Topology-Hiding Computation From Key Agreement in Diameter-Two Graphs

D'or Banoun

Elette Boyle

Ran Cohen

Secure Multiparty Computation (MPC)

A system of n parties

Each party P_i holds private input x_i

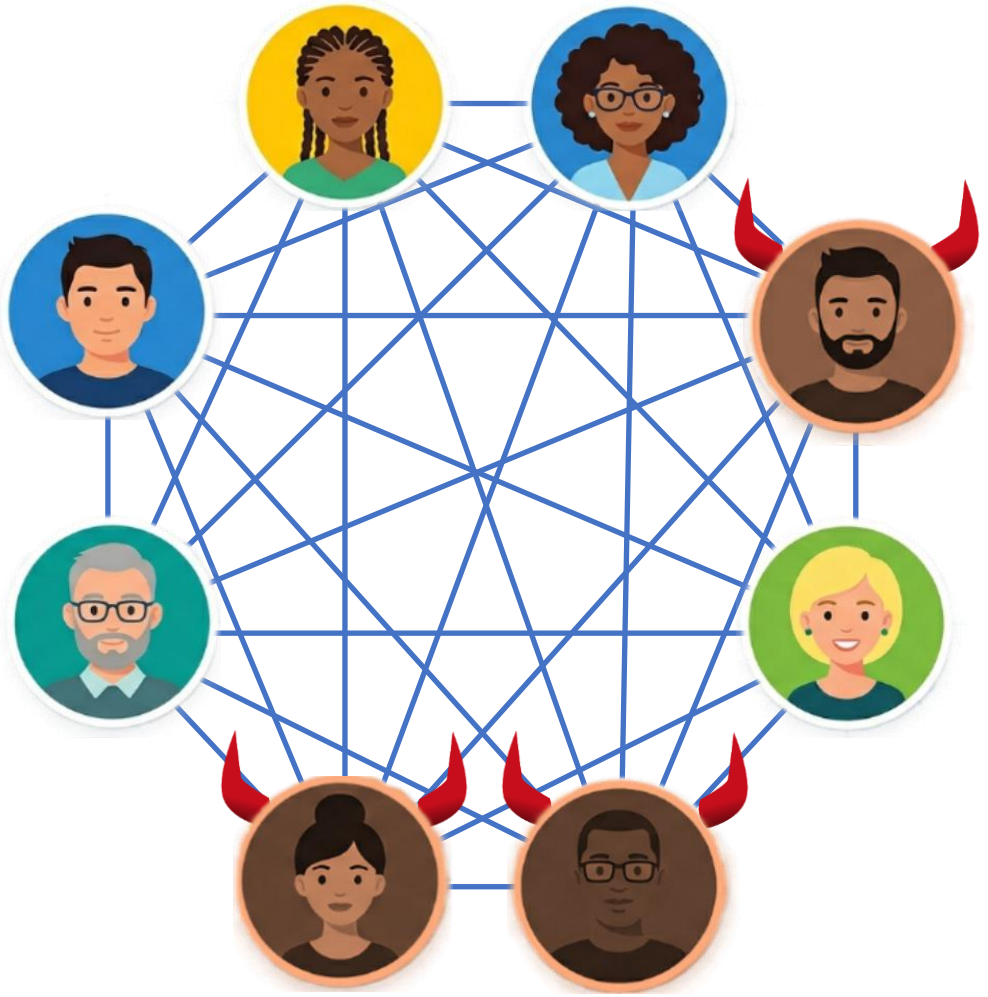
Their goal is to run a protocol to compute

$$y = f(x_1, \dots, x_n)$$

Up to t parties may collude

- **Correctess:** everyone obtains correct output
- **Privacy:** no one learns anything but the output

In this talk: corrupted parties do not cheat but try to break privacy (semi-honest)



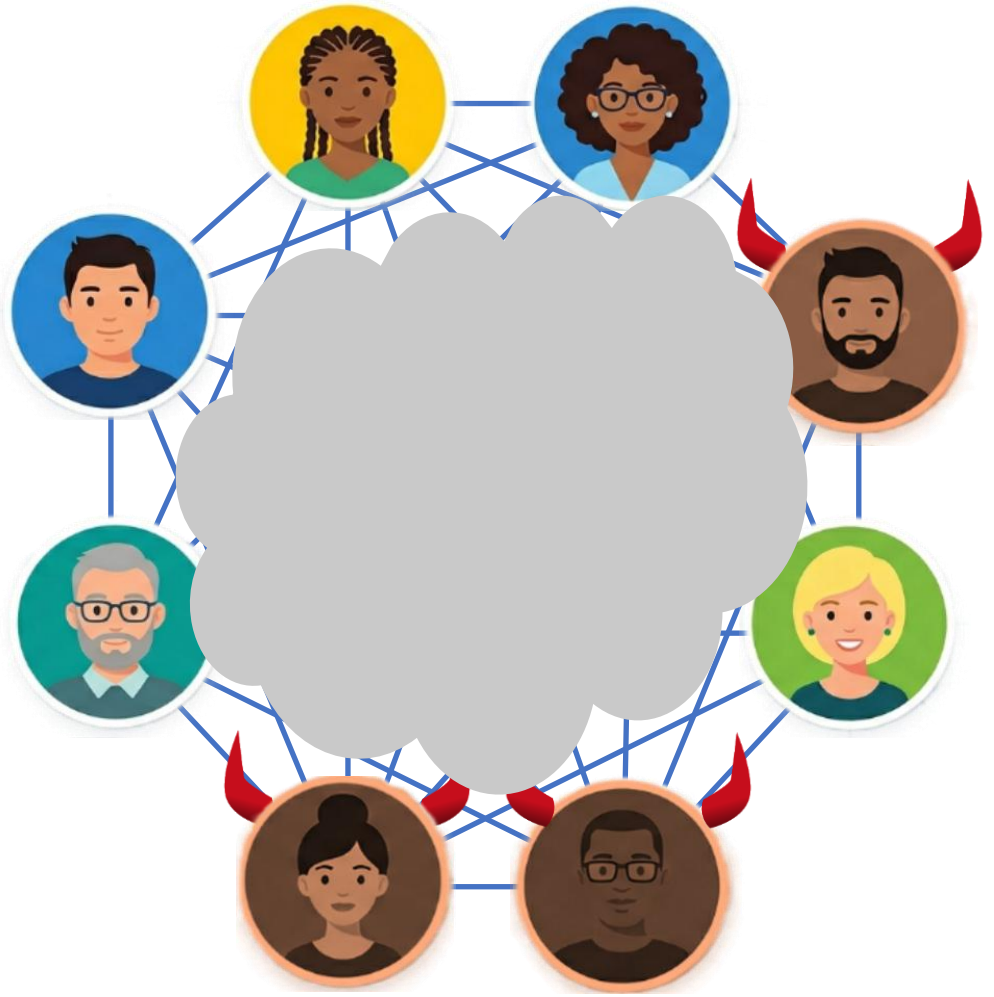
MPC over incomplete networks

Sometimes, by necessity or by design, the protocol is run over a **partial graph**

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

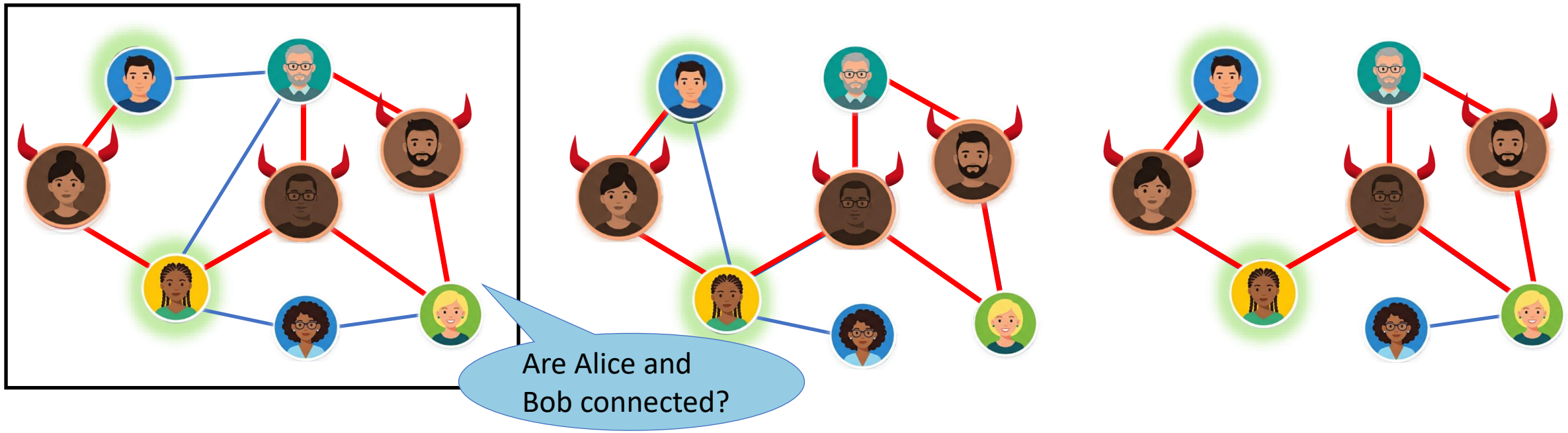
- Private social networks
- Vehicle-to-vehicle networks
- …

