The Broadcast Message Complexity of Secure Multiparty Computation

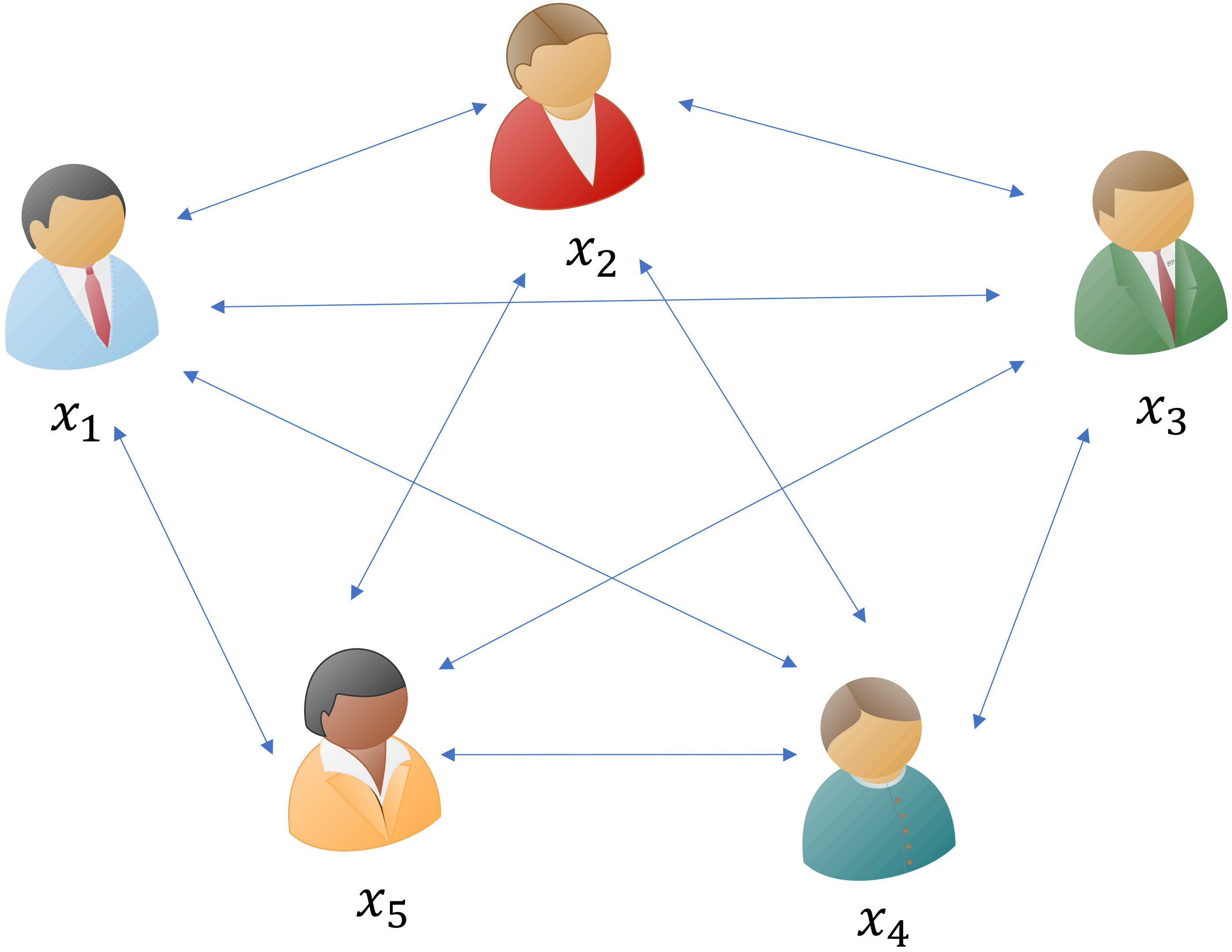
Sanjam Garg Aarushi Goel Abhishek Jain

Berkeley
NEVER EXPOSE THE WRONGDOING OF THE
UNIVERSITY OF CALIFORNIA

JOHNS HOPKINS
UNIVERSITY

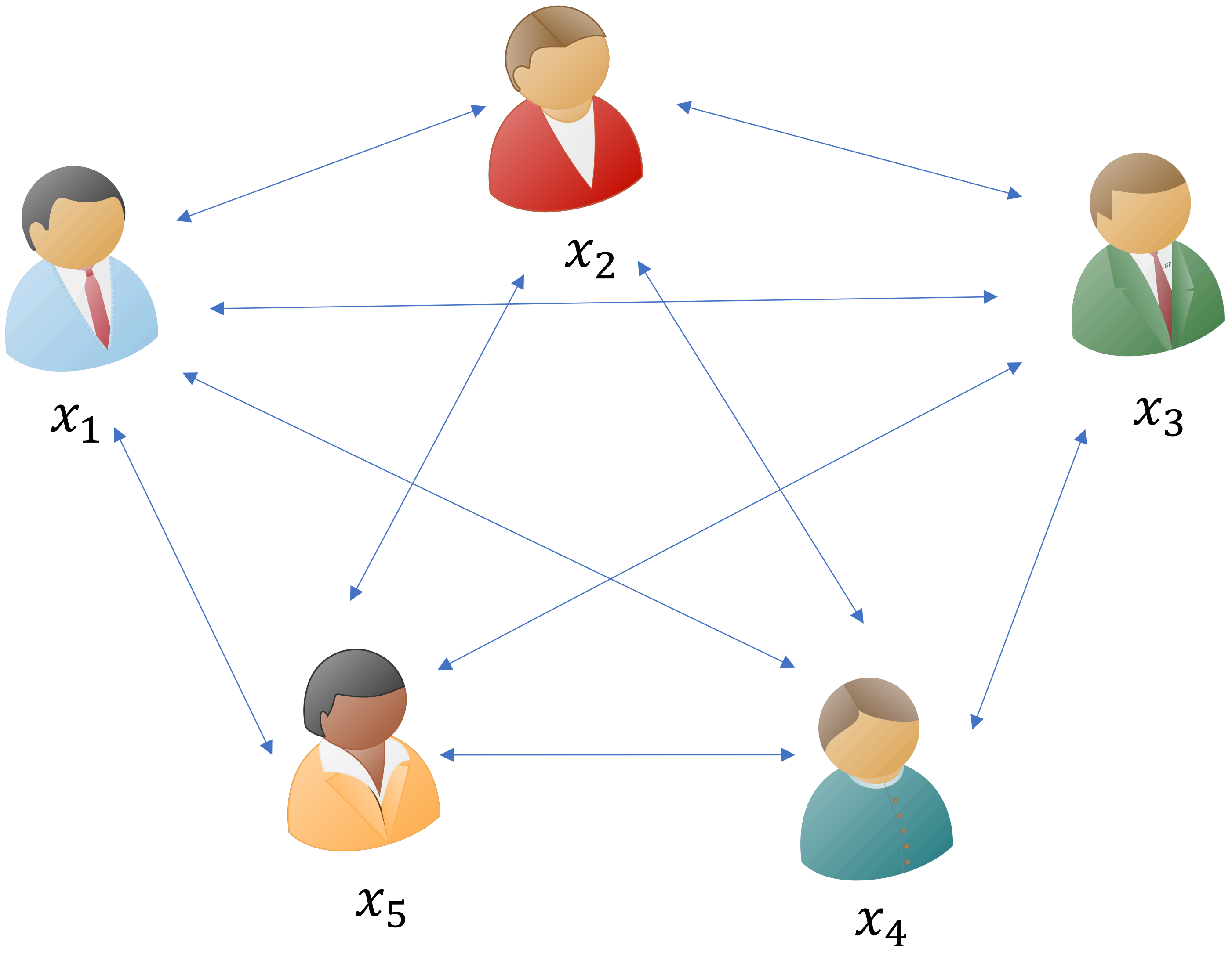
ASIACRYPT 2019

Secure Multiparty Computation



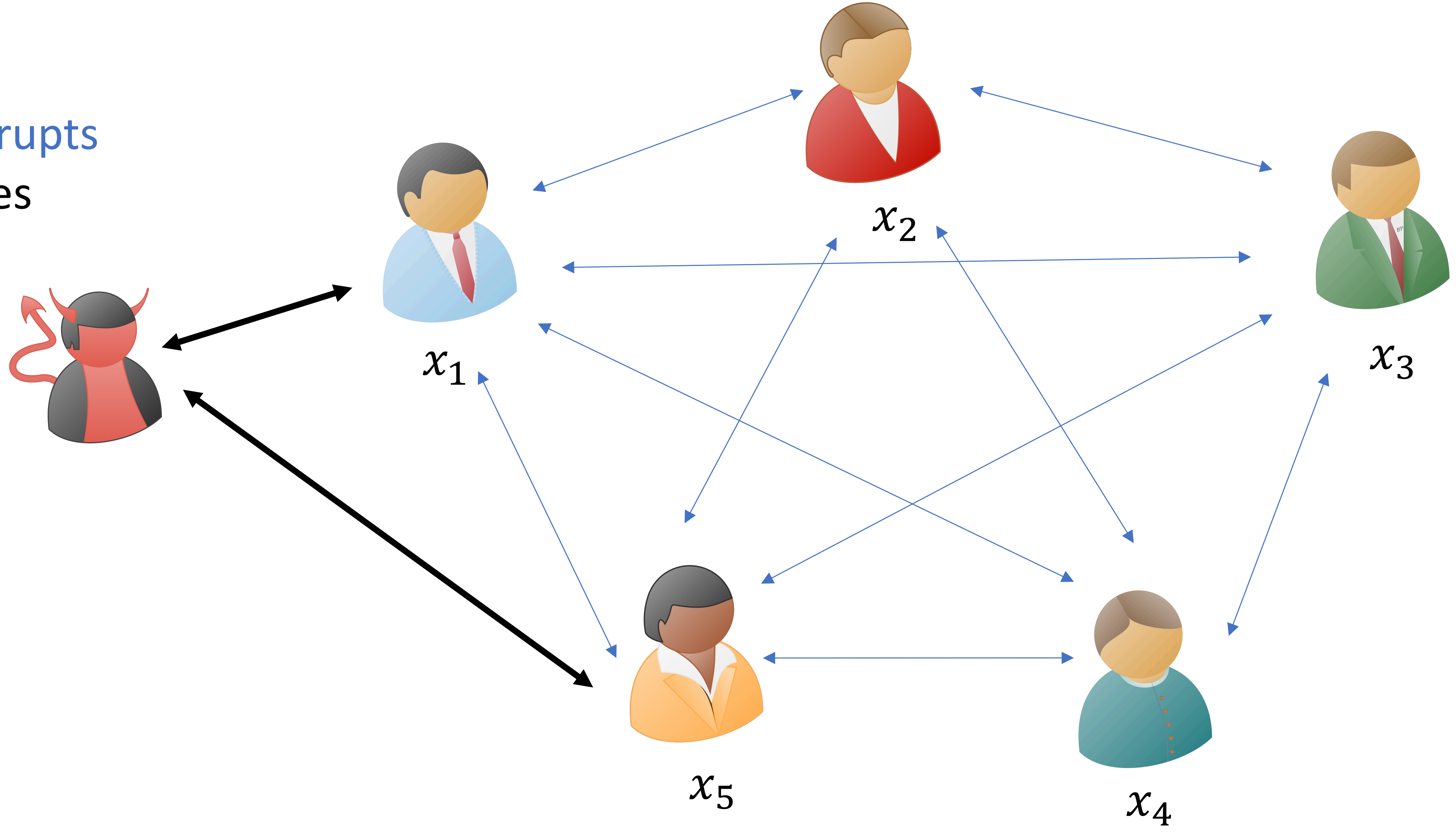
Secure Multiparty Computation

