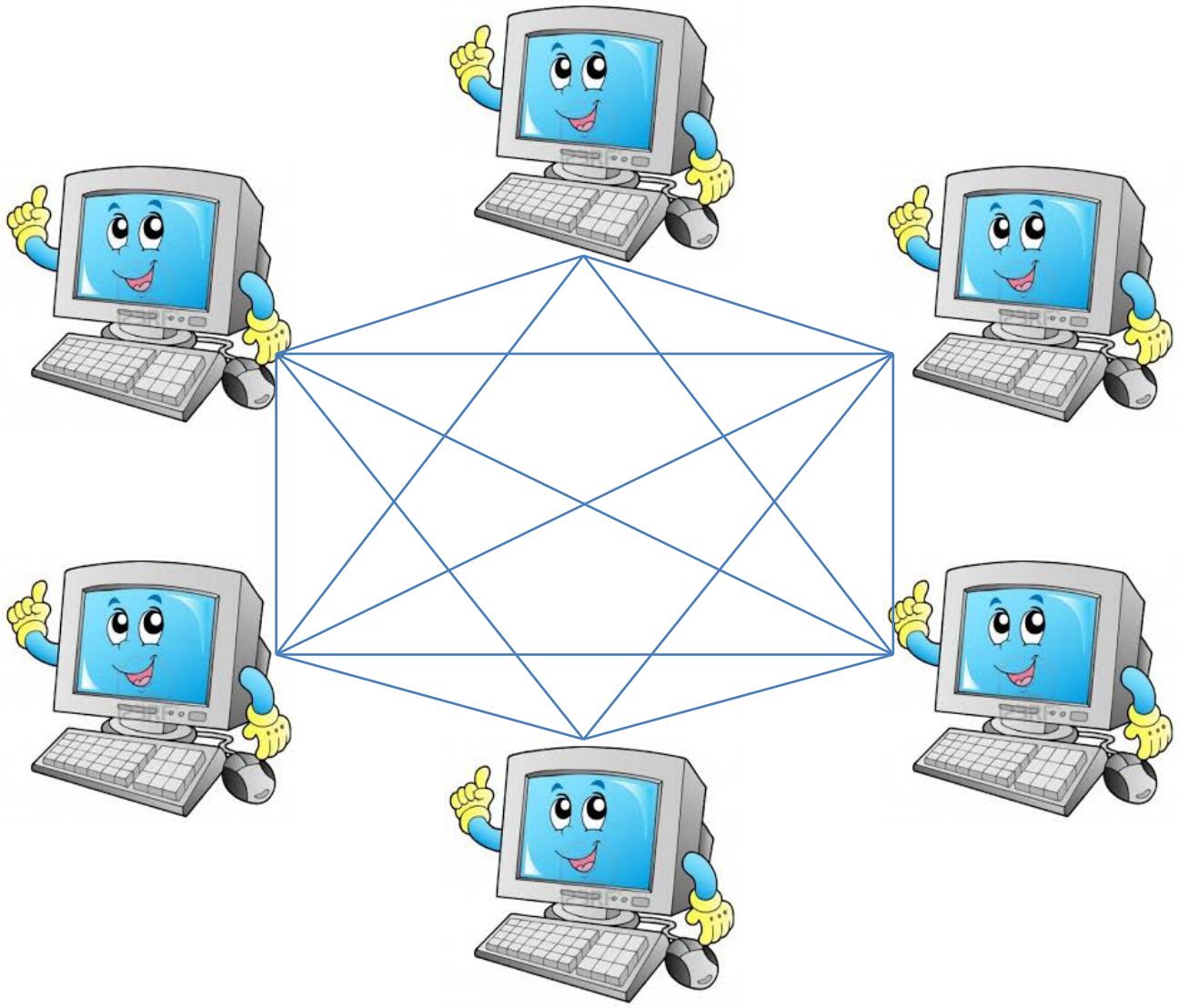