Goal: running a protocol while hiding the network topology



Topology-Hiding Computation (THC) [Moran, Orlov, Richelson '15]

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

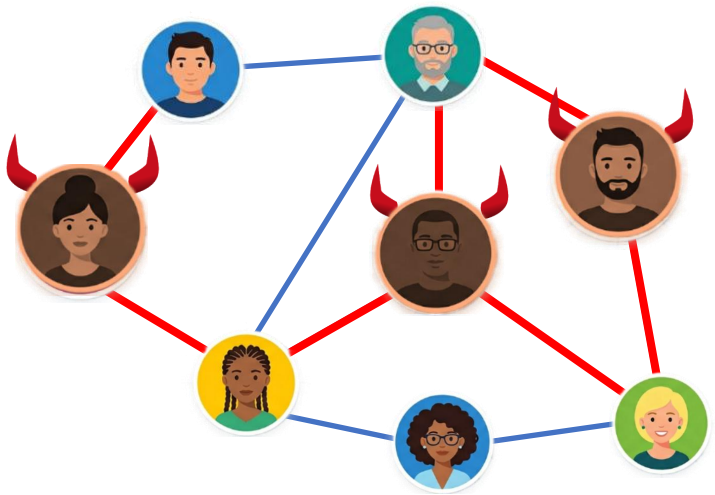


Topology-Hiding Computation (THC) [Moran, Orlov, Richelson '15]

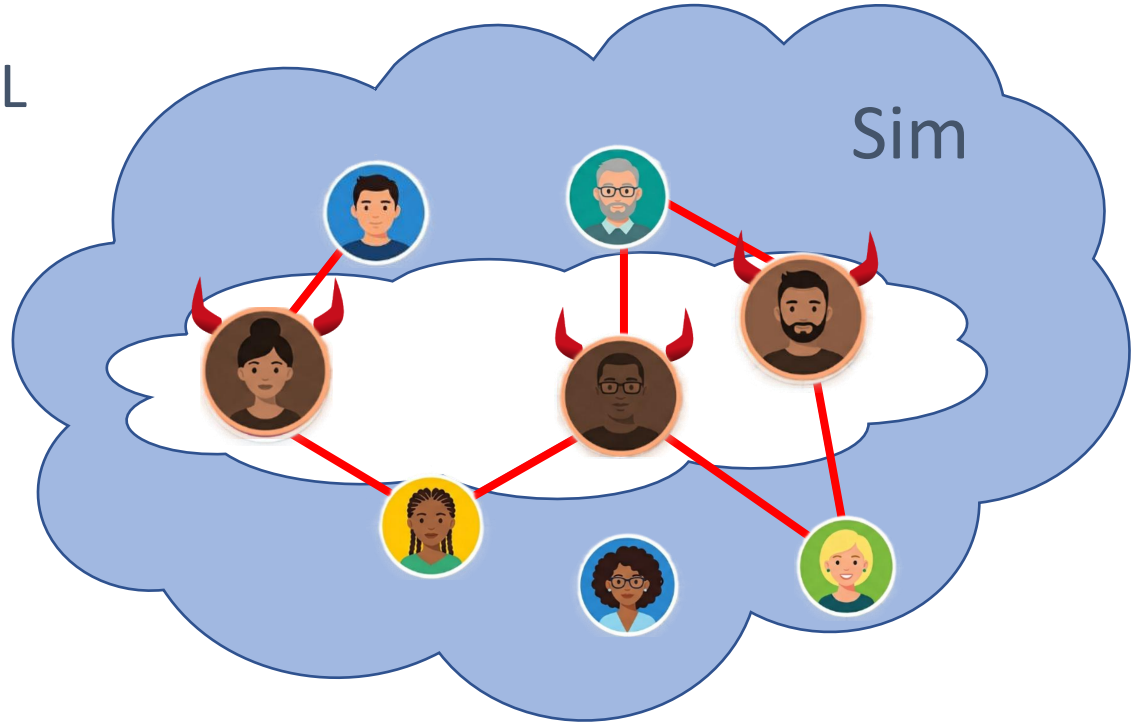
Everything Adv learns on the graph can be simulated from:

- Neighbor-set of corrupted parties
- Class of potential graphs

REAL

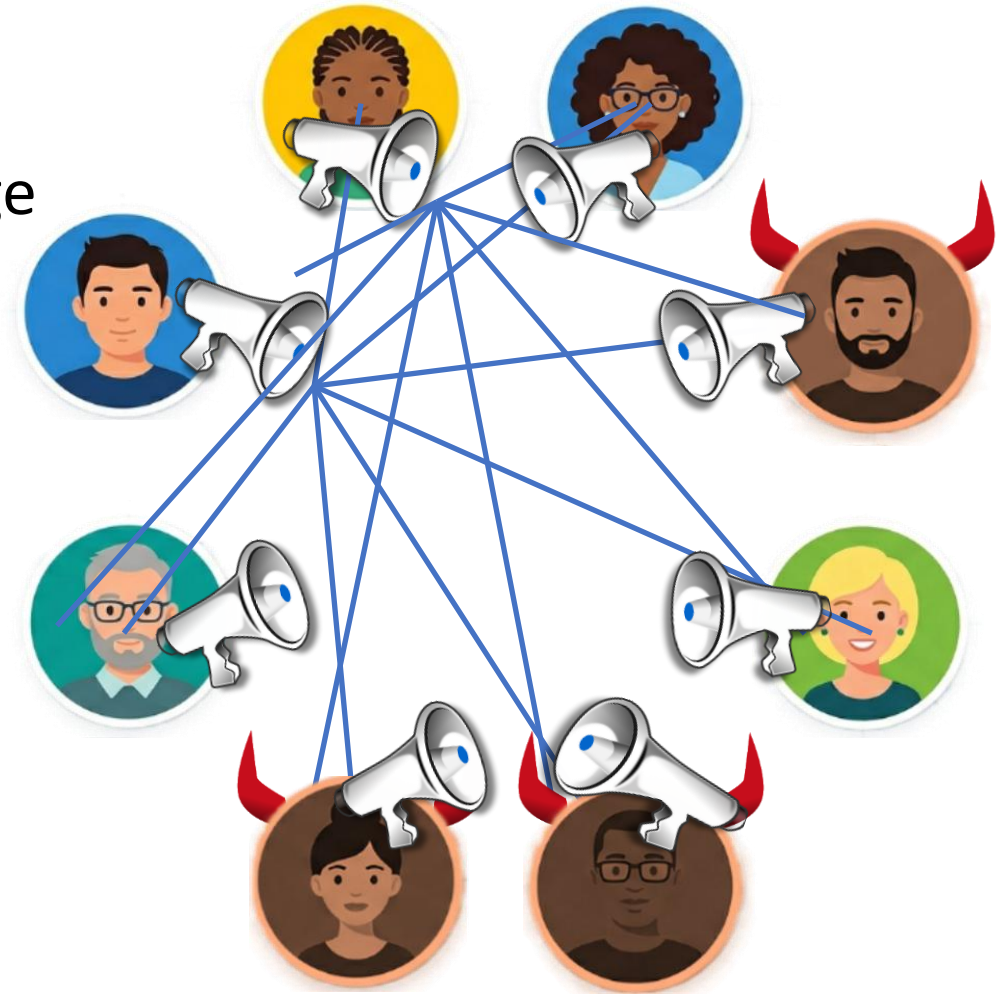


IDEAL



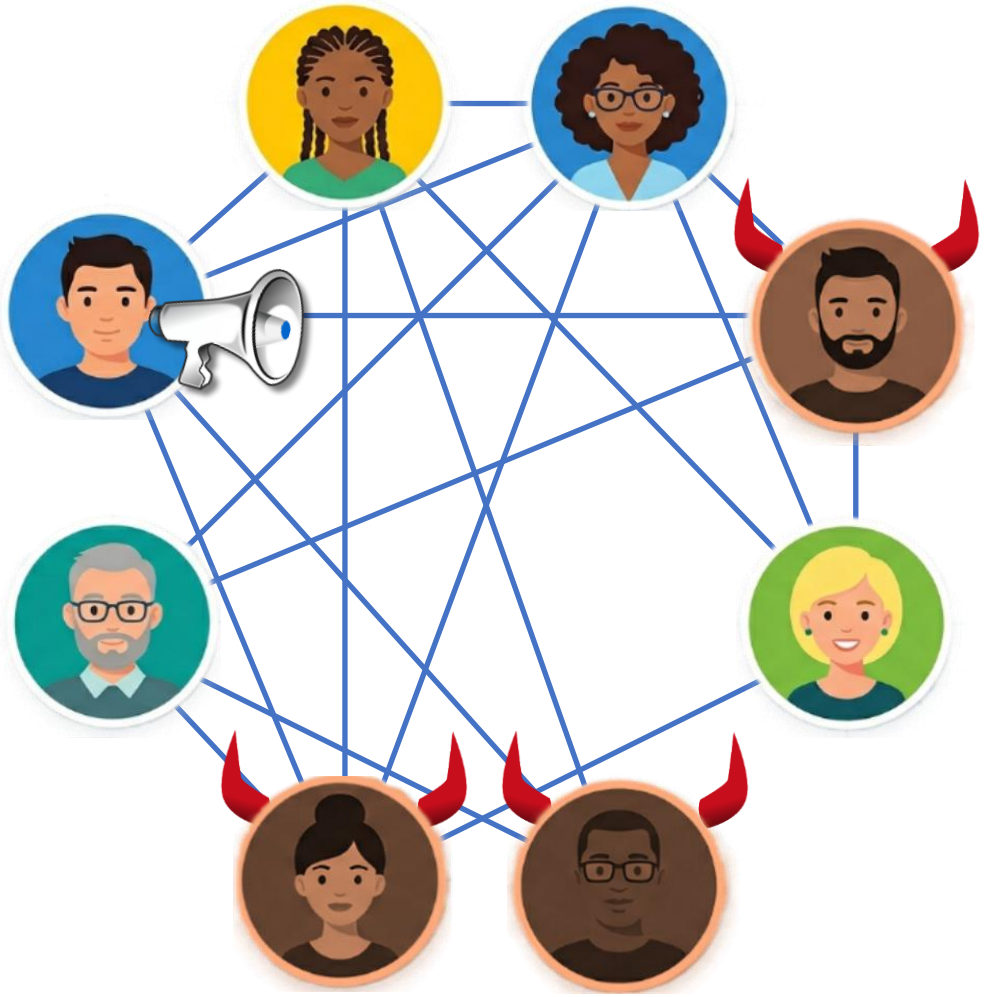
Blueprint for THC

1) Start with MPC over a broadcast channel
   - When a party talks everyone hears the message
   - No point-to-point communication
   - Can use key agreement (KA) to establish private communication over broadcast



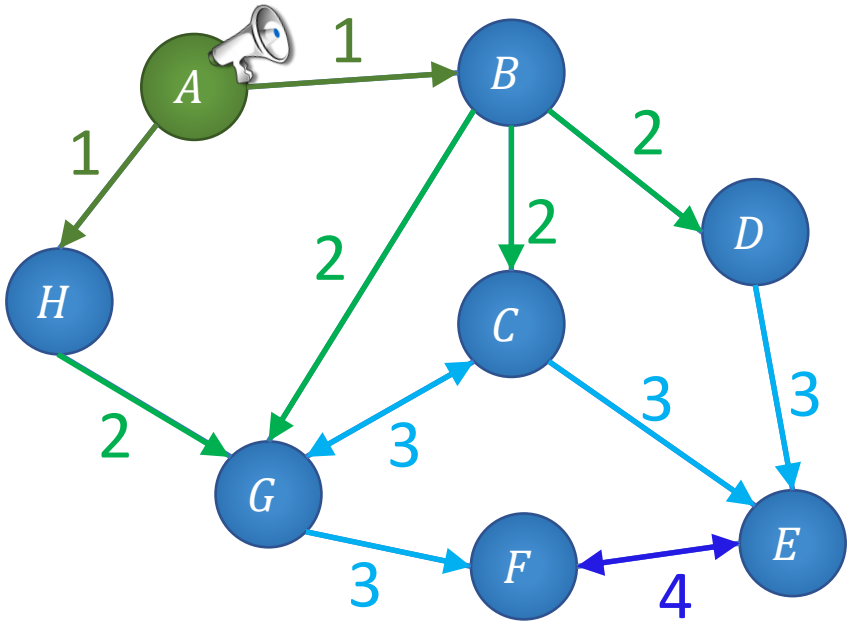
Blueprint for THC

1) Start with MPC over a broadcast channel
2) Build **topology-hiding broadcast (THB)**
   - One sender
   - All parties learn the sender's message
   - Hide graph's topology from corrupted parties



Topology-Hiding Broadcast isn't easy (even with one corruption)

Consider a flooding protocol:



Each party learns:

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

Cryptography relies on unproven assumptions

Cryptographers seldom sleep well

Hierarchy of cryptographic assumptions

No assumptions
(information-theoretic security)

One-time pad
MPC for $t < n/2$

Hierarchy of cryptographic assumptions

One-way functions (minicrypt)

Symetric encryption
Digital signatures
Zero-knowledge proofs for NP

No assumptions (information-theoretic security)

One-time pad
MPC for $t < n/2$

Hierarchy of cryptographic assumptions

Key agreement (cryptomania) 	Public-key encryption Security needed for the Internet
One-way functions (minicrypt) 	Symetric encryption Digital signatures Zero-knowledge proofs for NP
No assumptions (information-theoretic security) 	One-time pad MPC for $t < n/2$

Hierarchy of cryptographic assumptions

Oblivious transfer (MPC land) 	MPC for $t < n$
Key agreement (cryptomania) 	Public-key encryption Security needed for the Internet
One-way functions (minicrypt) 	Symetric encryption Digital signatures Zero-knowledge proofs for NP
No assumptions (information-theoretic security) 	One-time pad MPC for $t < n/2$

Hierarchy of cryptographic assumptions

DDH

LWE

QR

Specific mathematical assumptions

Oblivious transfer
(MPC land)

MPC for $t < n$

Key agreement
(cryptomania)

Public-key encryption
Security needed for the Internet

One-way functions
(minicrypt)

Symetric encryption
Digital signatures
Zero-knowledge proofs for NP

No assumptions
(information-theoretic security)

One-time pad
MPC for $t < n/2$

So, in which world is THC?

DDH

LWE

QR

Oblivious transfer
(MPC land)

Key agreement
(cryptomania)

One-way functions
(minicrypt)

No assumptions
(information-theoretic security)

Topology-Hiding Computation

Topology-Hiding Broadcast
(no input privacy)

So, in which world is THC?

DDH

LWE

QR

Oblivious transfer
(MPC land)

Key agreement
(cryptomania)

One-way functions
(minicrypt)

No assumptions
(information-theoretic security)

Topology-Hiding Computation

Topology-Hiding Broadcast
(no input privacy)

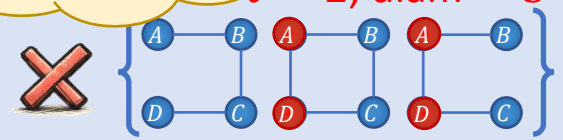
All graphs $t < n$
[ALM'17, LLMMMT'18, BBMM'18]

[HMTZ'16] [AM'17] [BBKM'23]

Small diameter $t < n$
[MOR'15]

What about
$t > 1$?

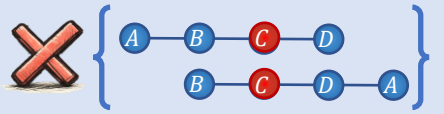
$t = 2$, diam $= 3$



[BBMM'18]

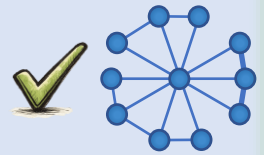
All graphs $n > 3$, $t = 1$
[BBCKMMM'20]

$t = 1$, 1-connected

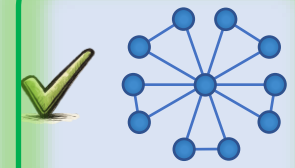


[BBCMM'19]

2-connected $t = 1$
[BBCKMMM'20]



$t = 1$



$t < n$

[BBC'24]

Our questions: consider $t > 1$

Is there non-trivial t-secure THC without assuming OT?

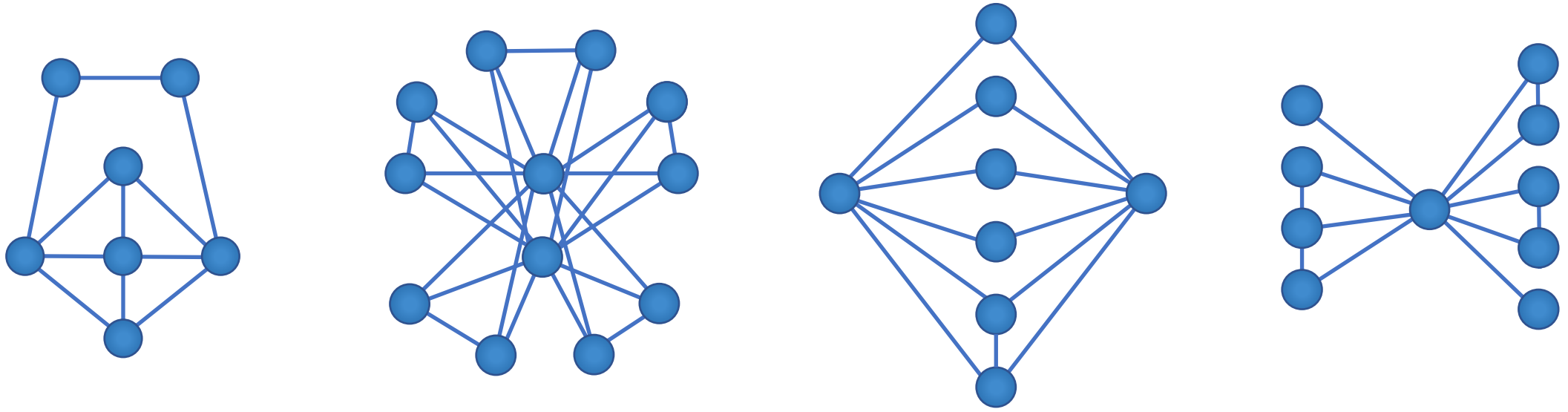
t-secure THB: either IT-secure or requires OT?
(zero-one law)