Compute
$f(x_1, x_2, x_3, x_4, x_5)$



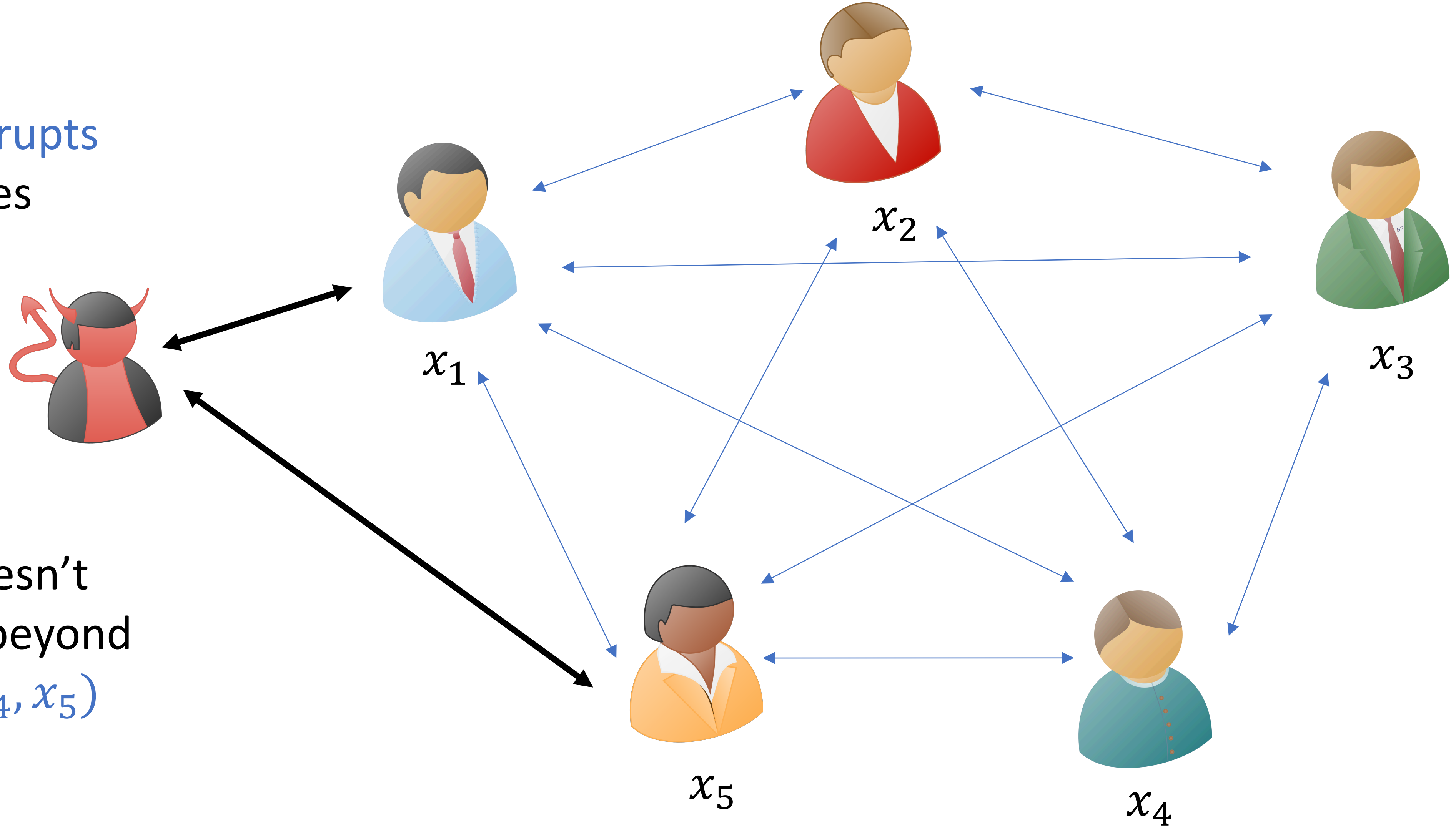
Secure Multiparty Computation

Adversary corrupts
t< n parties



Secure Multiparty Computation

Adversary corrupts
t< n parties



Adversary doesn't
learn anything beyond
$f(x_1, x_2, x_3, x_4, x_5)$

Communication Models

- Point to Point (P2P) Model
- Broadcast Model
- Hybrid Model (P2P + Broadcast)