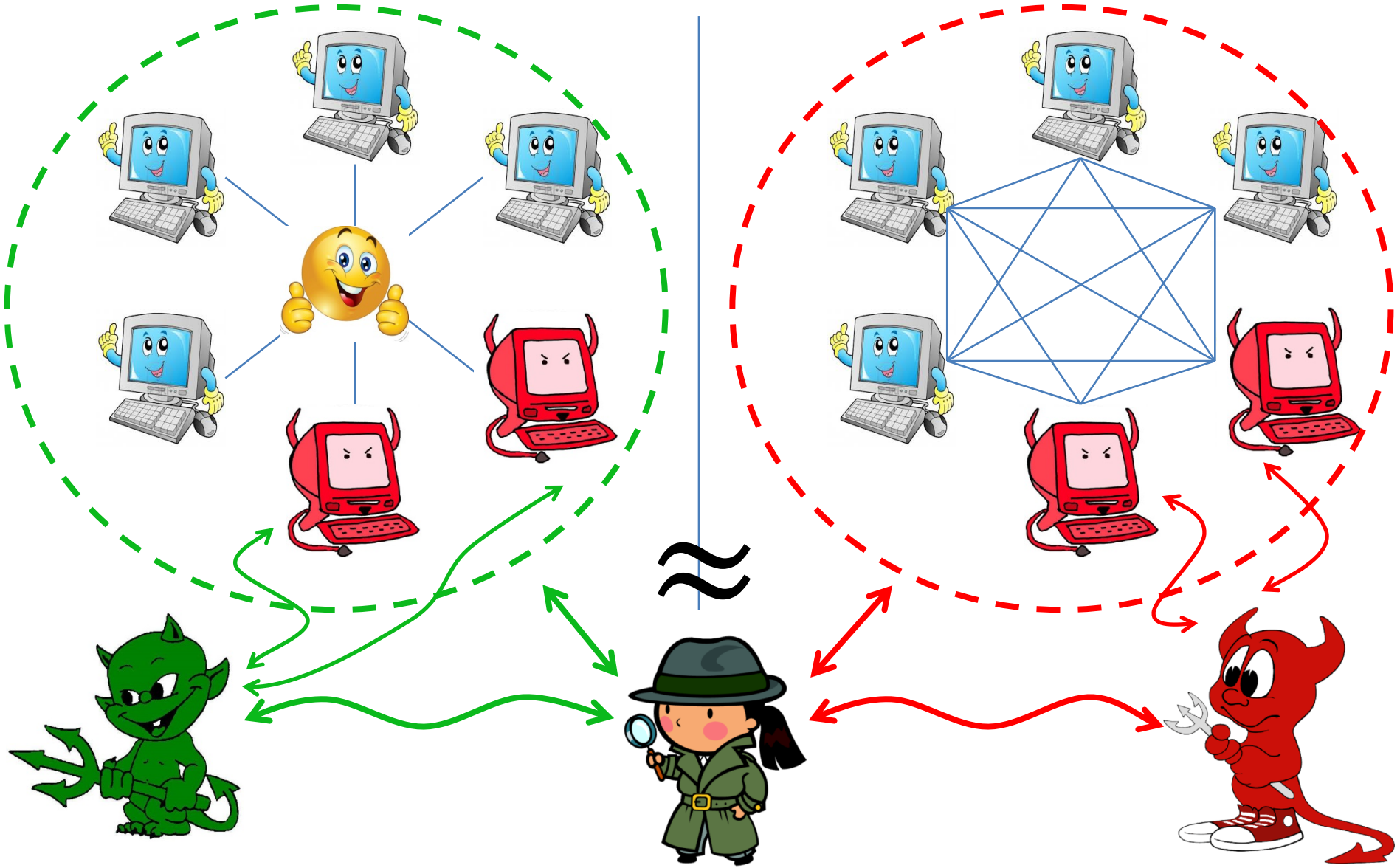
2-Round MPC: Do We Need a Megaphone?