Our results #1: feasibility

For a large family of diameter-2 graphs:

KA $\Longrightarrow$ t**-secure THB** with $t < n$

$\Longrightarrow$ t**-secure THC** with $t < n/2$



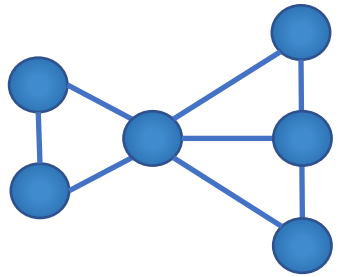
Our results #2: lower bound

Result #1

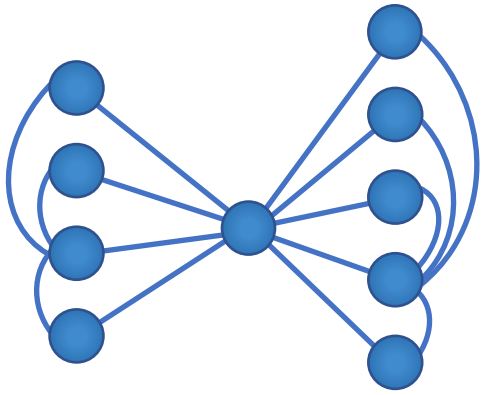
$\Leftarrow$

t-secure THB on "join-stars" $\Longrightarrow$ KA

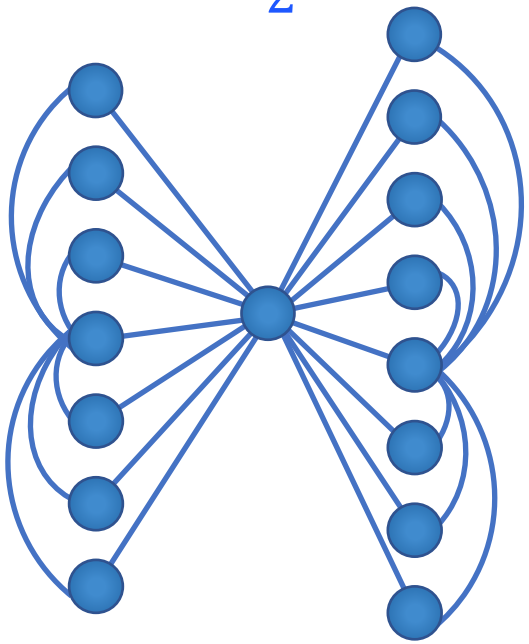
✗ $t = 2$
$n = 6$



✗ $t = 4$
$n = 10$



✗ $t = \frac{n}{2} - 1$



See paper for details

So, in which world is THC?

DDH

LWE

QR

Oblivious transfer
(MPC land)

Key agreement
(cryptomania)

One-way functions
(minicrypt)

No assumptions
(information-theoretic security)

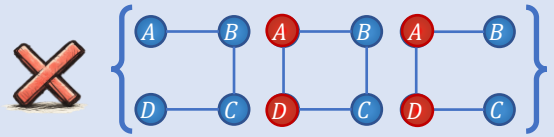
Topology-Hiding Computation

Topology-Hiding Broadcast
(no input privacy)

✓ All graphs $t < n$
[ALM'17, LLMMMT'18, BBMM'18]

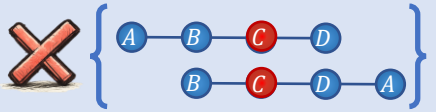
[HMTZ'16] [AM'17] [BBKM'23]

✓ Small diameter $t < n$
[MOR'15]



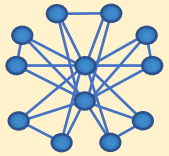
[BBMM'18]

✓ All graphs $n > 3, t = 1$
[BBCKMMM'20]



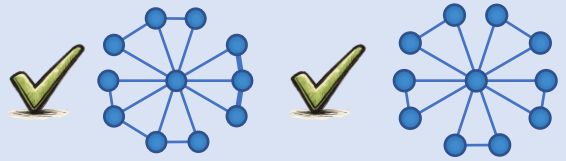
[BBCMM'19]

THC
$t < n/2$



THB
$t < n$

✓ 2-connected $t = 1$
[BBCKMMM'20]



$t = 1$ $t < n$

[BBC'24]

THC from KA on Diameter-2 Graphs

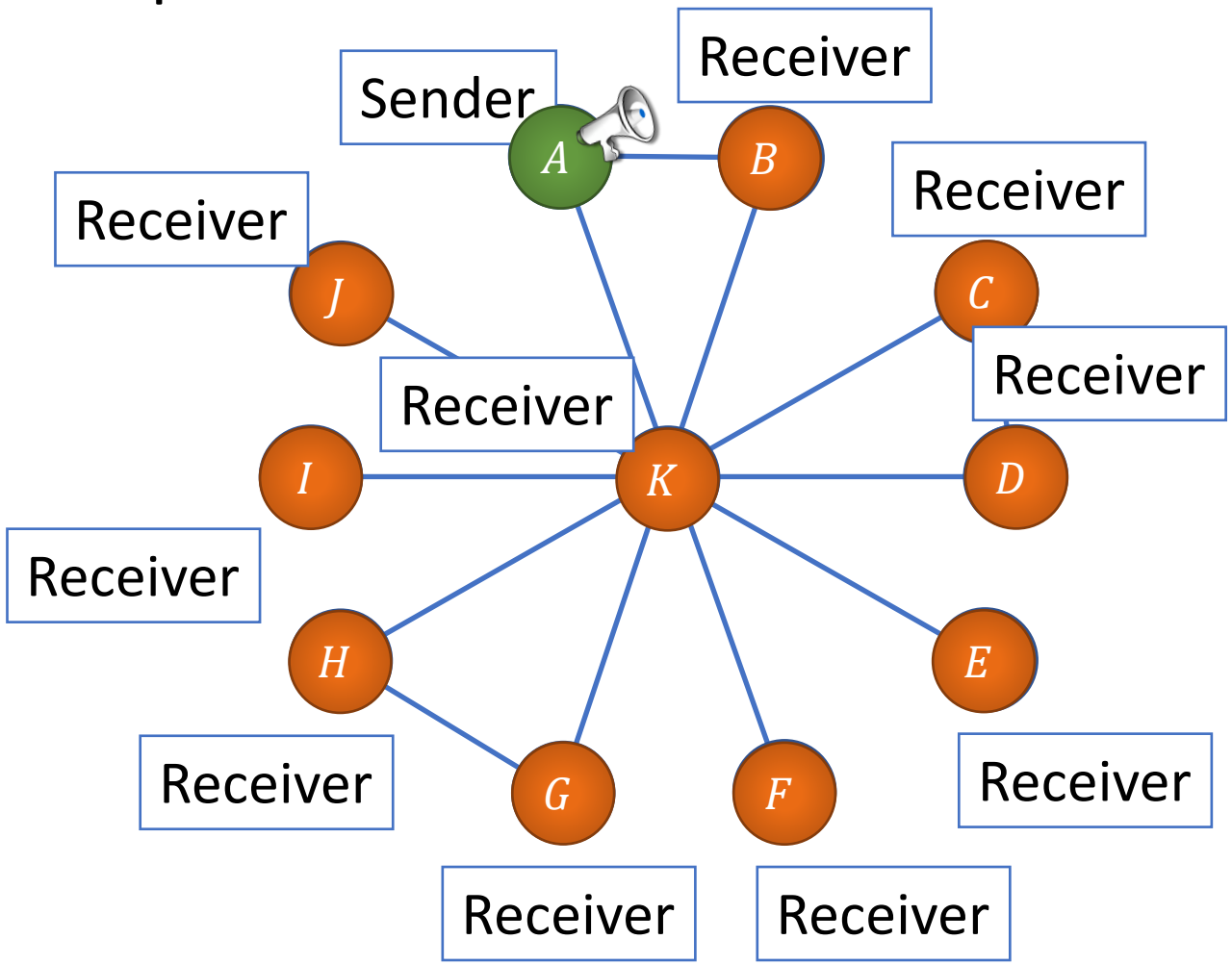
THC from KA on Diameter-2 Graphs

THB + KA + $t < n/2$ $\Longrightarrow$ THC

Construct THB via TH-RMT
(reliable message transmission)