Communication Models

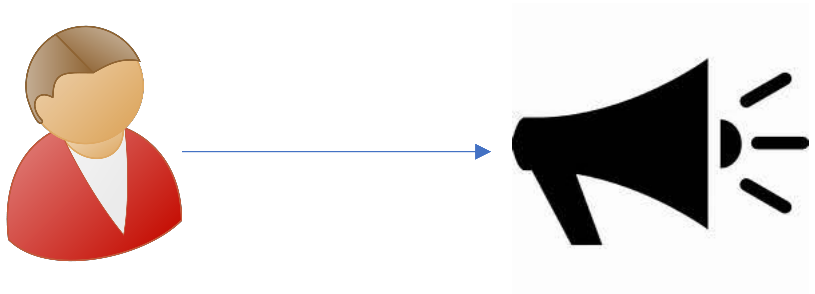
- Point to Point (P2P) Model
- Broadcast Model
- Hybrid Model (P2P + Broadcast)

Communication Model: Broadcast Model

Communication Model: Broadcast Model

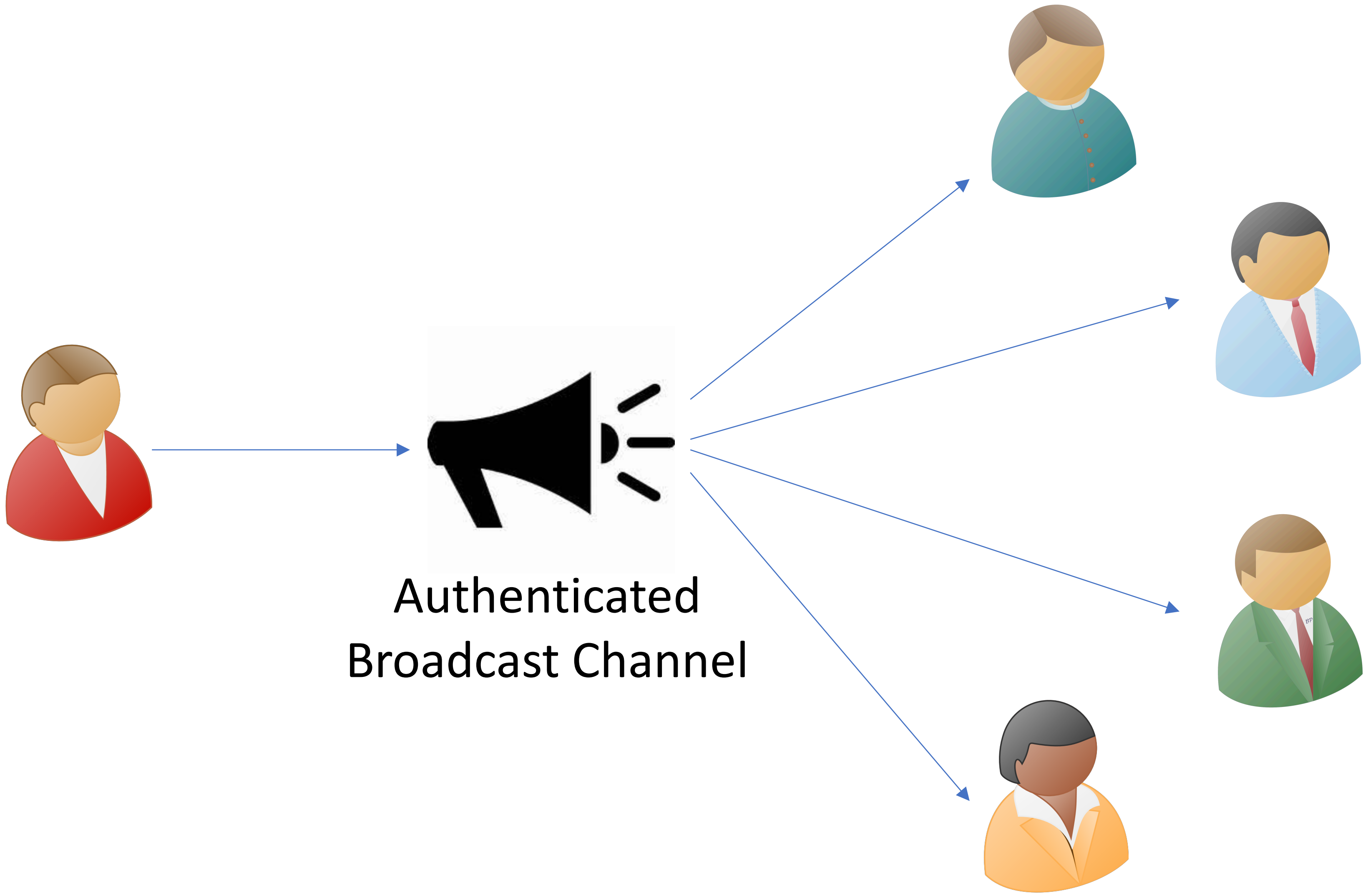
Authenticated
Broadcast Channel

Communication Model: Broadcast Model



Authenticated
Broadcast Channel

Communication Model: Broadcast Model

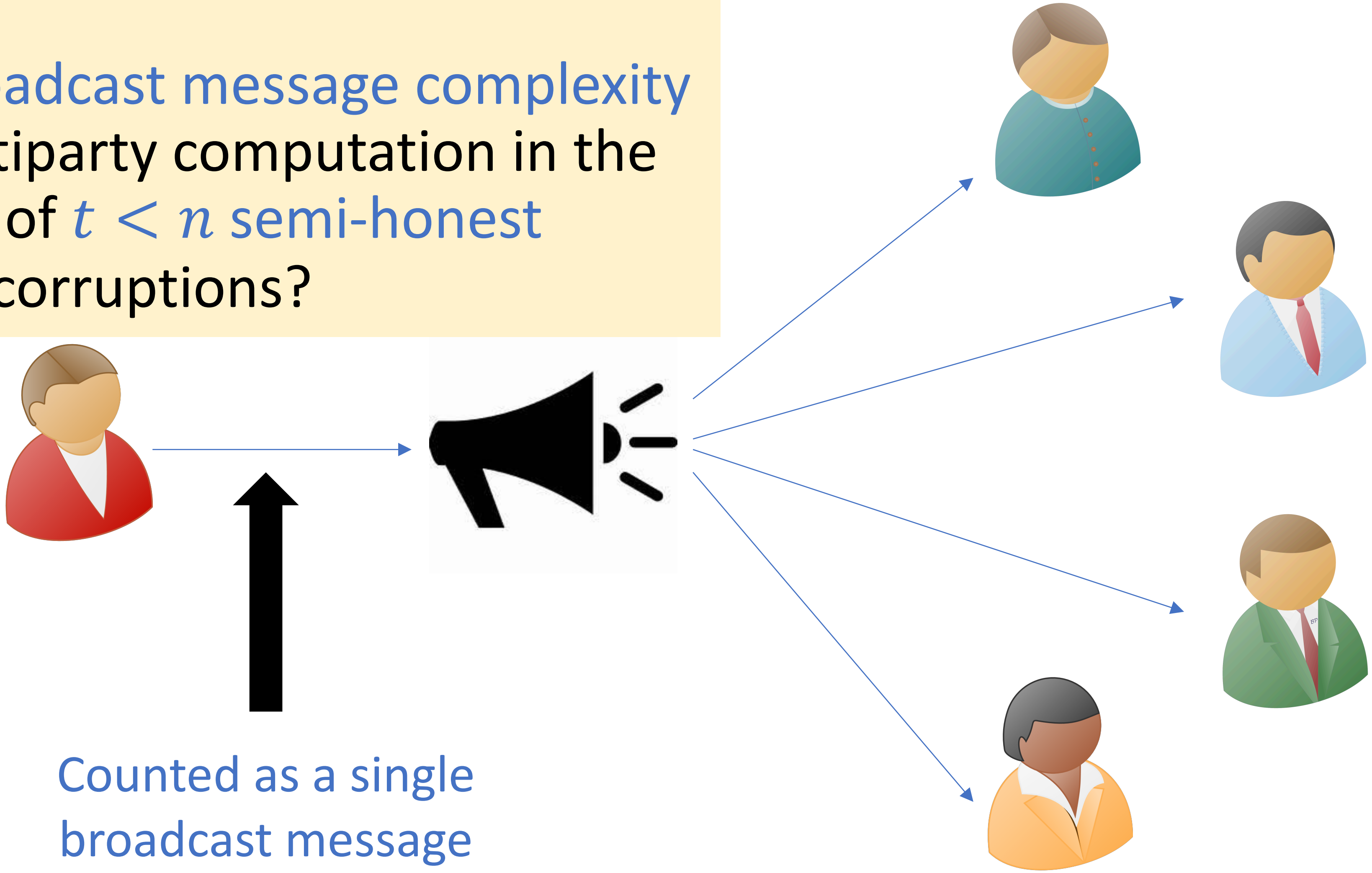


Problem Statement

What is the broadcast message complexity of secure multiparty computation in the presence of $t < n$ semi-honest corruptions?