Ran Cohen (Northeastern U. and BU)
Juan Garay (Texas A&M University)
Vassilis Zikas (U. of Edinburgh)

Secure Multiparty Computation (MPC)



Simulation-based Security



Round Complexity

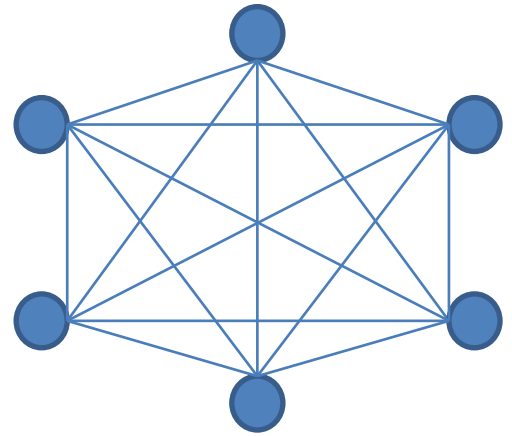
- Important efficiency measure
- “Holy grail”: Two-round MPC
  - First solutions: FHE/iO [AJLTVW12, GGHR14,MW16]
  - Recent work: 2-round MPC from standard assumptions
- Communication resources?

Round Complexity

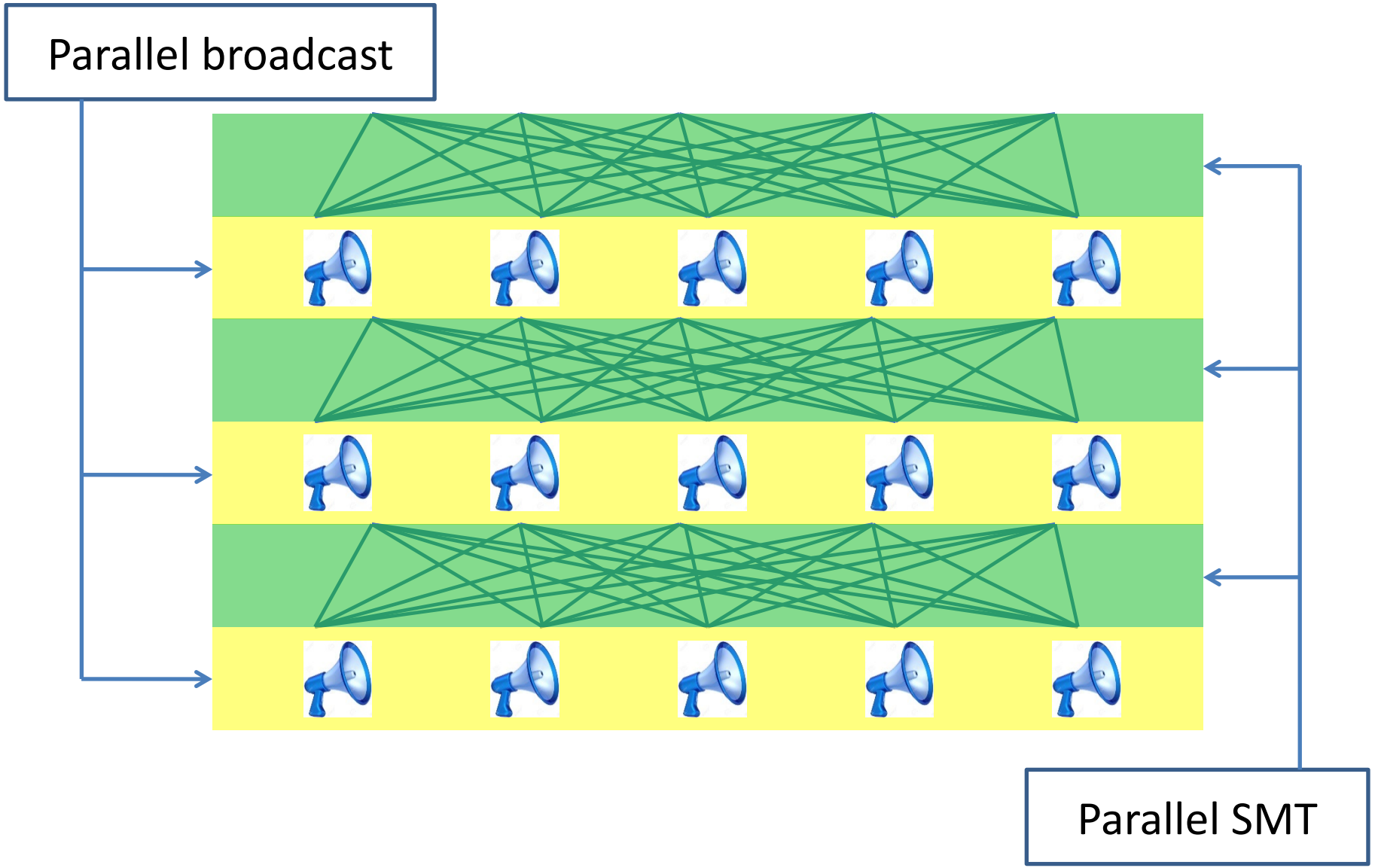
- Important efficiency measure
- “Holy grail”: Two-round MPC
  - First solutions: FHE/iO [AJLTVW12, GGHR14,MW16]
  - Recent work: 2-round MPC from standard assumptions
- Communication resources?

