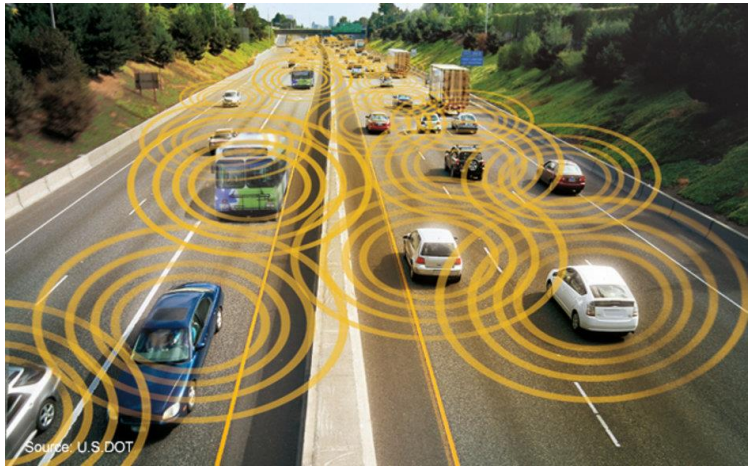
Ran Cohen — Northeastern University

Tal Malkin — Columbia University

Tal Moran — IDC Herzliya

MPC over incomplete graphs

- Each party talks only to its neighbors
- Standard MPC reveals topology
- This can be sensitive information
- Can MPC hide our neighbors?

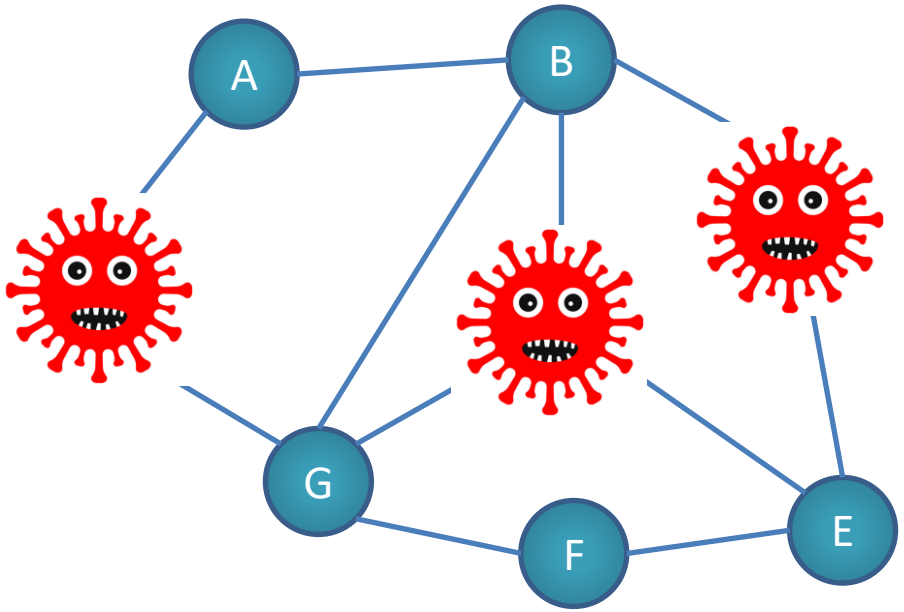


Topology-Hiding Computation (THC)

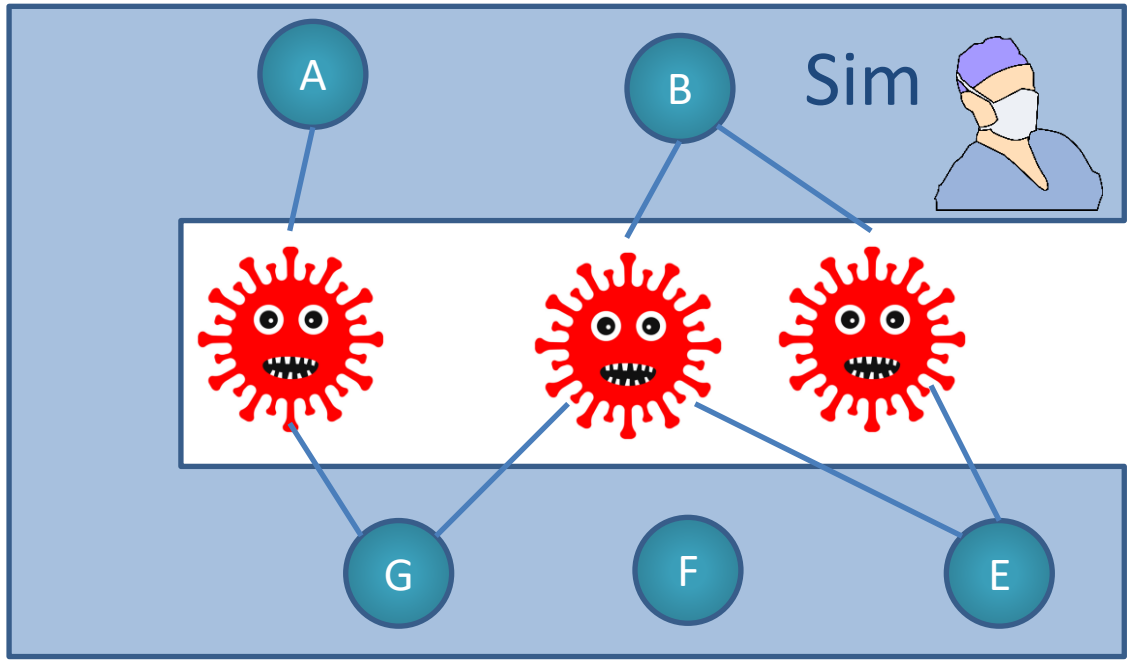
- Consider a class of graphs $\mathcal{G}$
- Run a protocol over communication graph $G \in \mathcal{G}$
- Adv shouldn't learn more than corrupted parties' neighbors, inputs, outputs
- Can compute functions of the graph (# triangles, avg degree, etc.)