- Send to one receiver at a time
- Sender & receiver are known

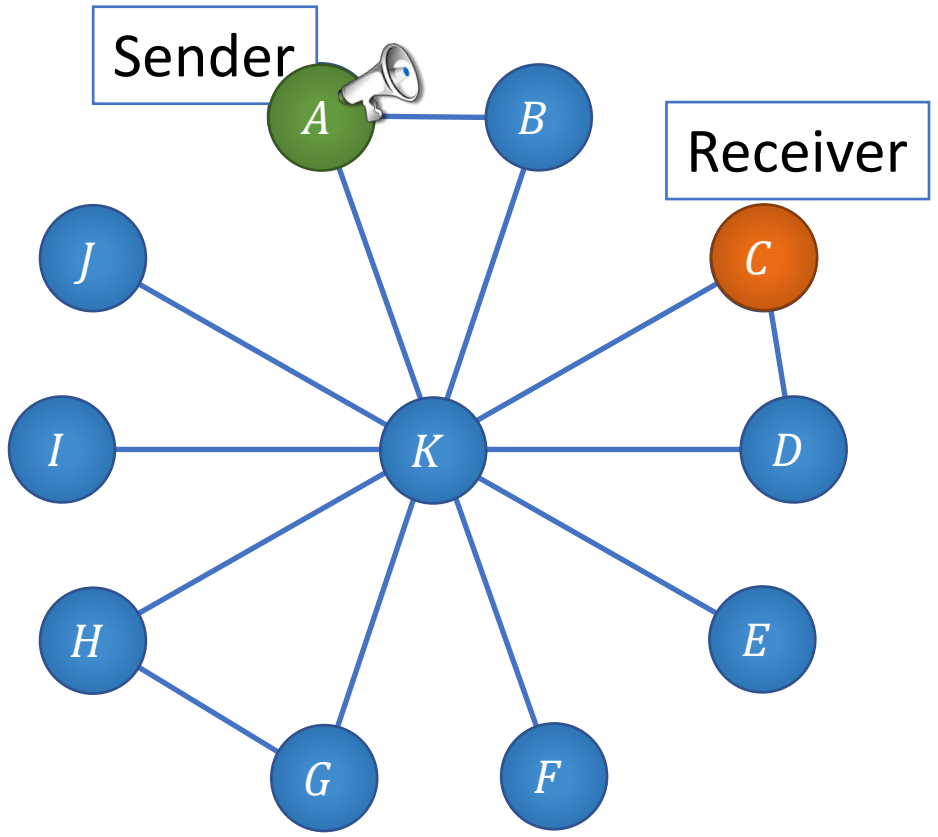
New goal: topology-hiding RMT



TH-RMT from KA on Diameter-2 Graphs (warm-up)

Warm-up:

- Single center
- Other nodes have degree 1 or 2



What's to hide?

- Non-center don't know who's the center
- Center doesn't know the parties' degree
- Center doesn't know who's connected to whom

TH-RMT from KA on Diameter-2 Graphs (warm-up)

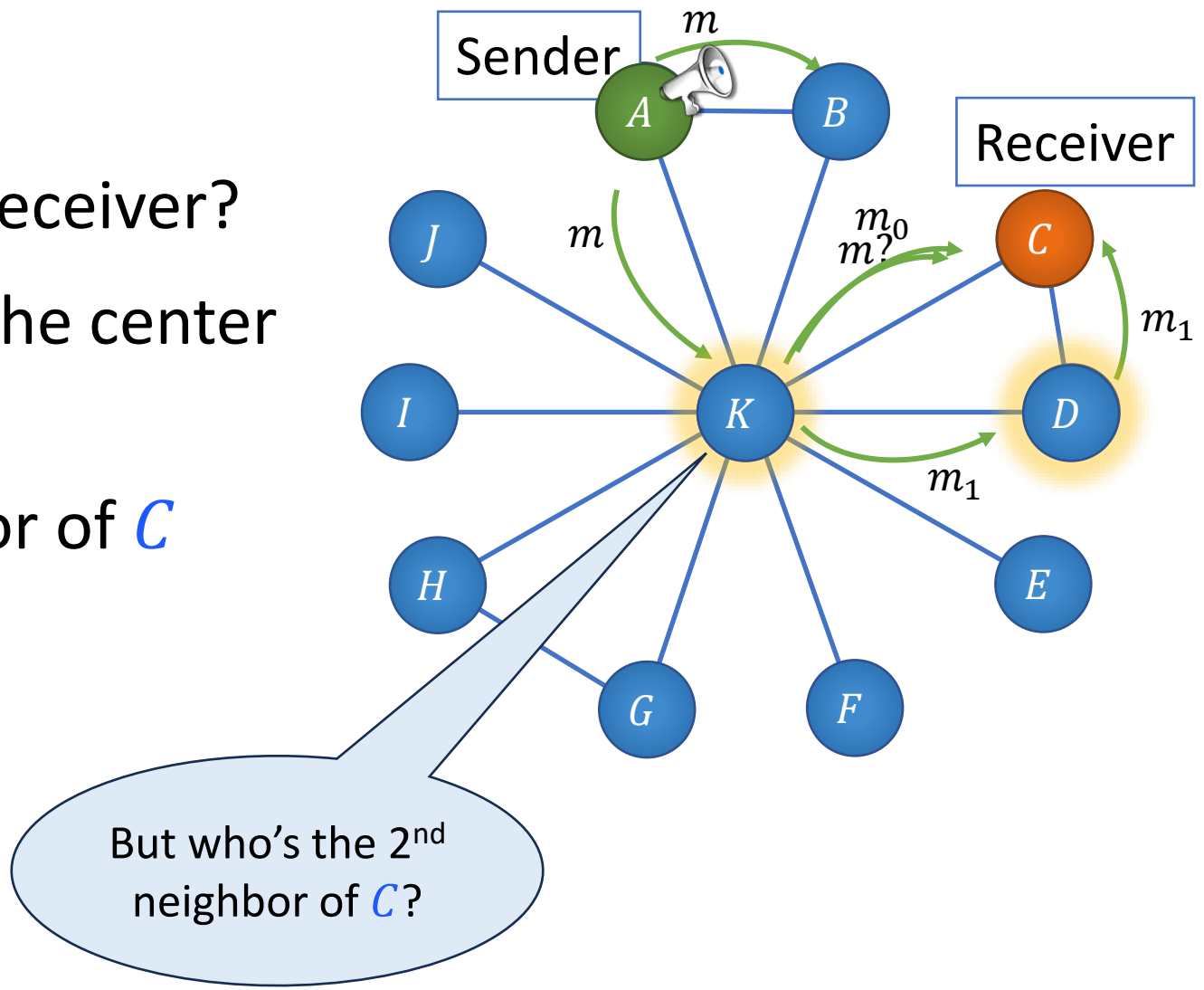
Sender sends m to its neighbors

Q: Can the center forward m to receiver?

A: No! Receiver will learn who's the center

Suppose: K knows D is a neighbor of C

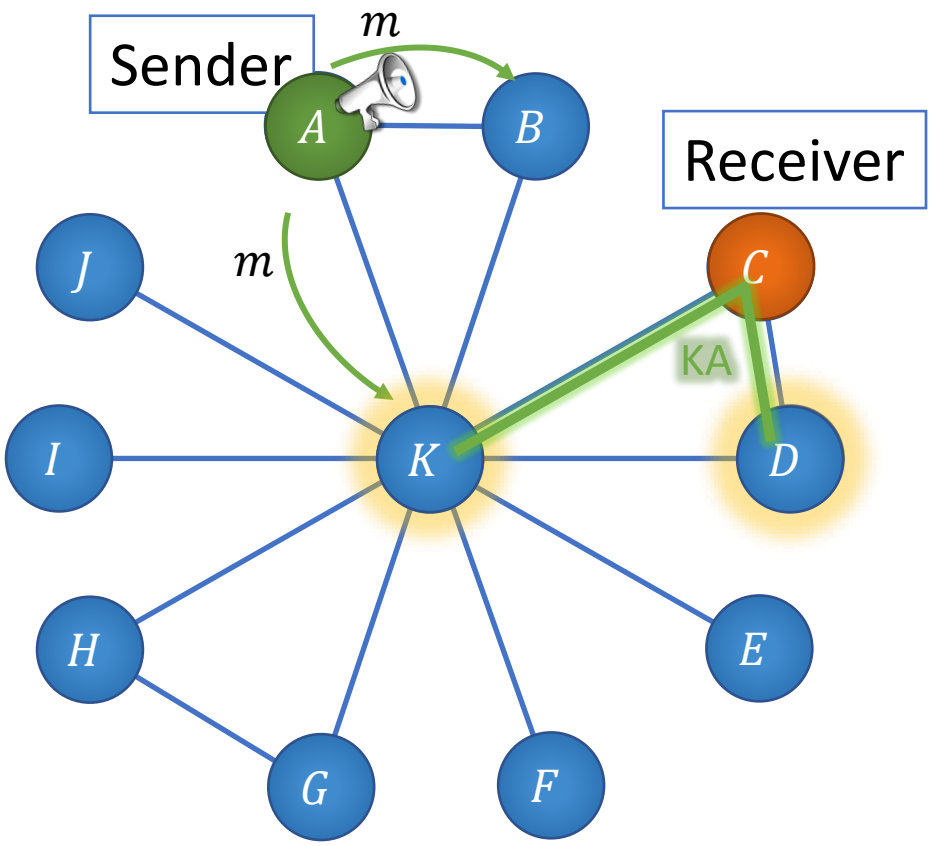
- K sets $m = m_0 \oplus m_1$
- K sends m_1 to D
- K and D send their share to C



TH-RMT from KA on Diameter-2 Graphs (warm-up)

K and D establish a private channel via C

- They run a KA protocol via C
- K doesn't know who is the 2nd neighbor



TH-RMT from KA on Diameter-2 Graphs (warm-up)