Communication Models

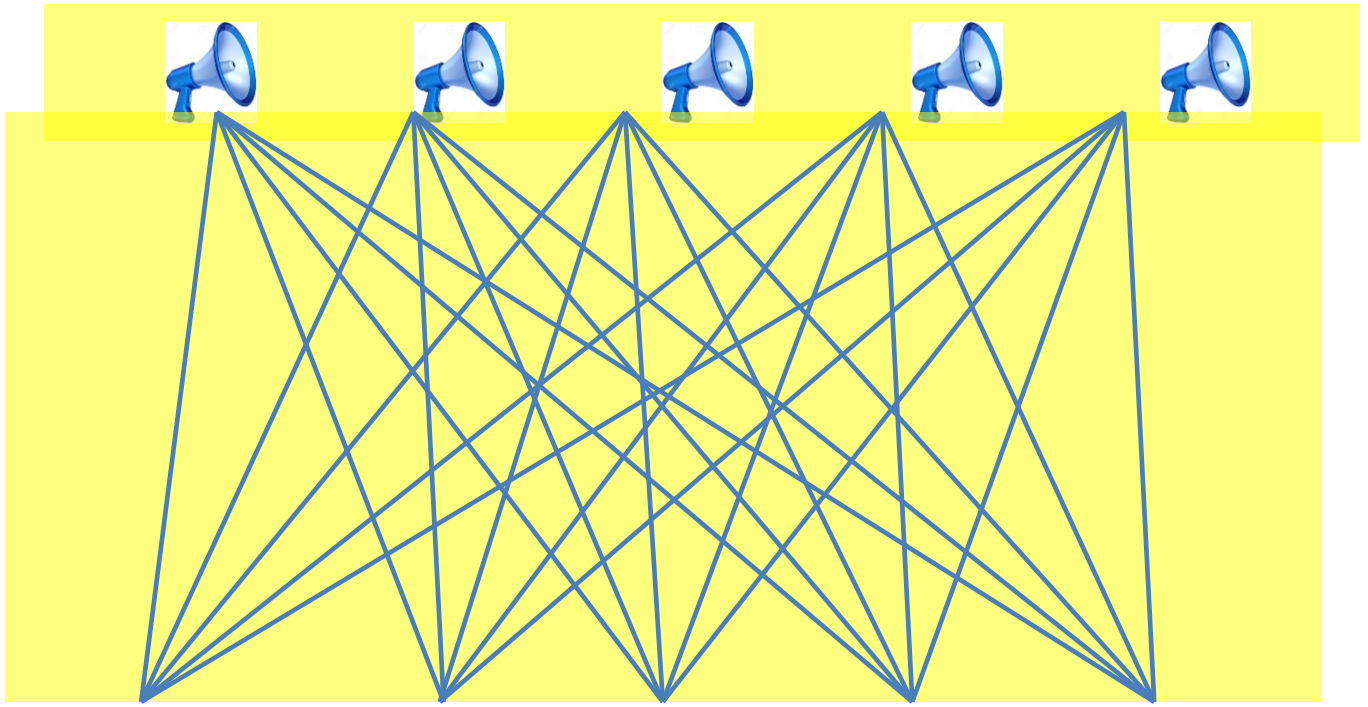
- Point-to-point model
  - Secure (private) channels between the parties (*Secure Message Transmission*)
- "Megaphone" model
  - Additional *broadcast channel*