This talk: semi-honest adv

REAL



IDEAL

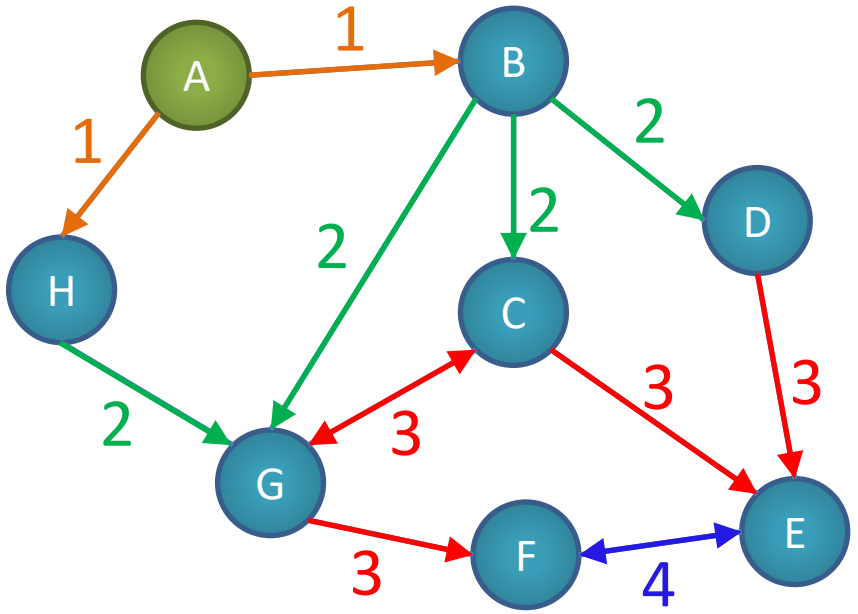


Simple THC Recipe

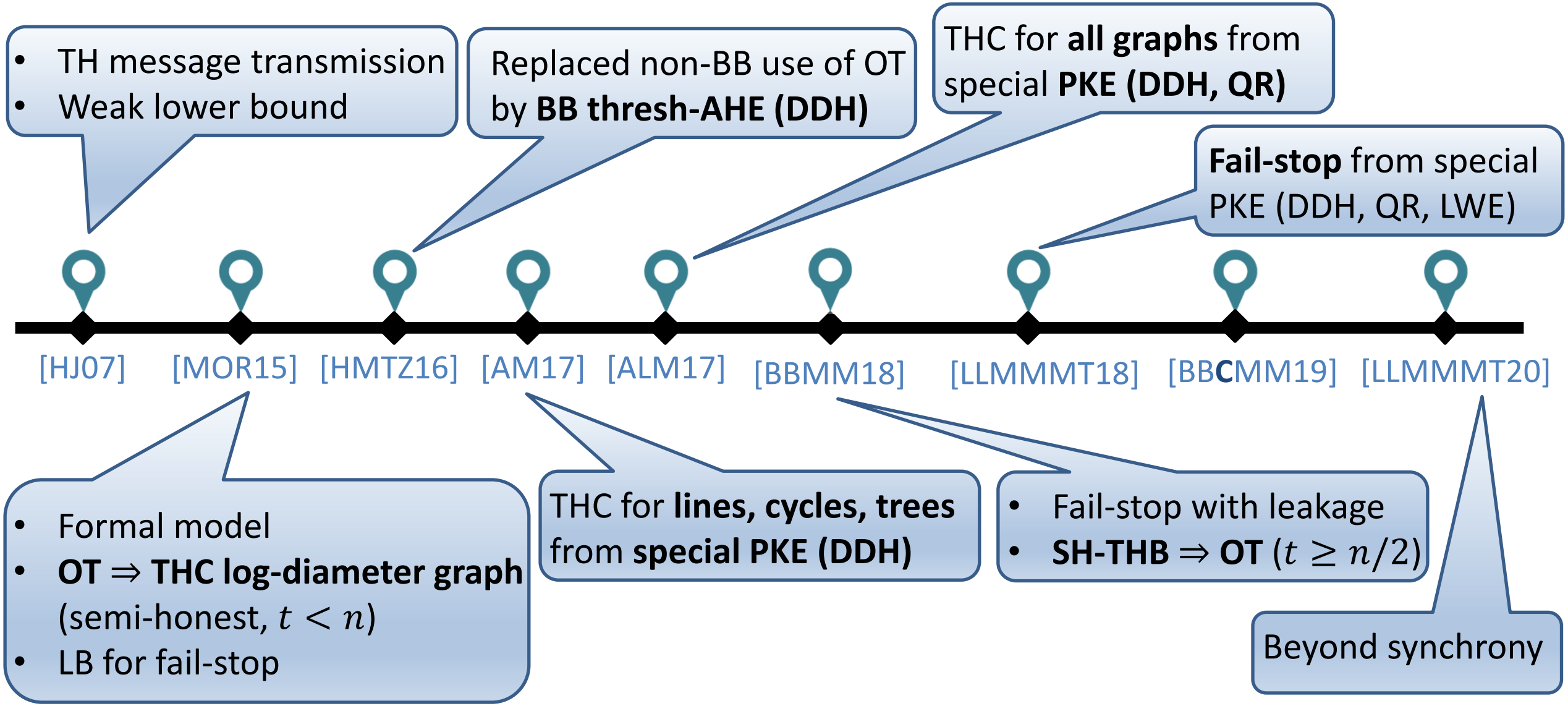
Topology-hiding broadcast (THB)

Crypto tools

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

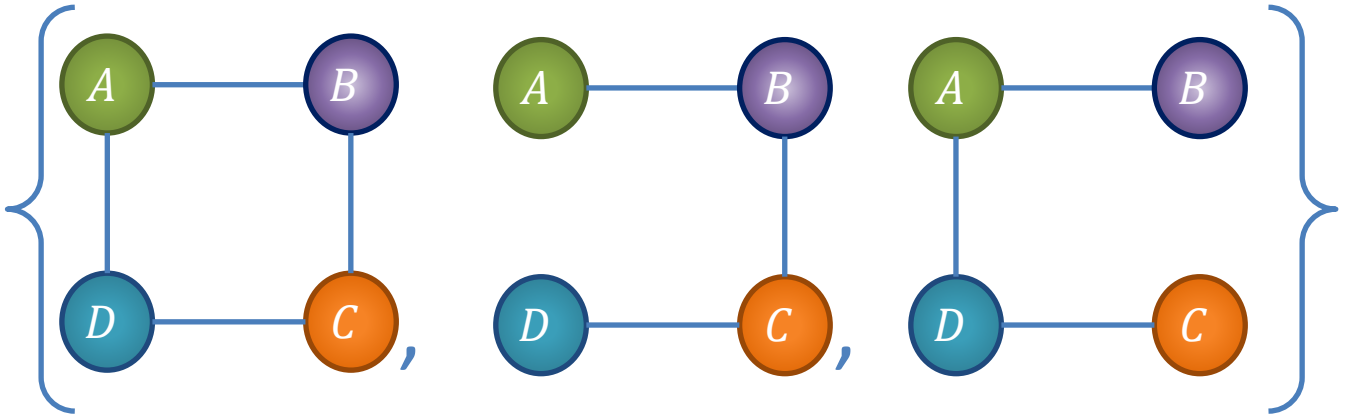


Ancient & Modern History



THB $\Longrightarrow$ OT (for $t = n/2$) [BBMM18]