Problem Statement

What is the broadcast message complexity of secure multiparty computation in the presence of $t < n$ semi-honest corruptions?



Related Work: P2P Message Complexity

$t = n - 1$ [Ishai, Mittal, Ostrovsky 18]

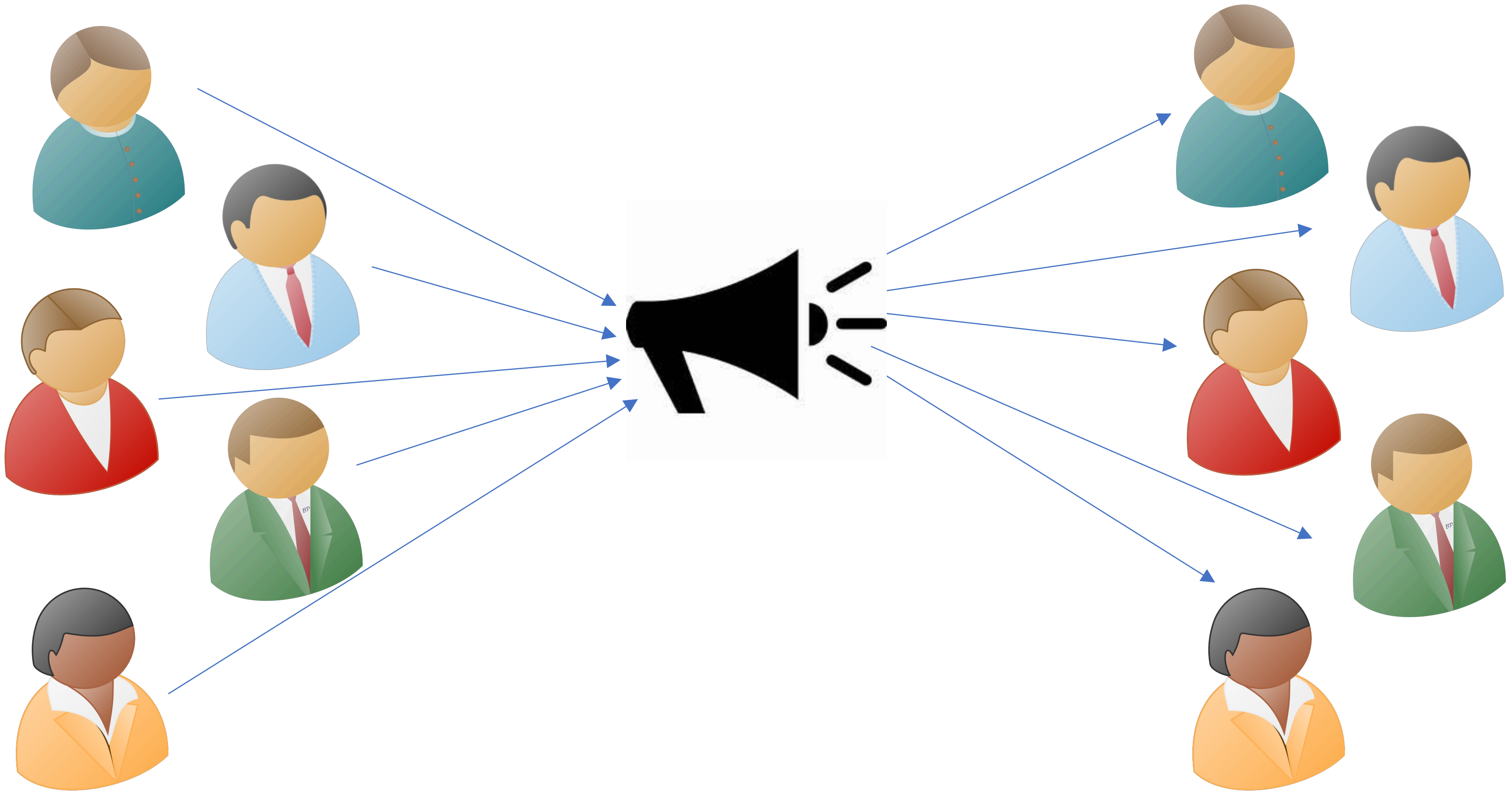
$t < n$ [Mittal 18]

Simultaneous Broadcast Model

Every party
broadcasts a message
in each round

Simultaneous Broadcast Model

Every party broadcasts a message in each round



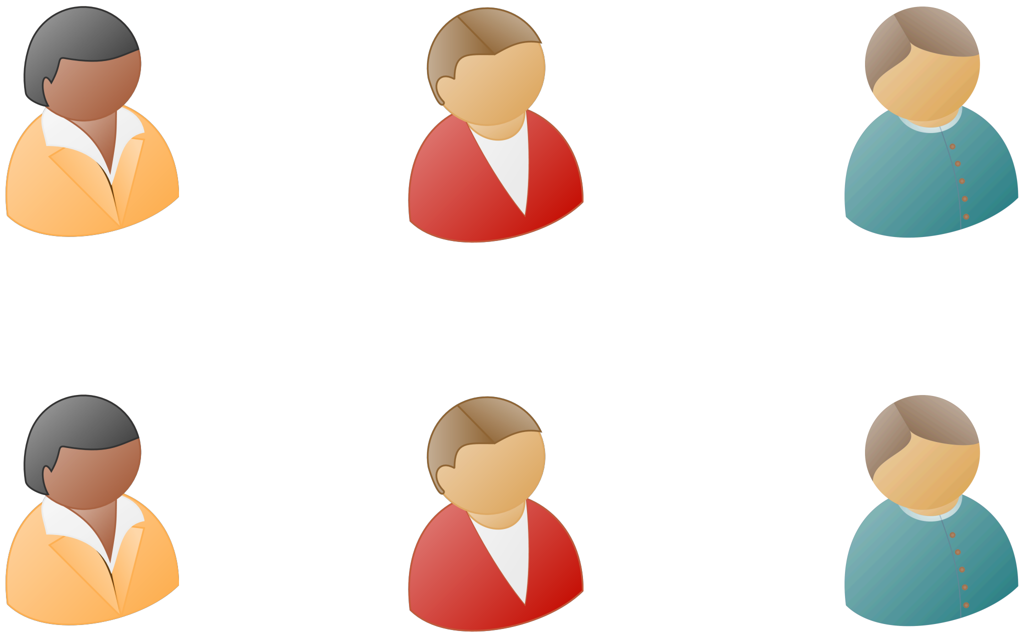
Simultaneous Broadcast Model

2 rounds are necessary for semi-honest secure computation [HLP11].