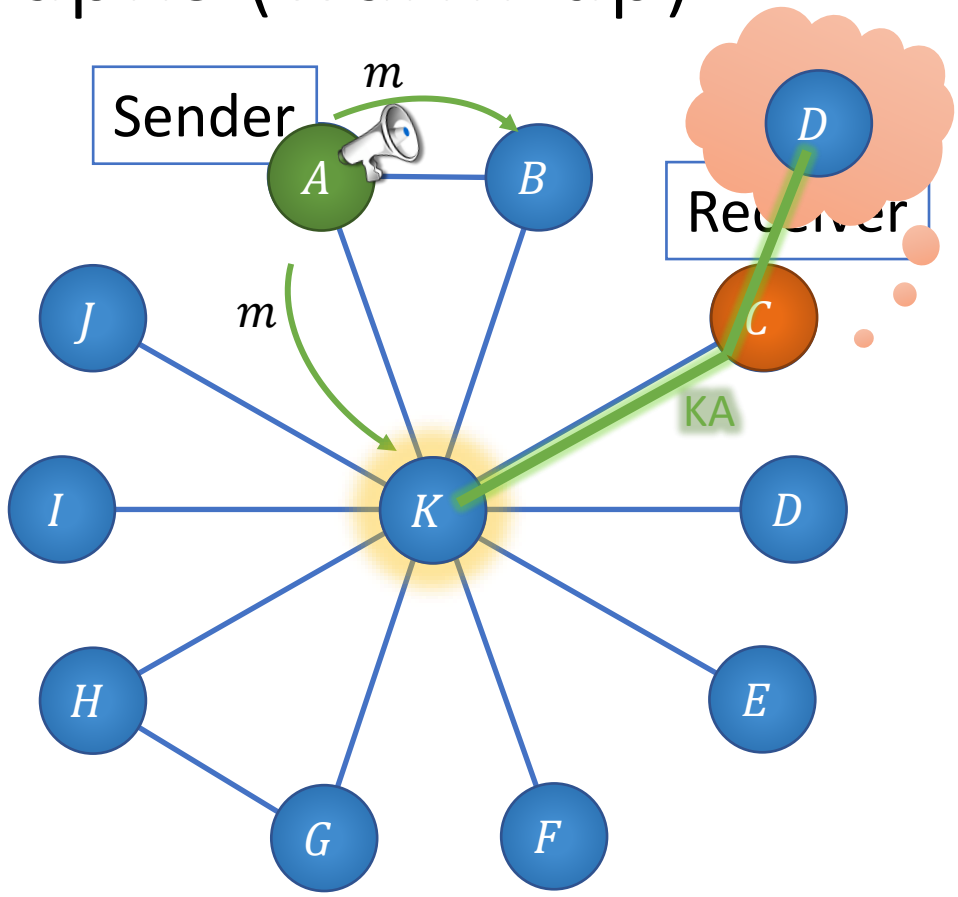
K and D establish a private channel via C

- They run a KA protocol via C
- K doesn't know who is the 2nd neighbor

Q: What if C has degree 1?

C must hide its degree from K

A: C emulates D in its his head

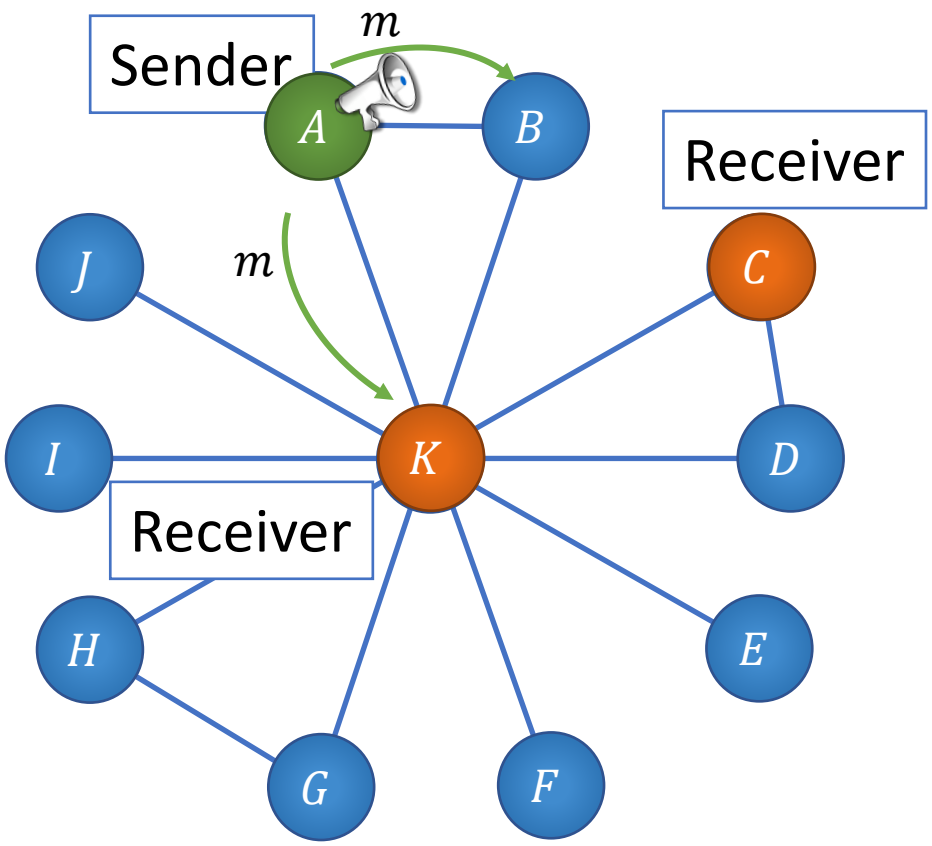


TH-RMT from KA on Diameter-2 Graphs (warm-up)

What if the receiver is the center?

Center already knows the message m

Q: Are we done?



TH-RMT from KA on Diameter-2 Graphs (warm-up)

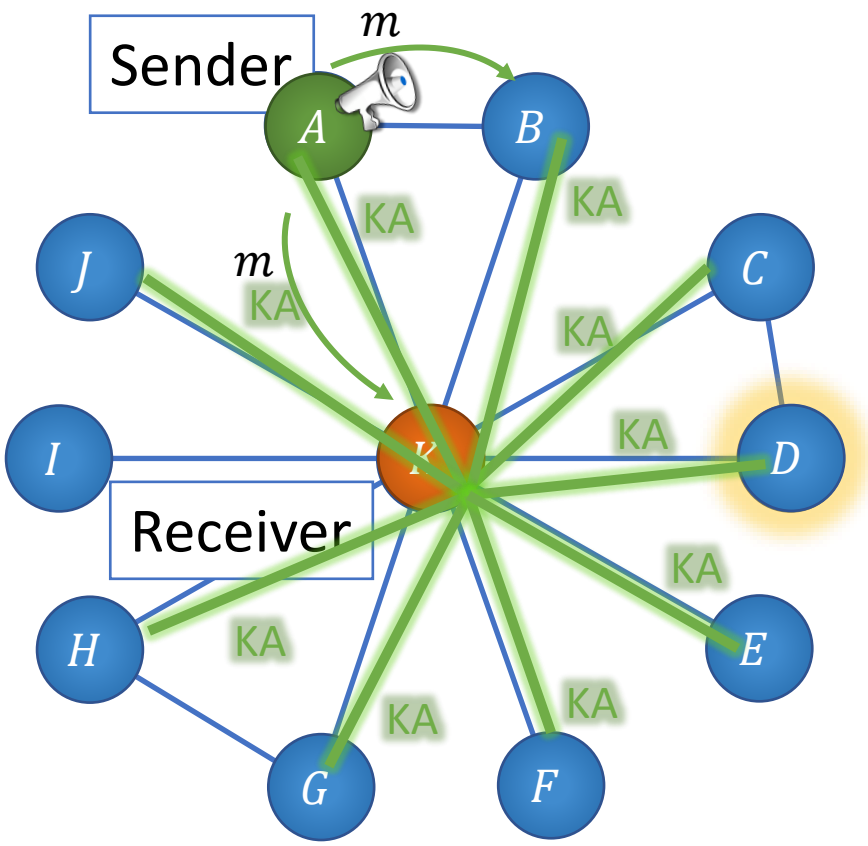
What if the receiver is the center?

Center already knows the message m

Q: Are we done?