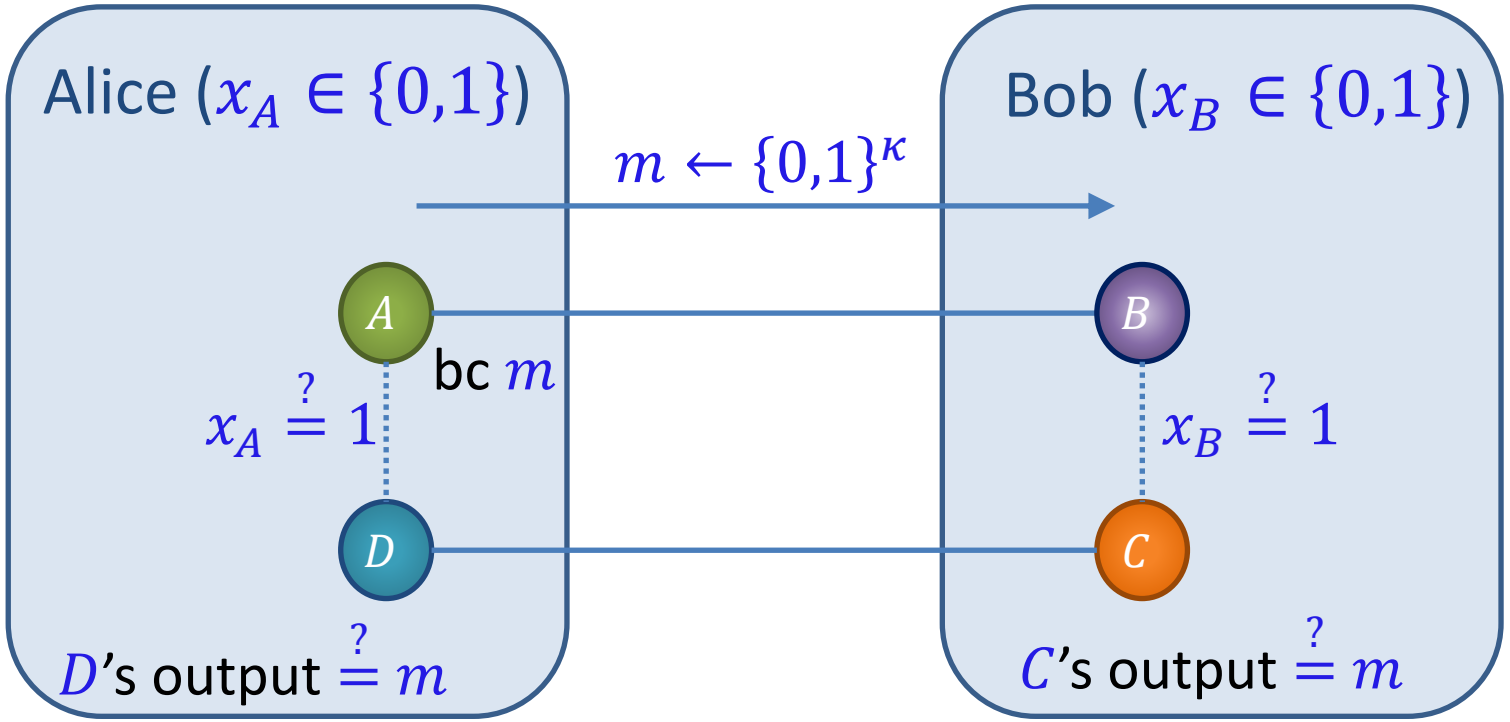
Assume a 2-secure 4-party THB for



Construct a 2PC for OR

Analysis:

- If $x_A \vee x_B = 1$
  security reduces to THB
- If $x_A \vee x_B = 0$
  C,D output m wp $2^{-\kappa}$



Main Question

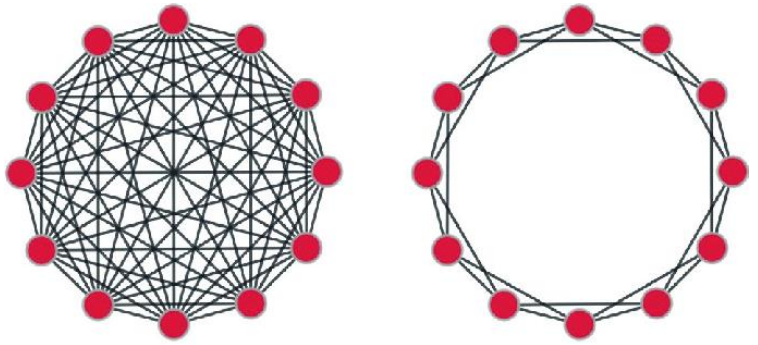
- All THC protocols use crypto and tolerate $t < n$ corruptions
- Can we "replace" **crypto** assumptions by **honest-majority** assumptions?

Can we get info-theoretic THC?

It depends

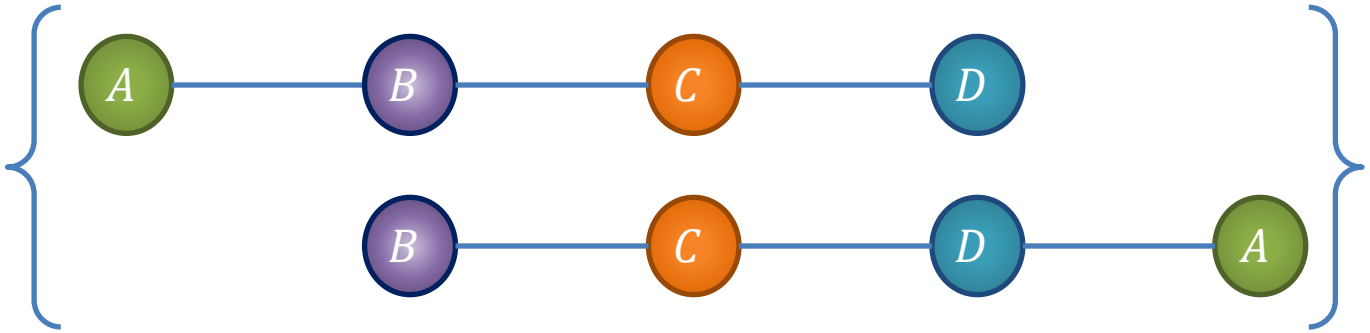
- On which classes of graphs
- On how the graph is chosen