Simultaneous Broadcast Model

Round 1

Round 2

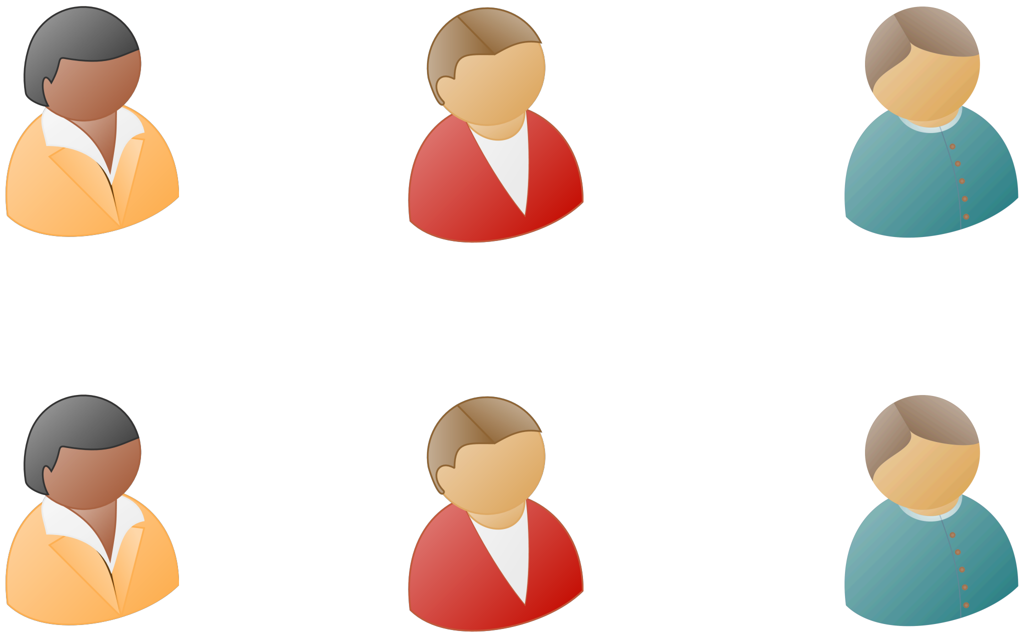


2 rounds are necessary for semi-honest secure computation [HLP11].

Simultaneous Broadcast Model

Round 1

Round 2



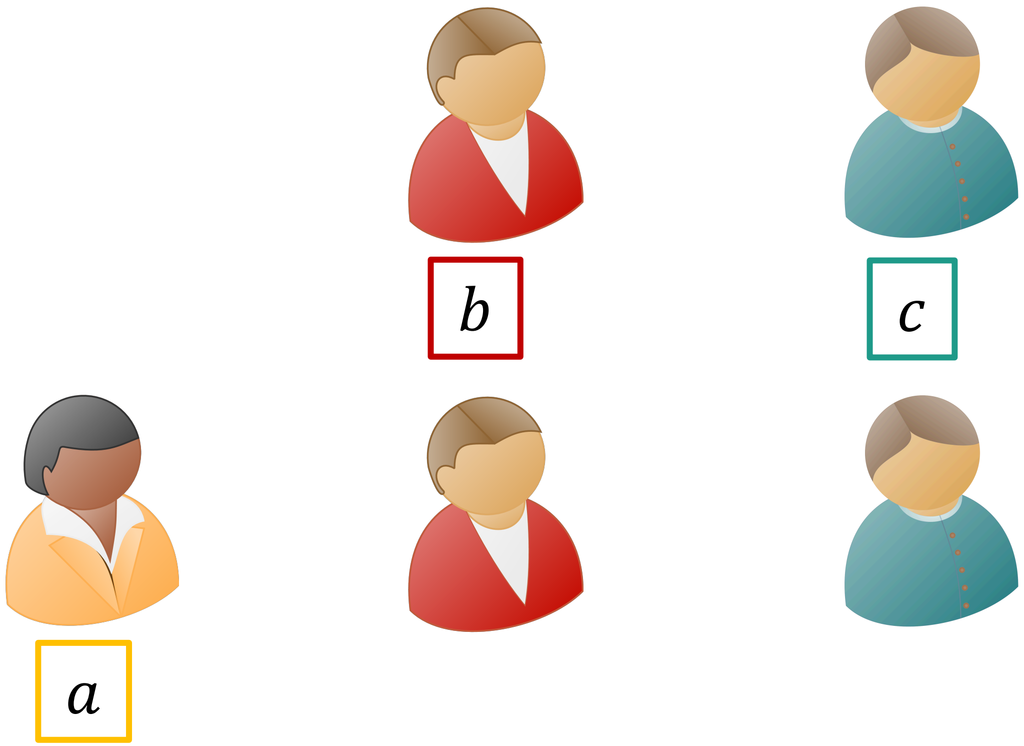
2 rounds are necessary for semi-honest secure computation.

Is the Broadcast Message Complexity $2n$?

Seems Inherent? (Scenario 1)

Round 1

Round 2

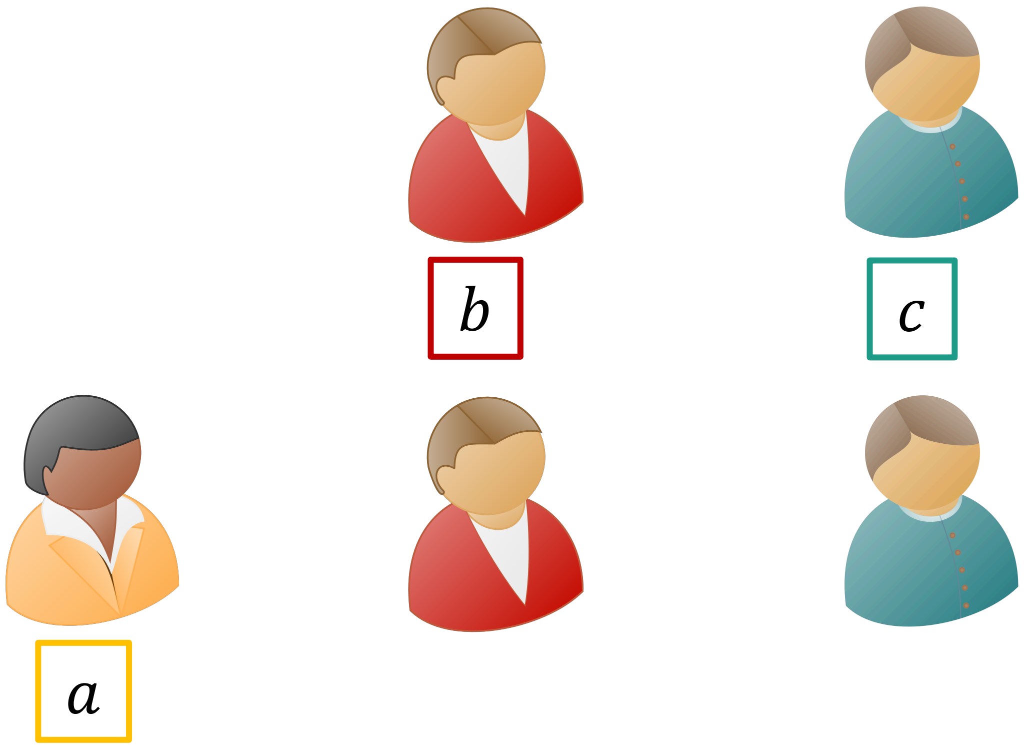


- Alice doesn't broadcast a message in the first round

Seems Inherent? (Scenario 1)