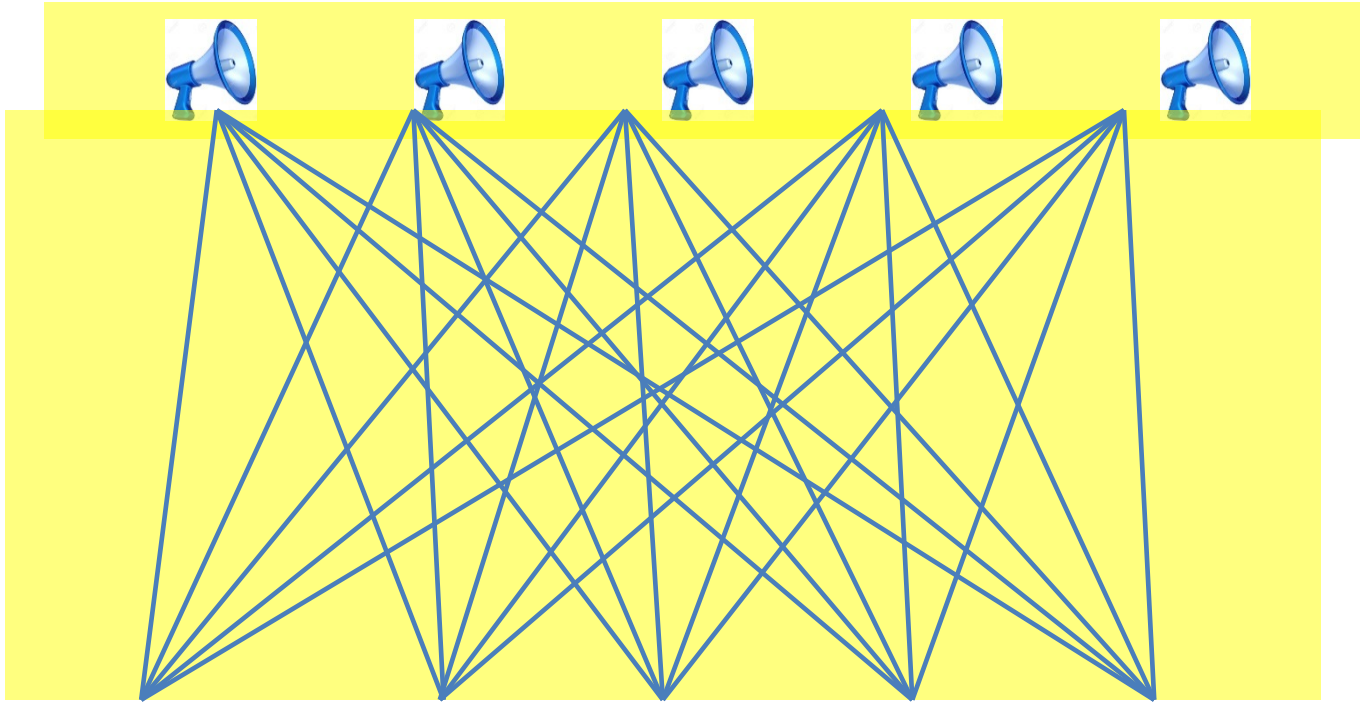
Protocols with Broadcast



Emulating Broadcast



Emulating Broadcast



- Expected constant round protocols
- $t \geq n/2$: $O(k)$ rounds, where $n = n/2 + k$

Dishonest Majority ($t \geq n/2$)