Part I
Which classes of graphs

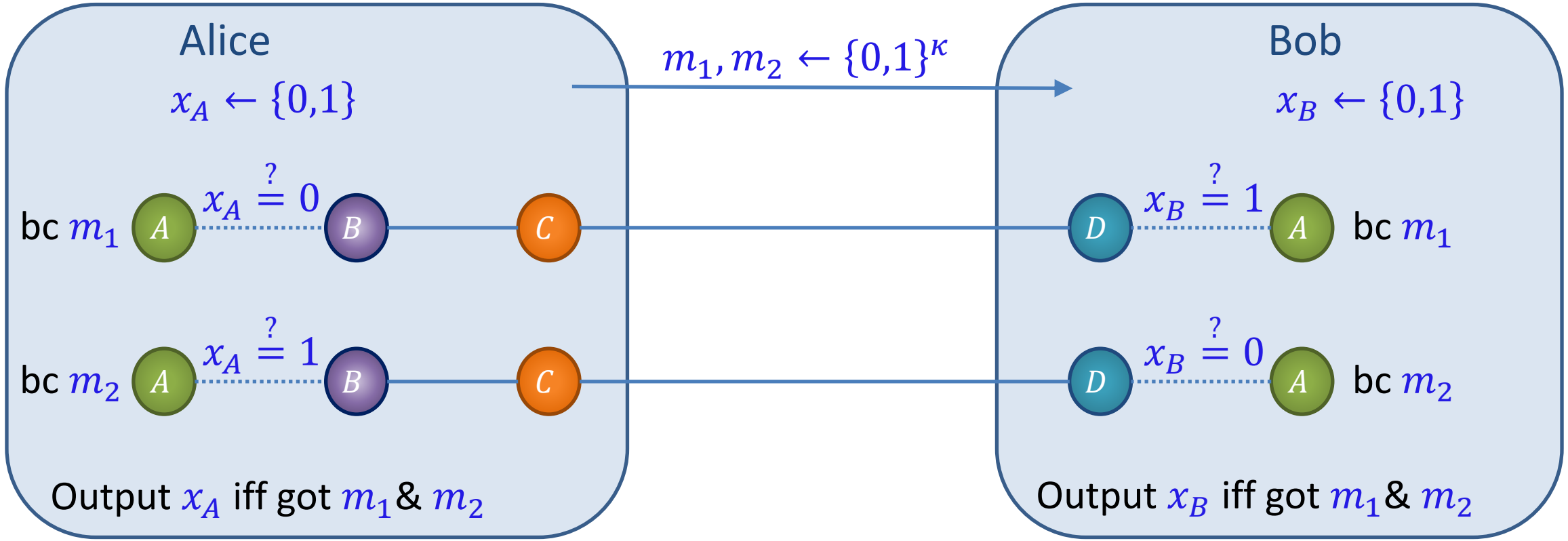


Thm 1: 1-secure THB on 4-line $\Longrightarrow$ KA

Assume a 1-secure 4-party THB for

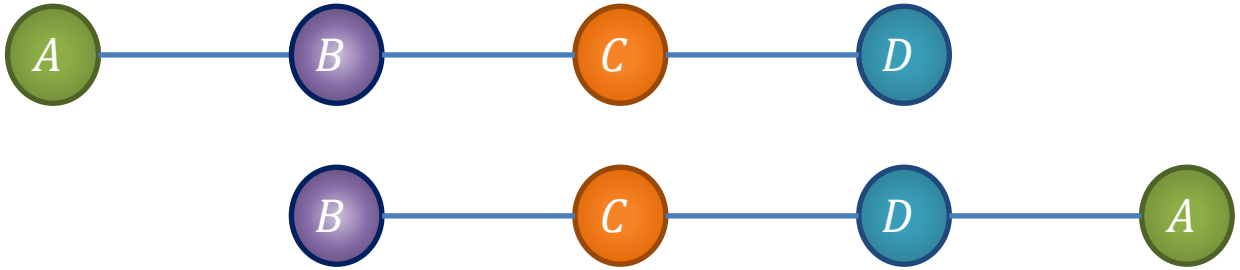


Construct KA



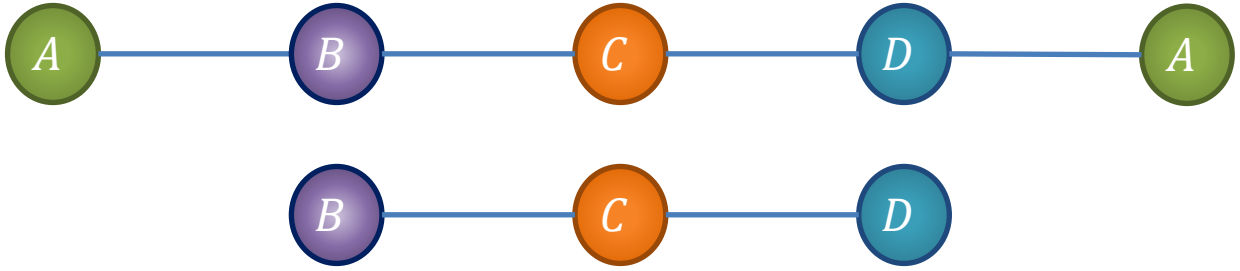
Thm 1: 1-secure THB on 4-line $\Longrightarrow$ KA