A: No! Stopping will leak who's the center

Receiver establishes a secure channel between every pair of neighbors



Problem: D can distinguish

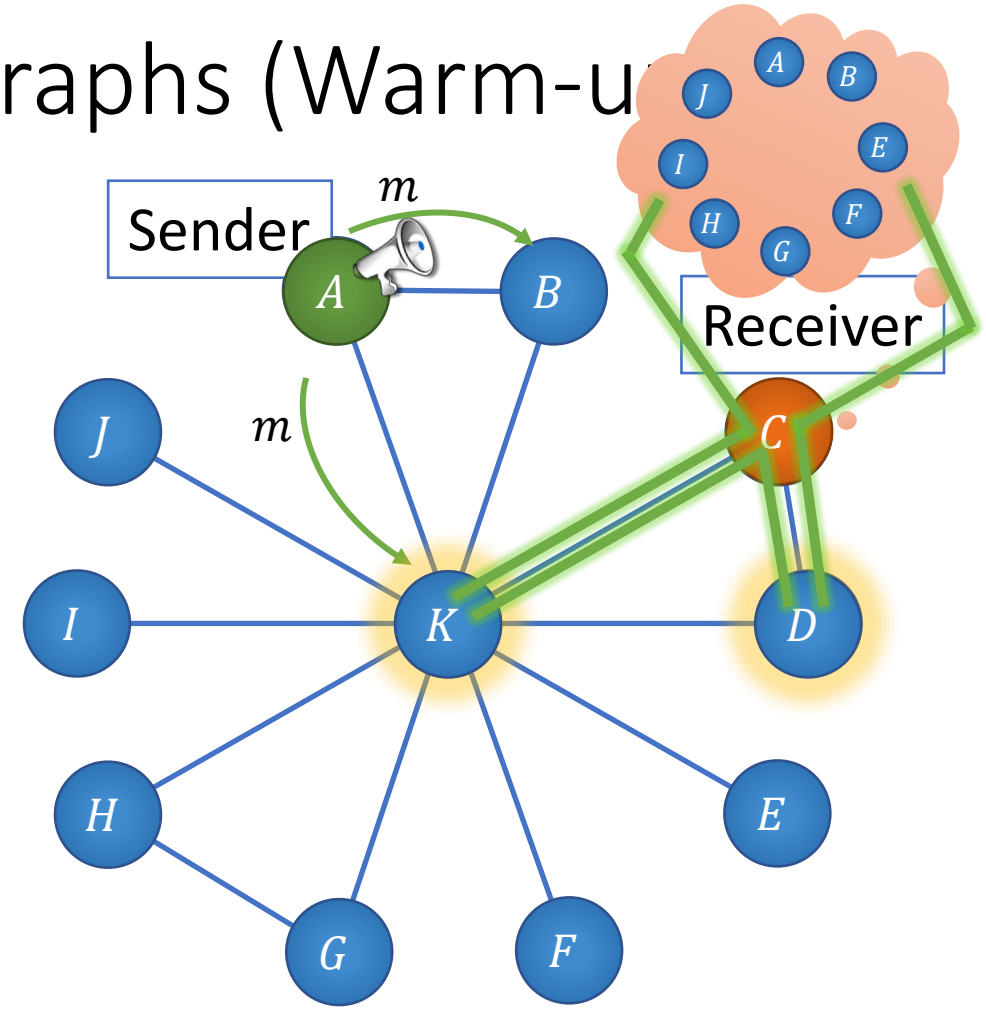
- If receiver is center: $n-2$ channels
- If receiver is non-center: 1 channel

TH-RMT from KA on Diameter-2 Graphs (Warm-u

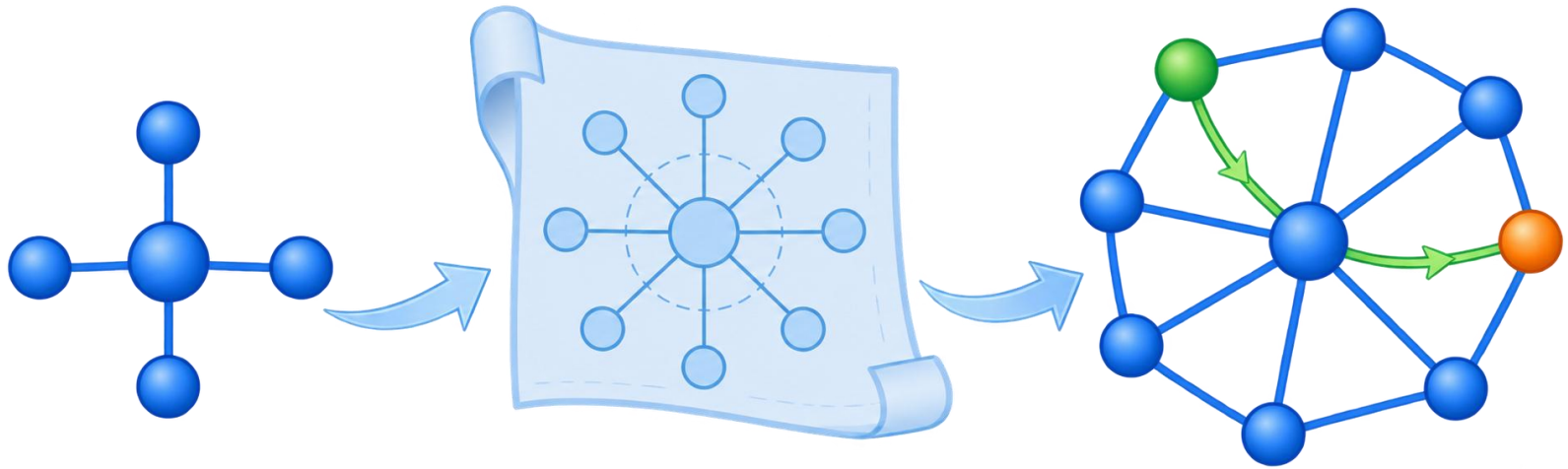
Problem: D can distinguish

- If receiver is center: $n-2$ channels
- If receiver is non-center: 1 channel

Solution:
If C is the receiver emulates
all non-neighboring parties



Template for THC from KA on Diameter-2 Graphs

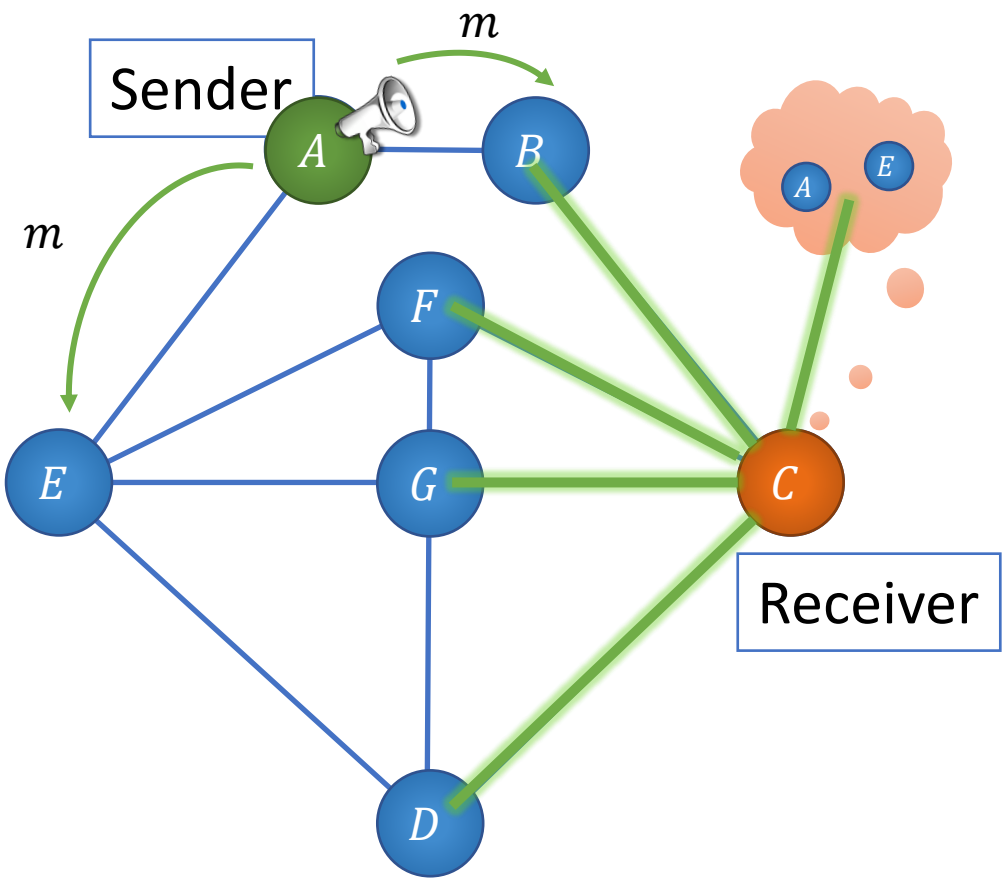


Template for general diameter-2 graphs

1. Sender sends m to its neighbors
2. Receiver's neighbors generate pair-wise secure channels

   Receiver emulates non-neighboring parties
3. Using MPC, receiver obliviously obtains message from its neighbors
   Effectively compute Boolean OR