- *Fairness* cannot be achieved [Cle86]
- *Security with abort*
- Three flavors:
  - Identifiable abort
  - Unanimous abort
  - Selective (non-unanimous) abort

Two-Round MPC: State of the Art

- t < n: Unanimous abort using **broadcast** [BL18,GS18]
- t < n: Unanimous abort *cannot* be achieved using **p2p** [PR18]
- t < n/2: Selective abort using **p2p** [ACGJ19,ABT19]

Two-Round MPC: State of the Art

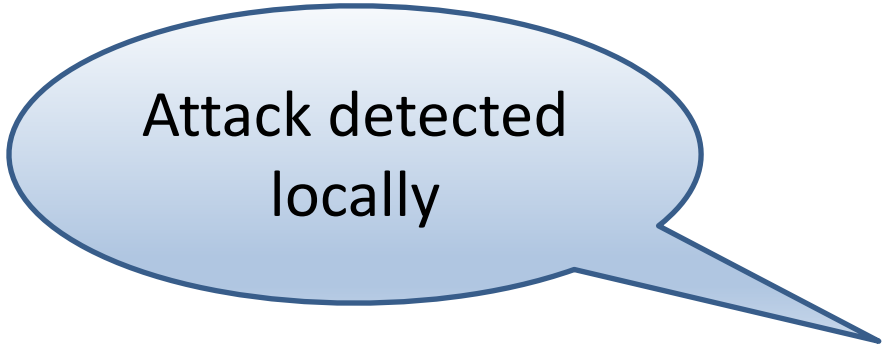
- t < n: Unanimous abort using **broadcast** [BL18,GS18]
- t < n: Unanimous abort *cannot* be achieved using **p2p** [PR18]
- t < n/2: Selective abort using **p2p** [ACGJ19,ABT19]

What's the tradeoff between the use of broadcast and achievable security in two-round MPC?

Broadcast-Optimal 2-Round MPC ($t < n$)

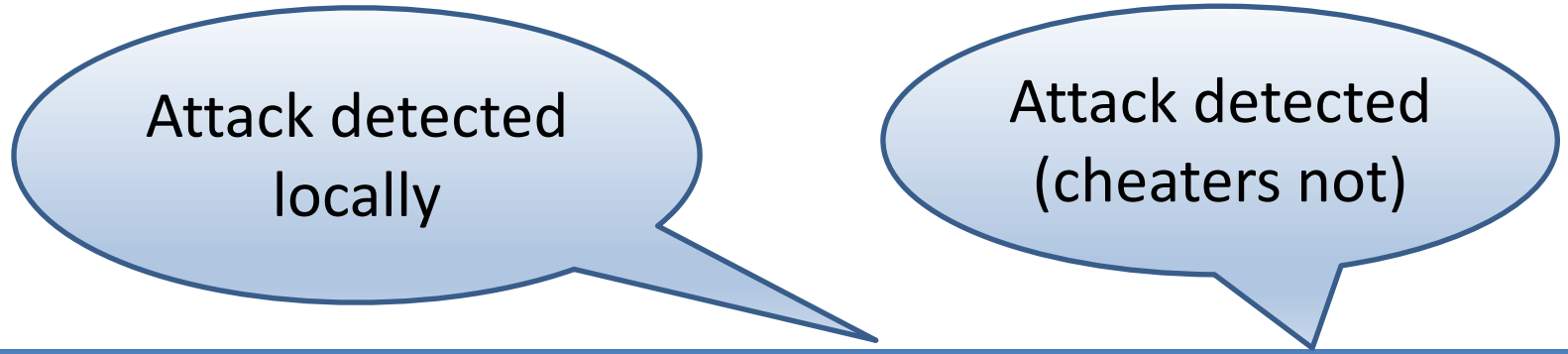
1st round	2nd round

Broadcast-Optimal 2-Round MPC ($t < n$)