If $x_A = x_B$ then THB runs are

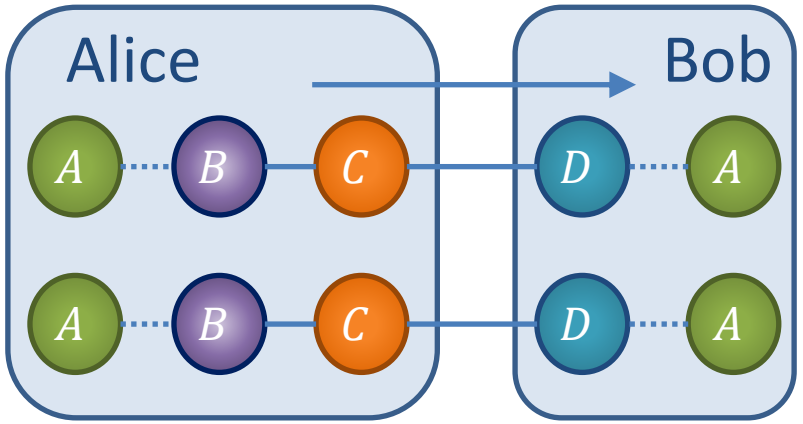


Attack on KA $\Rightarrow$ Attack on THB

If $x_A \neq x_B$ then THB runs are



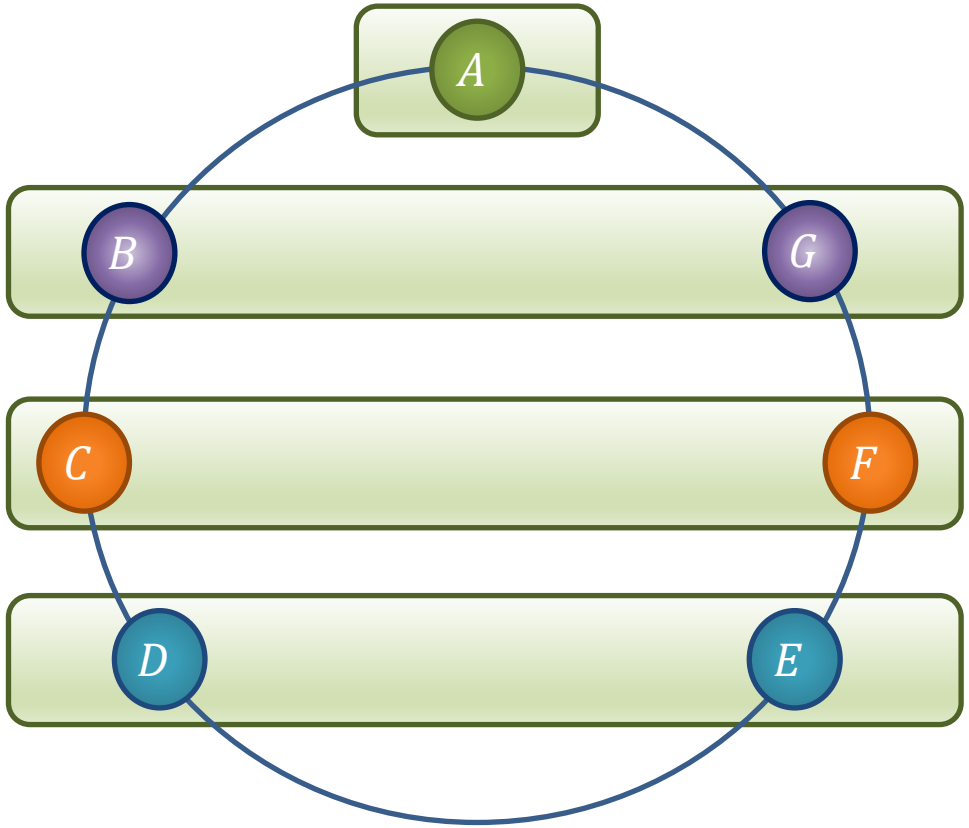
Output is m_1, m_2 wp $2^{-\kappa}$

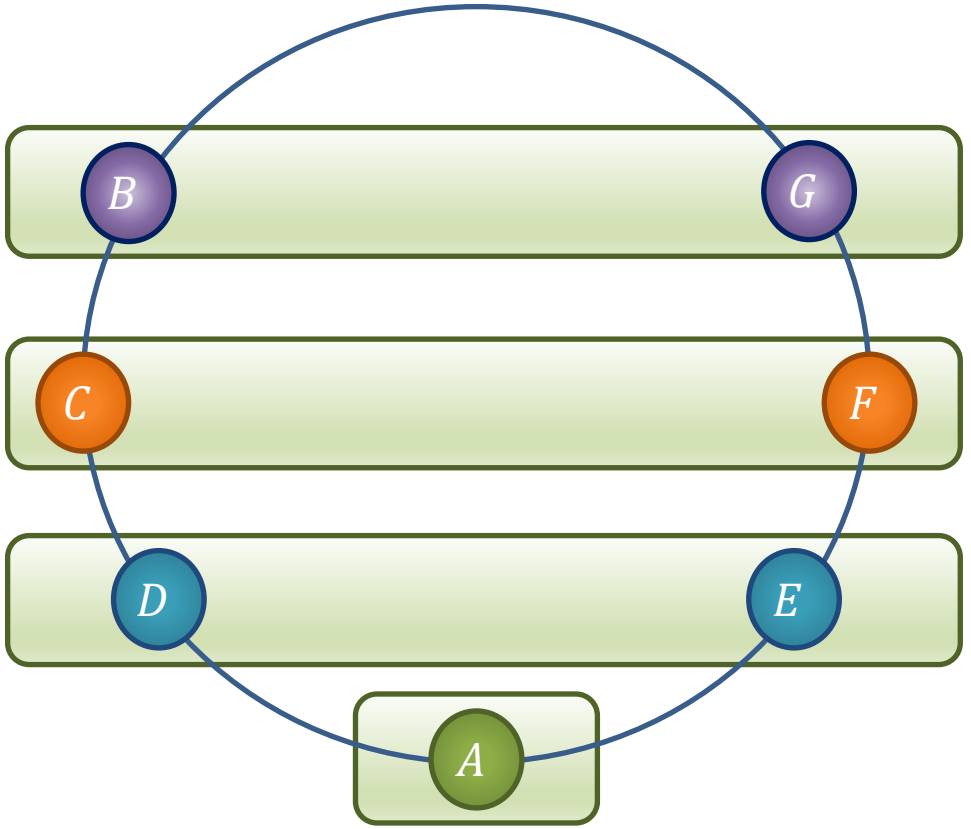


Corollary

No info-theoretic THB if graph can be **partitioned** to 4 subsets on a line

Example: 2-secure THB on 7-cycle $\Longrightarrow$ KA





What about cycles with 1 corruption?

Thm 2: 1-secure perfect THC on cycles

1) Establish secure and "anonymous" pairwise communication on the cycle

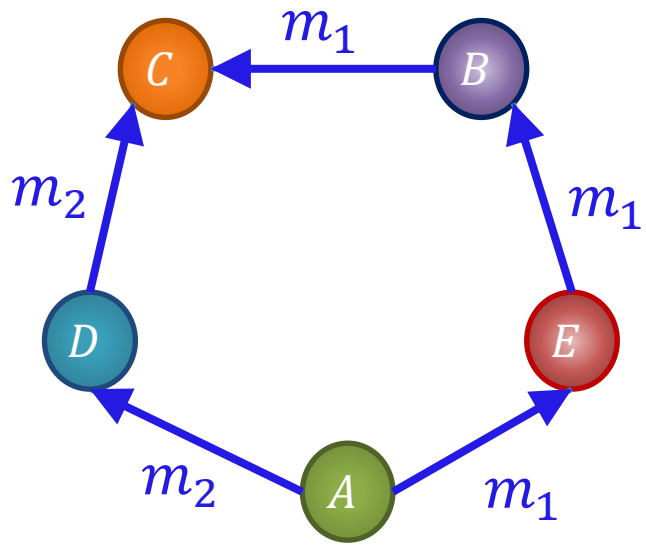
   Can send a message i hops to its left (receiver knows i hops to its right)

2) BGW ⇒ perfect THC for symmetric functions

$$f(x_1, \dots, x_n) = f\left(x_{\pi(1)}, \dots, x_{\pi(n)}\right)$$

   (doesn't capture $f(x_1, x_2, x_3) = (x_1 + x_2) \cdot x_3$)