Challenge: for $t \geq n/2$, OR requires OT



d-common neighbors, for a known d

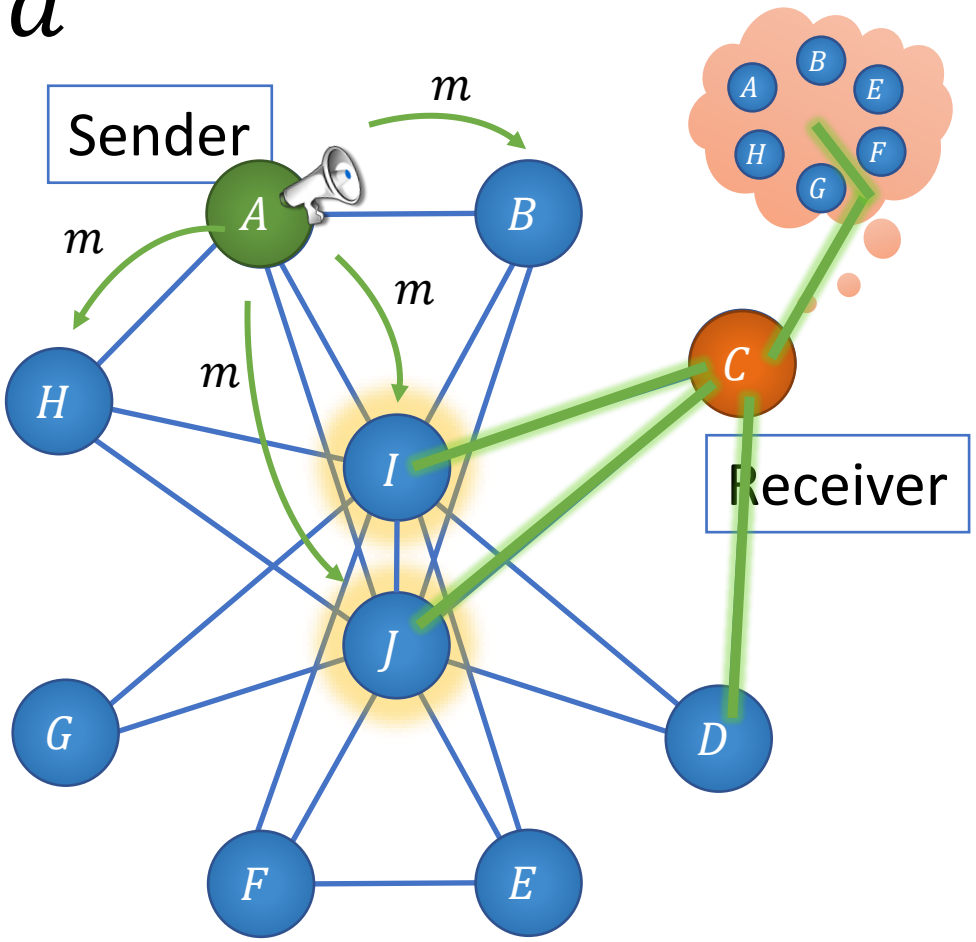
d common neighbors input $m_i = m$

Every other neighbor inputs $m_i = 0$

Compute the linear function:

$$\frac{1}{d} \cdot \sum m_i = m$$

BGW is secure for $t < n$



$d = 2$

Unknown-but-odd common neighbors

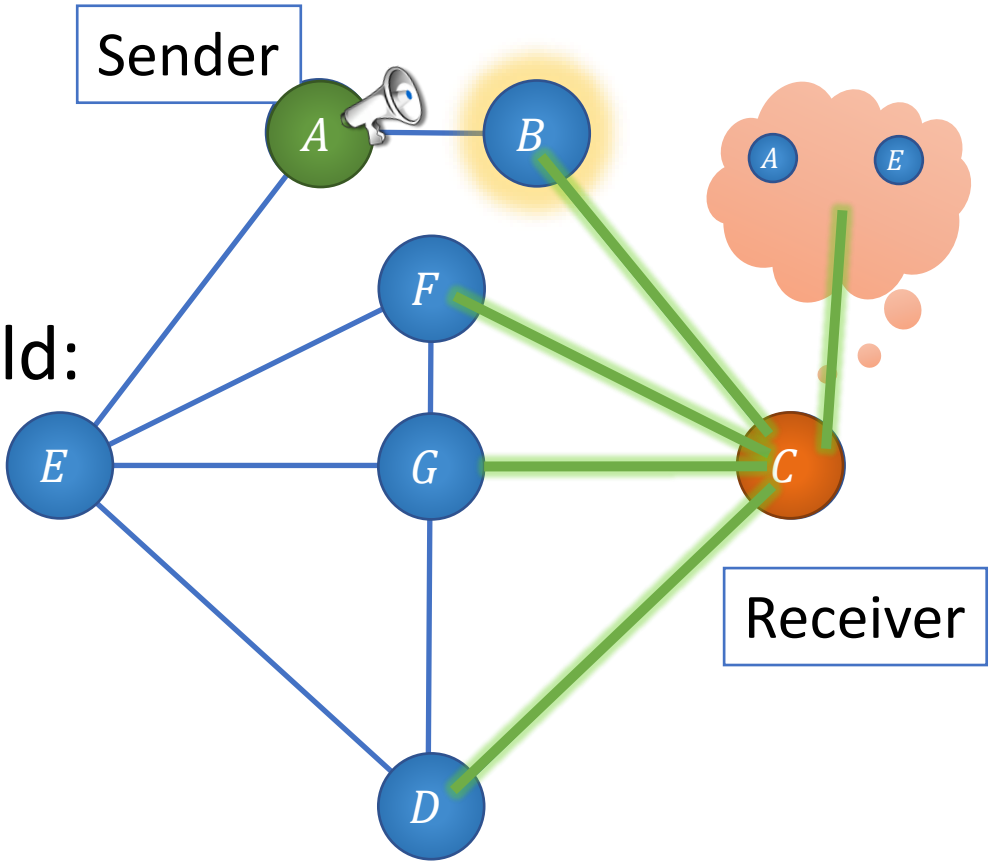
All common neighbors input $m_i = m$

Every other neighbor inputs $m_i = 0$

Compute the linear function over a binary field:

$$\bigoplus m_i$$

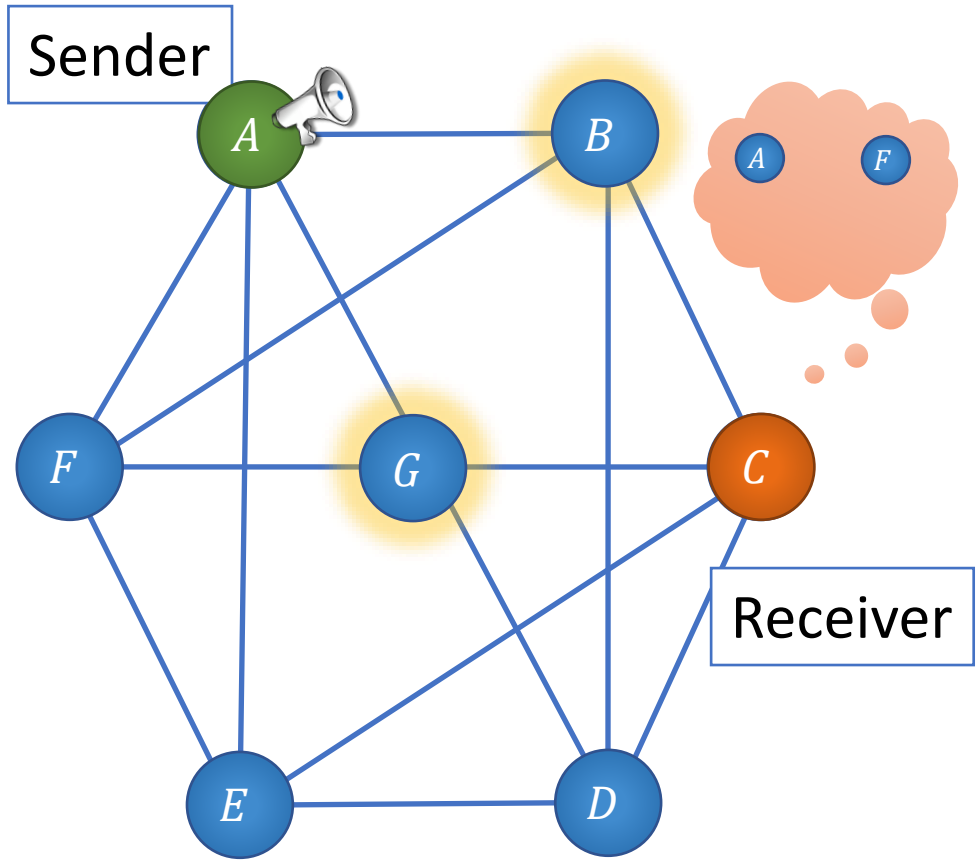
BGW secure for $t < n$



Degree condition

Can use non-linear BGW given
an honest majority in each neighborhood

See paper for more details



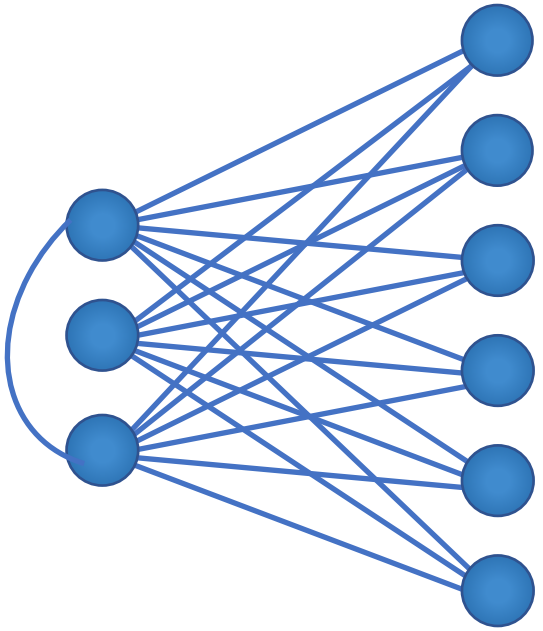
Summary (diameter 2, $t > 1$)

Is there non-trivial t-secure THC without assuming OT?

t-secure THB: either IT-secure or requires OT?
(zero-one law)

Many open questions:

- Fully characterise diameter 2 graphs?
- Malicious security?
- THC from Minicrypt?



Thank you for listening!