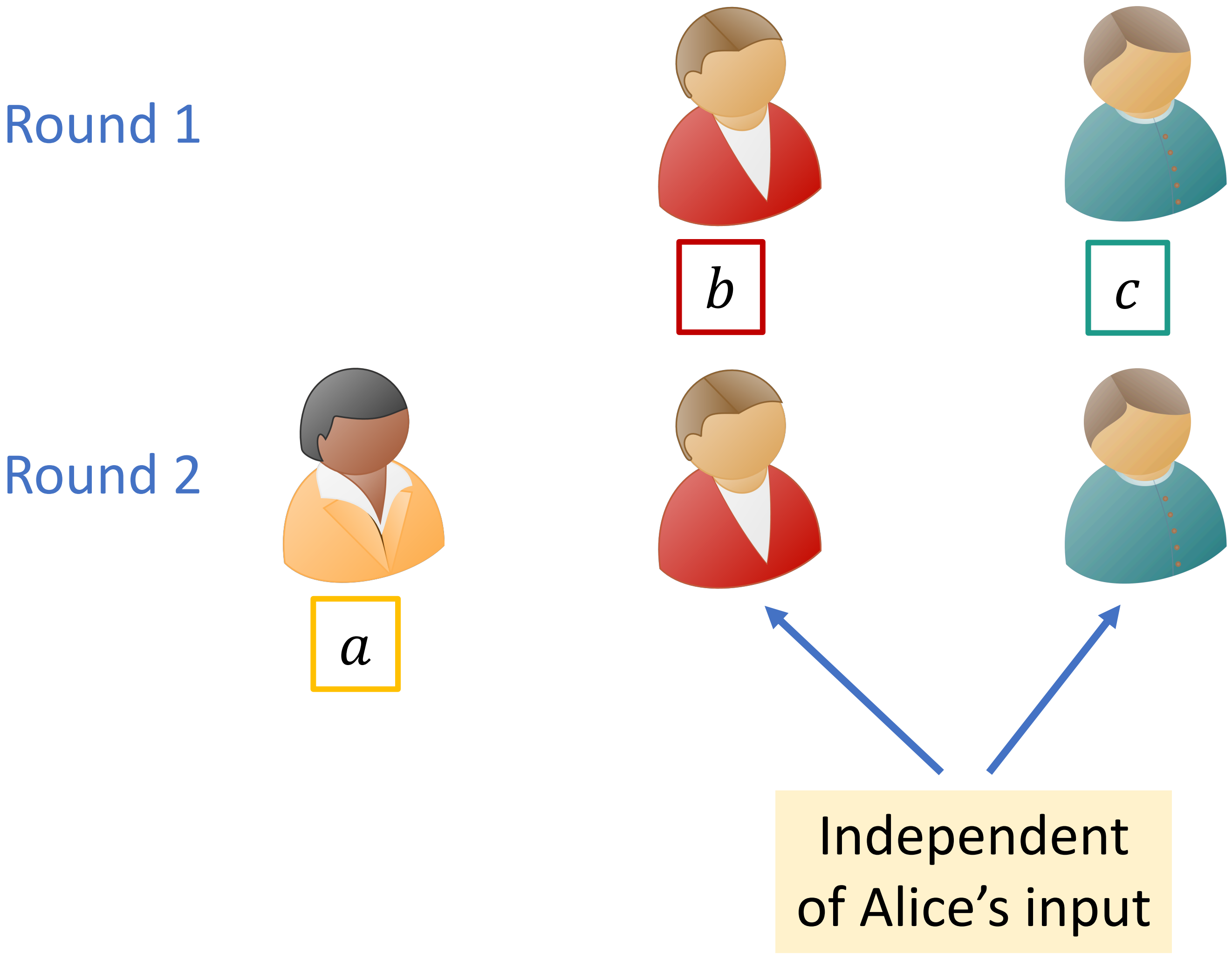
Round 1

Round 2



- Alice doesn't broadcast a message in the first round
- In a given round, honest parties broadcast messages at the same time.

Seems Inherent? (Scenario 1)

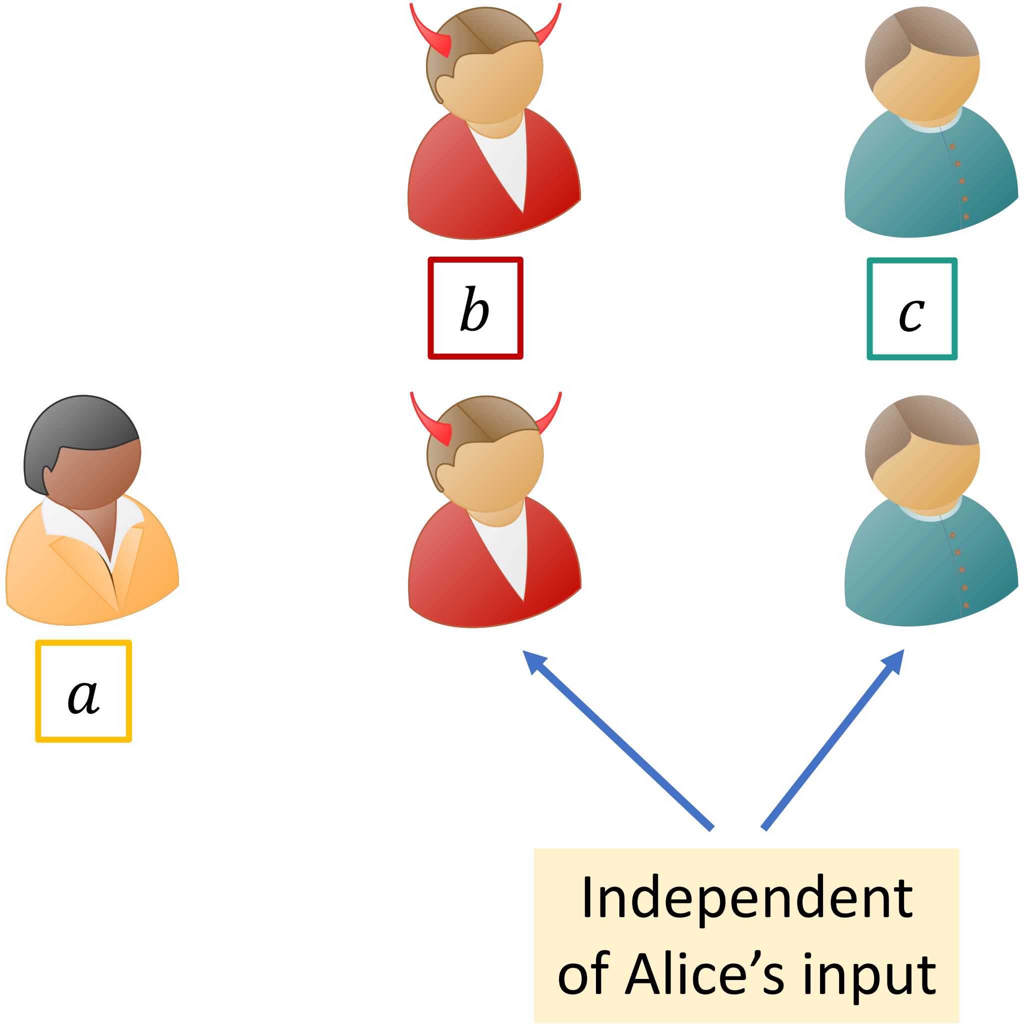


- Alice doesn't broadcast a message in the first round
- In a given round, honest parties broadcast messages at the same time.