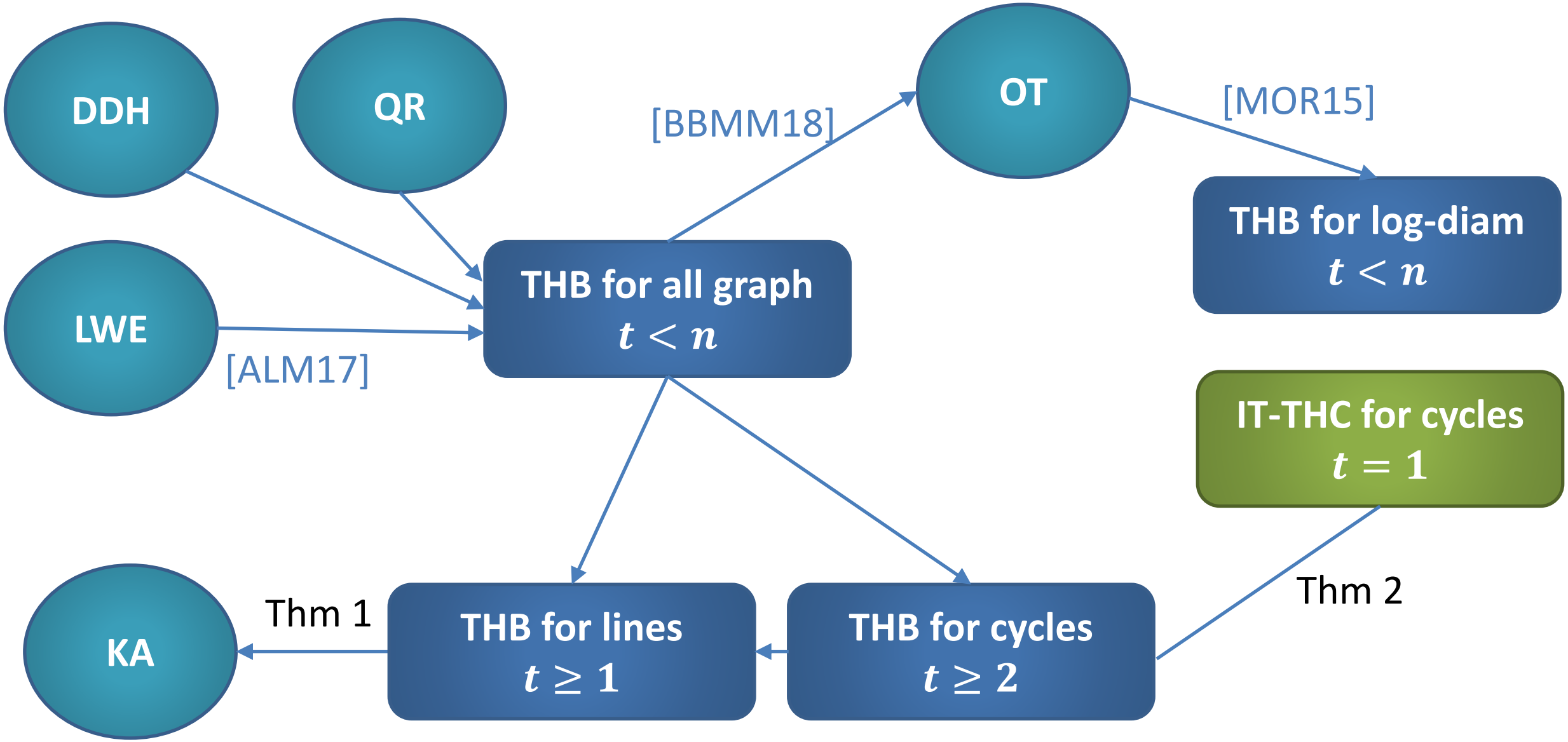
3) Compute $\tilde{f}\left((1, x_1), \dots, (n, x_n)\right) = f(x_1, \dots, x_n)$



Proof of (1) by example:

- A sends 2 hops to its left (to B/C) message m
- Share $m = m_1 \oplus m_2$
- Run a 3-round protocol

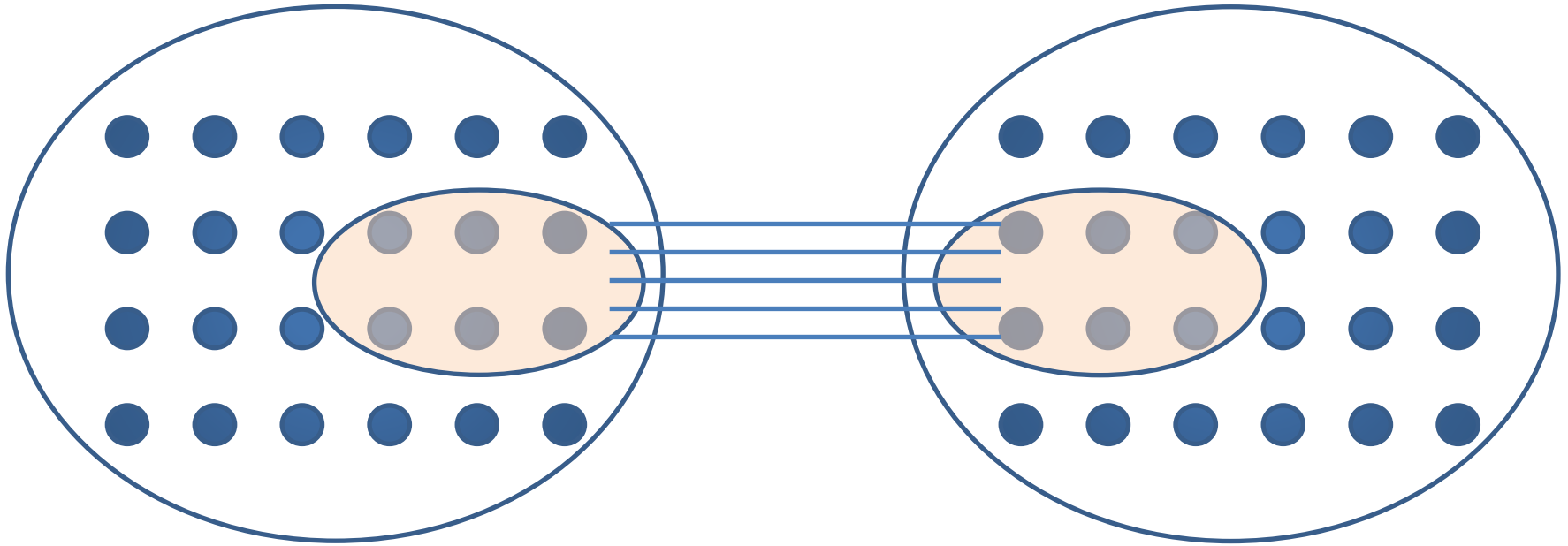
The Landscape



Part II
How the graph is chosen

Motivation: hiding partial information

- Adaptively secure MPC with sublinear cuts [B**C**DH18]
- Intuitively, this hides ***something*** about topology
- Standard THC doesn't capture this intuition (even for static)
  - THC provides protection wrt worst-case graphs
  - Environment chooses both graph and corruptions in a correlated way