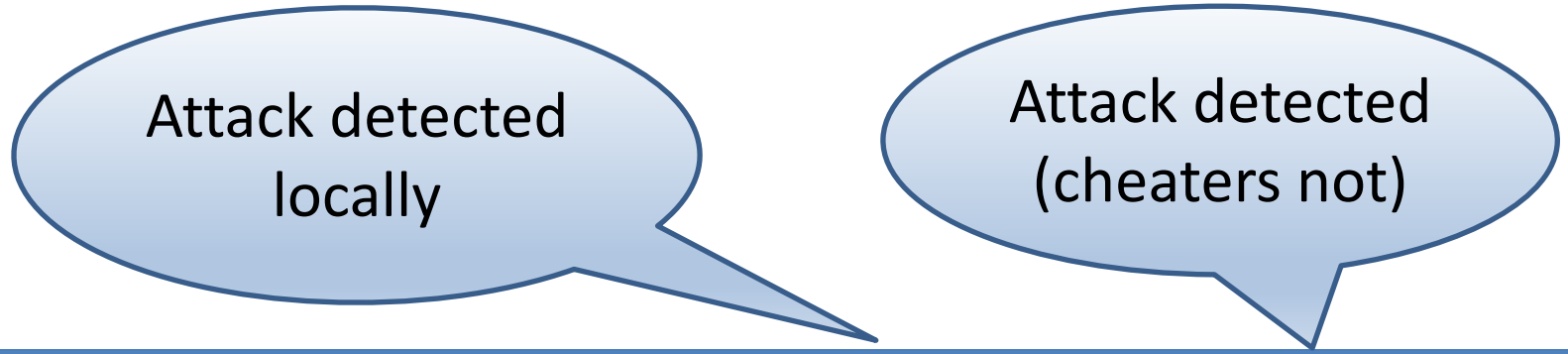
1st round	2nd round	Non-unanimous abort
P2P	P2P	✓

Broadcast-Optimal 2-Round MPC ($t < n$)



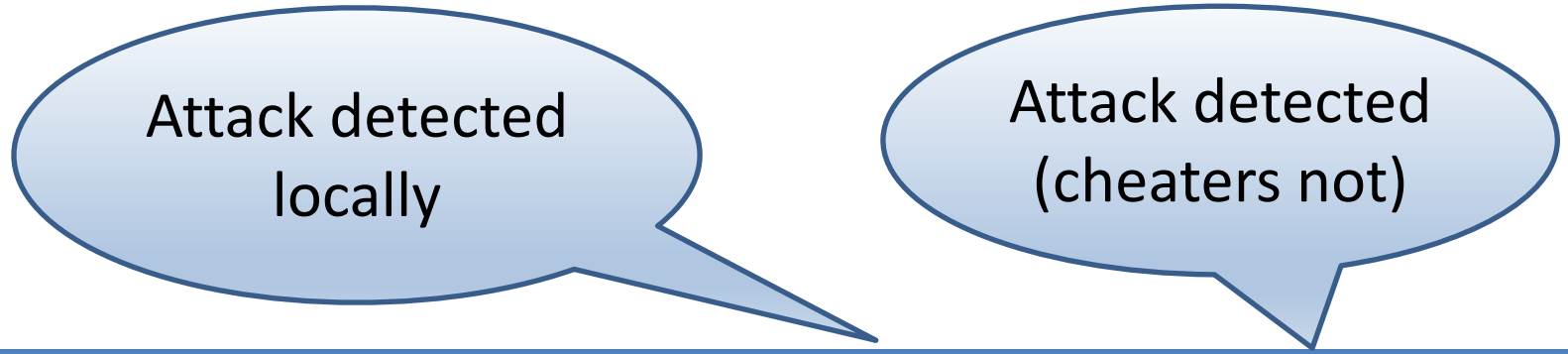
1st round	2nd round	Non-unanimous abort	Unanimous abort
P2P	P2P	✓	✗

Broadcast-Optimal 2-Round MPC ($t < n$)