Seems Inherent? (Scenario 1)

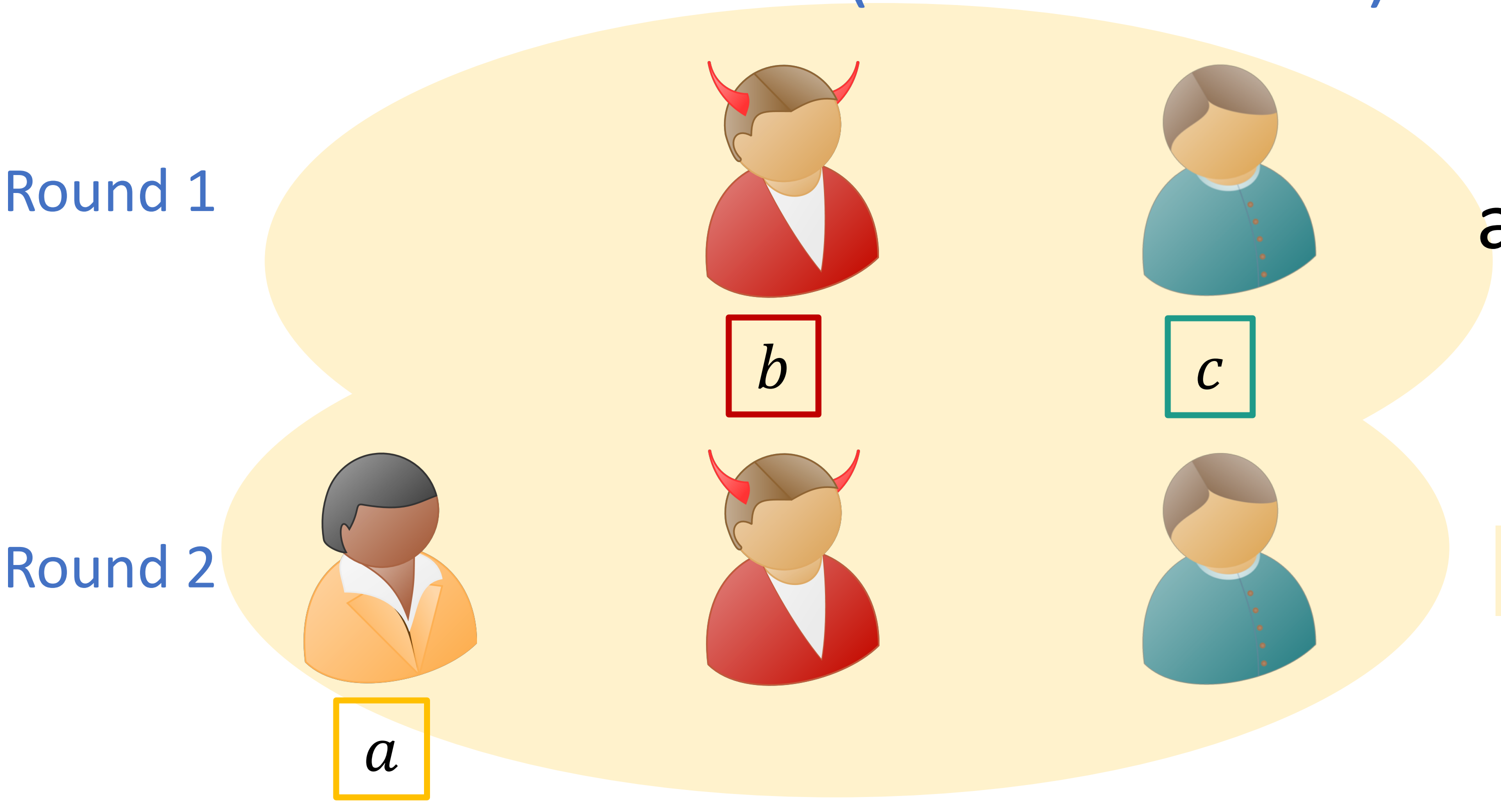
Round 1

Round 2



Corrupt Bob can launch an offline spoofing attack

Seems Inherent? (Scenario 1)



Corrupt Bob can launch an offline spoofing attack

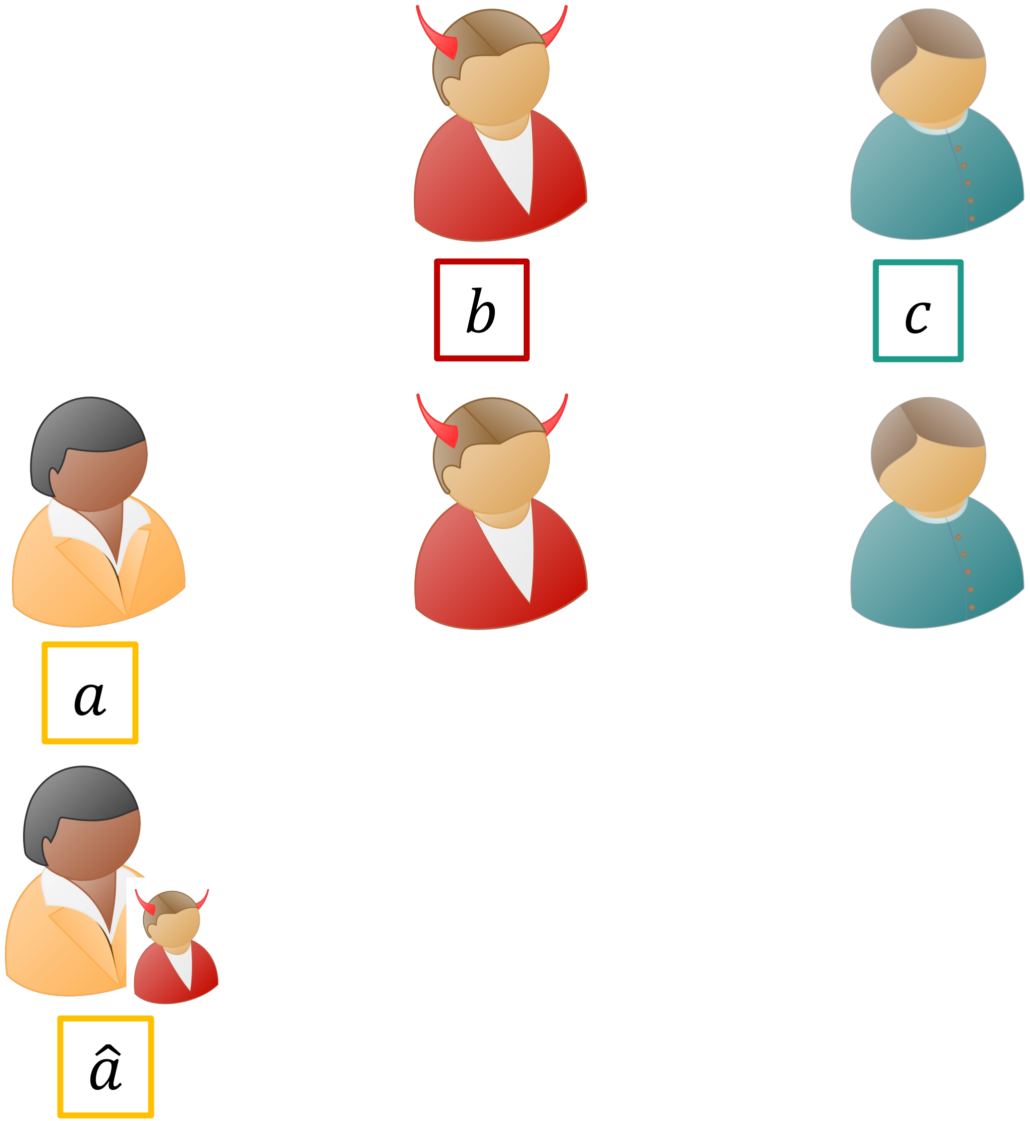
Output: $y = f(a, b, c)$

Seems Inherent? (Scenario 1)