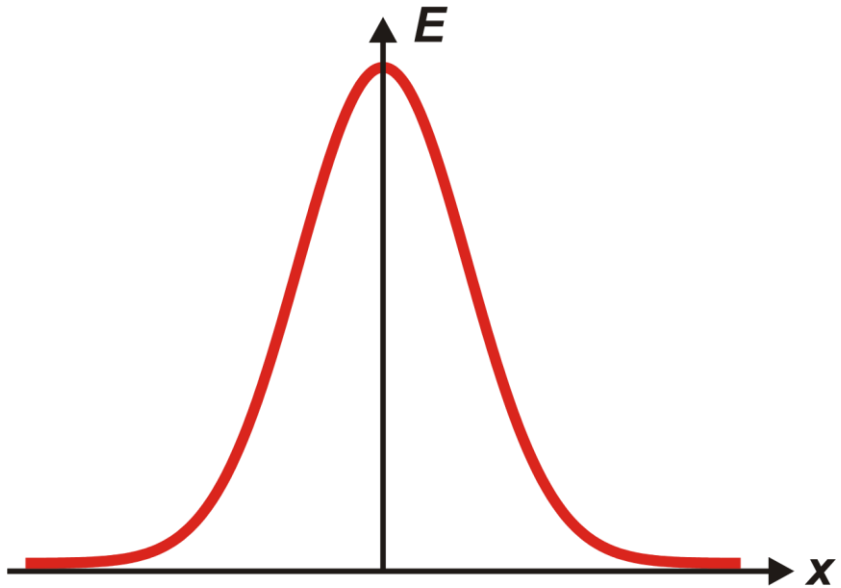


Distributional THC

New definition:

- Environment knows the distribution $\mathcal{D}$ over a class of graphs
- The network functionality samples the communication graph
- Environment can ask for the graph before deciding real/ideal

- Very subtle to formalize (see paper for details)
- Does not support computations about the graph



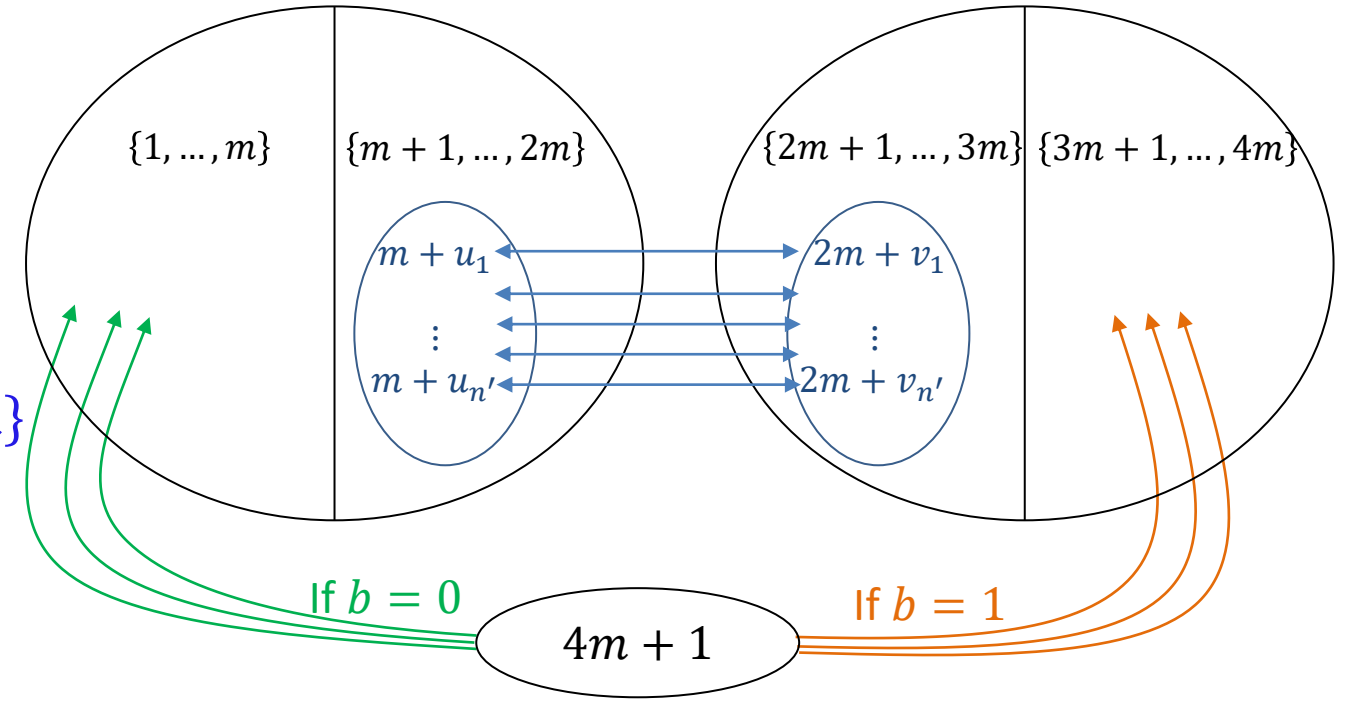
THC vs. Dist-THC

Thm 3: $\forall$ distribution $\mathcal{D}$, THC for $\mathrm{supp}(\mathcal{D}) \Rightarrow$ dist-THC for $\mathcal{D}$ (simple)

Thm 4: $\exists$ distribution $\mathcal{D}$, dist-THC for $\mathcal{D} \not\Rightarrow$ THB for any $G \in \mathrm{supp}(\mathcal{D})$

Defining the distribution $\mathcal{D}_{cut}$

- Let $n = 4m + 1$ (for $m \in \mathbb{N}$) and $n' = \log^c n$ for $c > 1$
- Let $b \in \{0,1\}$ and $\vec{u} = (u_1, \dots, u_{n'}), \vec{v} = (v_1, \dots, v_{n'}) \in [m]^{n'}$
- The graph $\boldsymbol{G_{n,c}(b, \vec{u}, \vec{v})}$:
  - Cliques $\{1, \dots, 2m\}$ and $\{2m + 1, \dots, 4m\}$
  - Edges $(m + u_j, 2m + v_j)$ for $j \in [n']$
  - If $b = 0$, $(4m + 1, i)$ for $i \in \{1, \dots, m\}$
  - If $b = 1$, $(4m + 1, i)$ for $i \in \{3m + 1, \dots, 4m\}$
- The distribution $\boldsymbol{\mathcal{D}_{cut}(n, c)}$:
  - Sample $b \leftarrow \{0,1\}$ and $\vec{u}, \vec{v} \leftarrow [m]^{n'}$
  - Output $G_{n,c}(b, \vec{u}, \vec{v})$



Lemma 1: Dist-THC for $\mathcal{D}_{cut}$

Let $\beta < 1/4$, let $c > 1$, and let f be a function

$\exists$ dist-THC protocol for f wrt $\mathcal{D}_{cut}(n, c)$ with statistical security