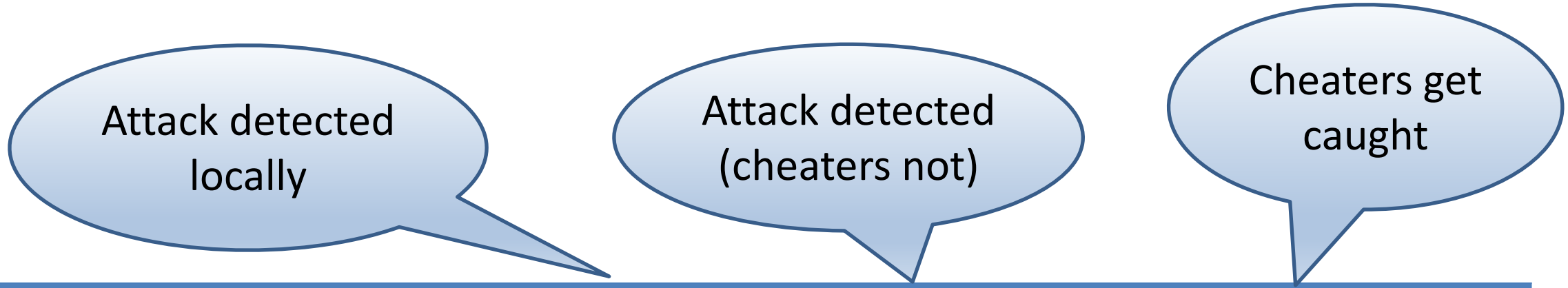
1st round	2nd round	Non-unanimous abort	Unanimous abort
P2P	P2P	✓	✗
BC	P2P	✓	✗

Broadcast-Optimal 2-Round MPC ($t < n$)



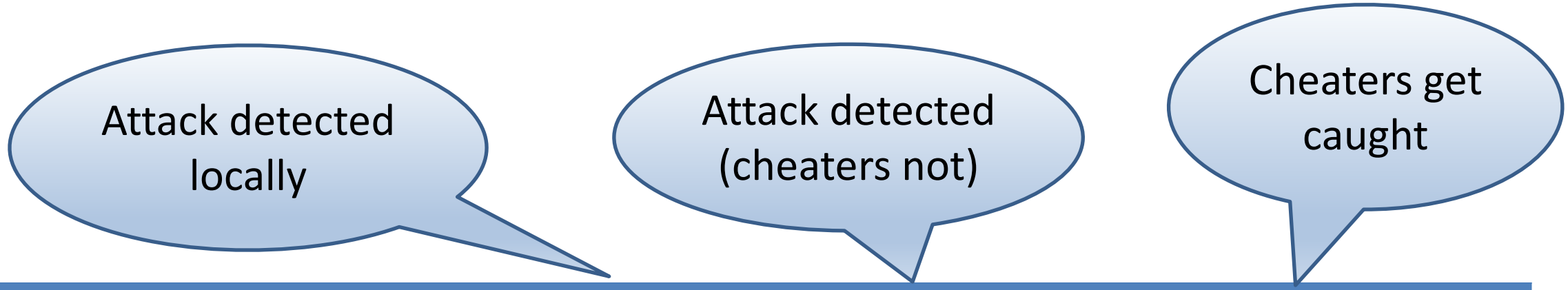
1st round	2nd round	Non-unanimous abort	Unanimous abort
P2P	P2P	✓	✗
BC	P2P	✓	✗
P2P	BC	✓	✓

Broadcast-Optimal 2-Round MPC ($t < n$)



1st round	2nd round	Non-unanimous abort	Unanimous abort	Identifiable abort
P2P	P2P	✓	✗	✗
BC	P2P	✓	✗	✗
P2P	BC	✓	✓	✗

Broadcast-Optimal 2-Round MPC ($t < n$)



1st round	2nd round	Non-unanimous abort	Unanimous abort	Identifiable abort
P2P	P2P	✓	✗	✗
BC	P2P	✓	✗	✗
P2P	BC	✓	✓	✗
BC	BC	✓	✓	✓

2-Round MPC: Do We Need a Megaphone?

Ran Cohen (Northeastern U. and BU)
Juan Garay (Texas A&M University)
Vassilis Zikas (U. of Edinburgh)