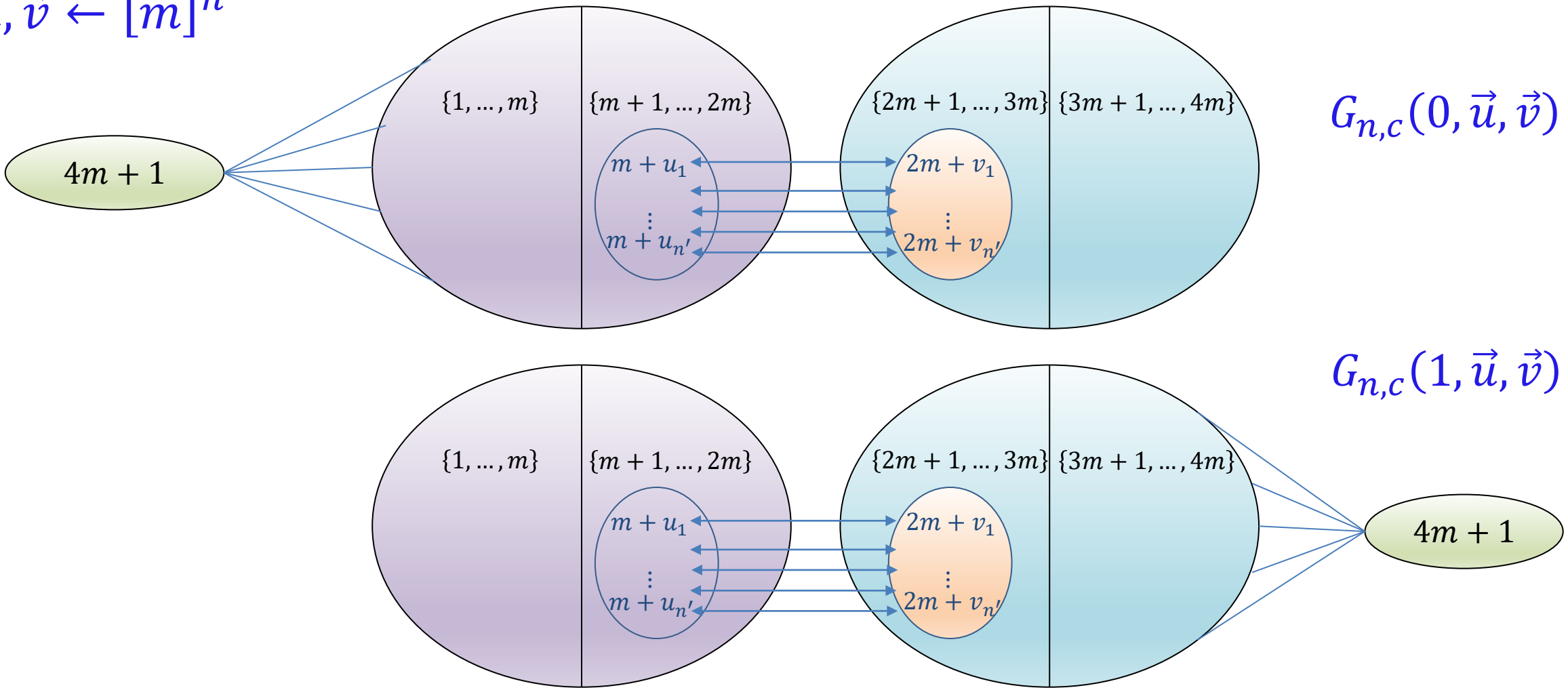
tolerating adaptive, unbounded, semi-honest, βn-adversary

Proof: similar to [B**C**DH18]

Lemma 2: No THB for $G \in \mathrm{supp}(\mathcal{D}_{cut})$

THB wrt $\mathrm{supp}\big(\mathcal{D}_{cut}(n,c)\big)$ tolerating static $\log^c n$-adversary $\Longrightarrow$ KA

Fix $\vec{u}, \vec{v} \leftarrow [m]^{n'}$



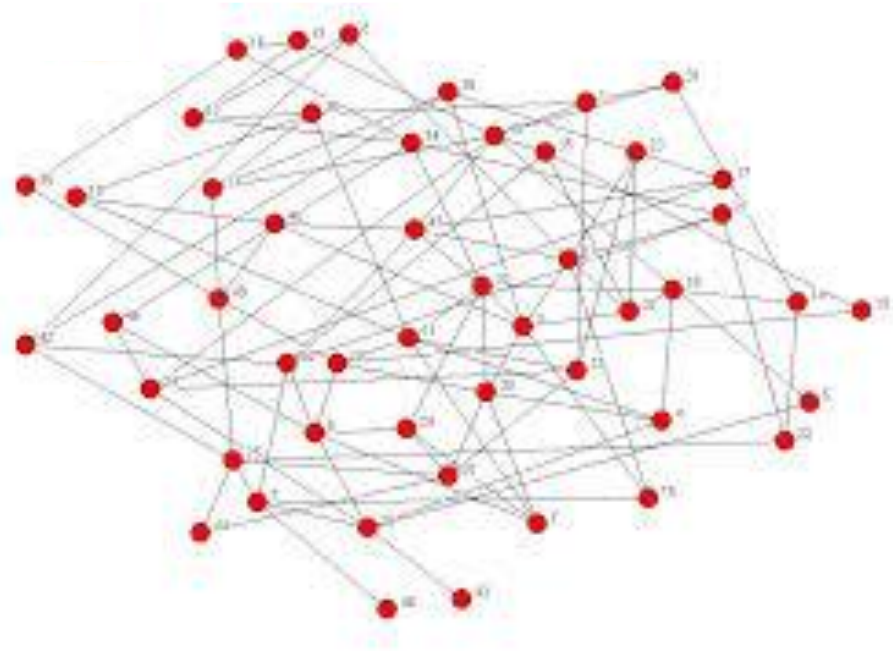
Great, but what is it good for?

Potential application:

- Adaptively secure MPC with sublinear locality [CCGGOZ15]
- Supports bounded sequential composition
- Use the hidden graph model for (topology revealing) message transmission
- For every round parties make one-time use of Erdős-Renyi graph

Thm 5: dist-THC (message transmission) for $\mathcal{D}_{ER}$

$\Rightarrow$ unbounded composition for [CCGGOZ15]



Summary & open questions

Standard THC:

- Strong impossibility of info-theoretic THC
- First feasibility result
- **Open: understand more classes of graphs**
- **Open: is there 0/1 feasibility law (Adv can/not disconnect the graph)**
- **Open: THC from OT**
- **Open: malicious THC**

New definition, dist-THC:

- Strictly weaker than standard THC
- Can hide sublinear cuts
- **Open: feasibility for other distributions**
- **Open: Erdős-Renyi graphs**