Round 1

Round 2

Offline Computation



Corrupt Bob can launch an offline spoofing attack

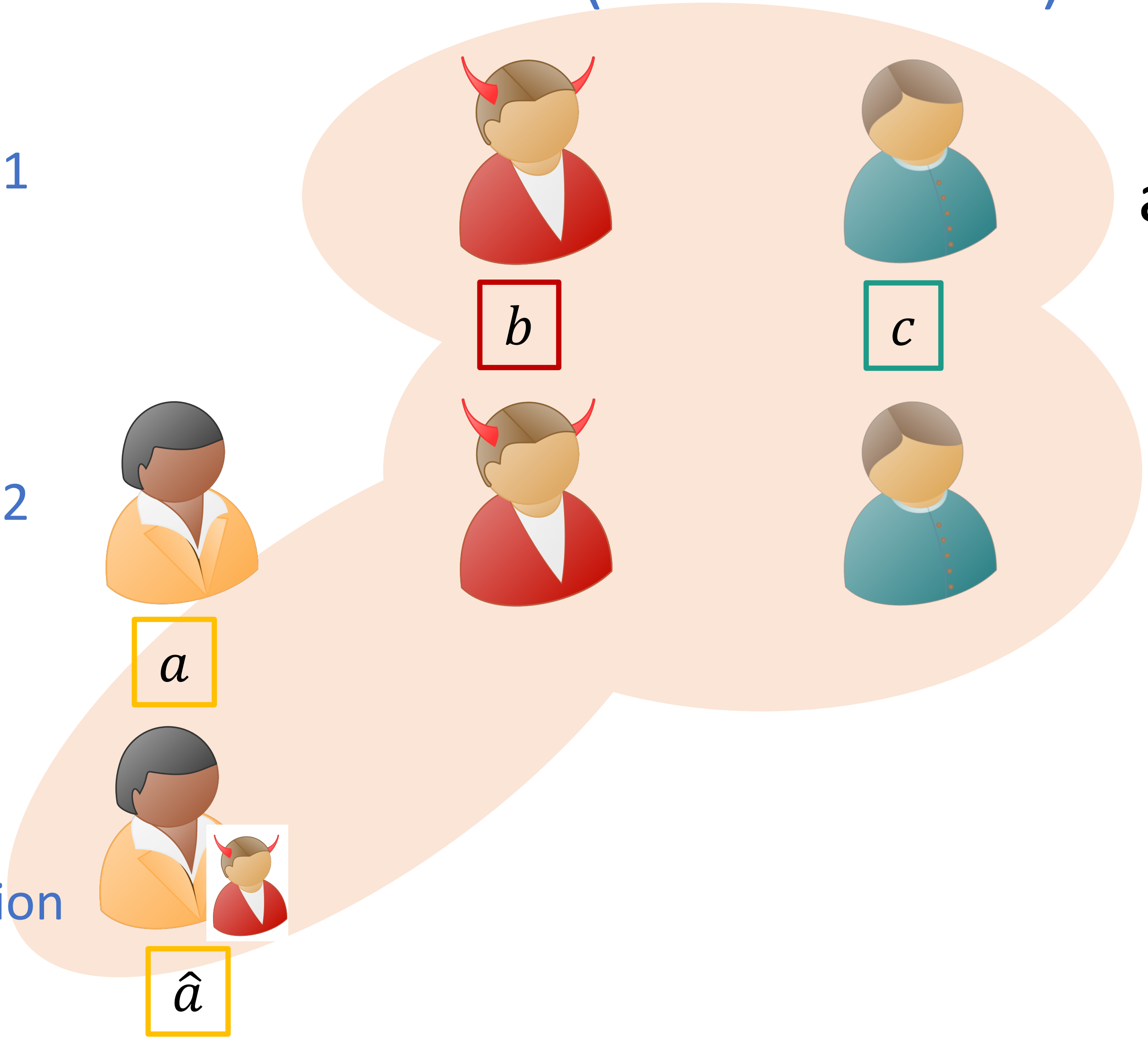
Output: $y = f(a, b, c)$

Seems Inherent? (Scenario 1)

Round 1

Round 2

Offline Computation

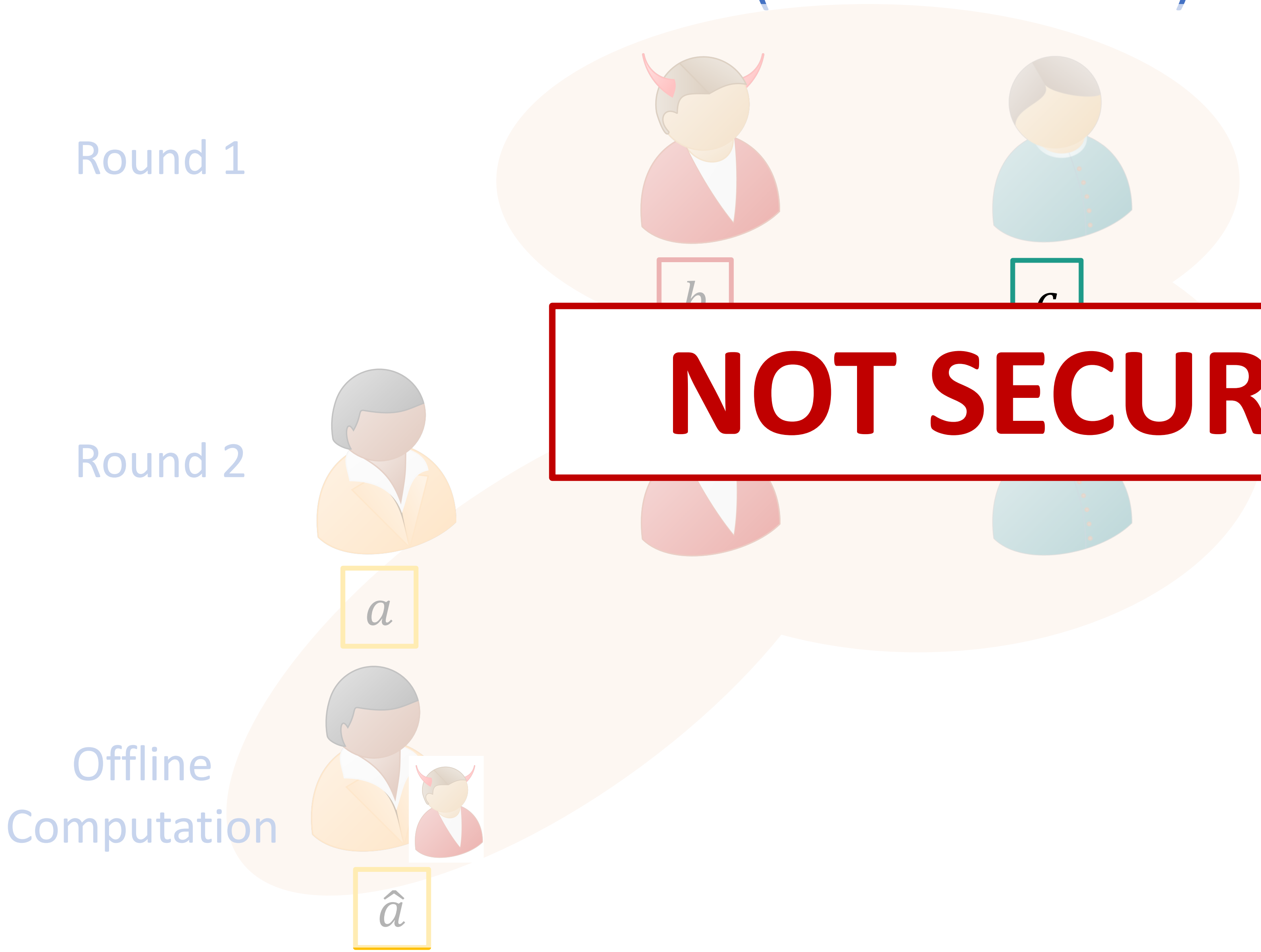


Corrupt Bob can launch an offline spoofing attack

Output: $y = f(a, b, c)$

Output: $\hat{y} = f(\hat{a}, b, c)$

Seems Inherent? (Scenario 1)



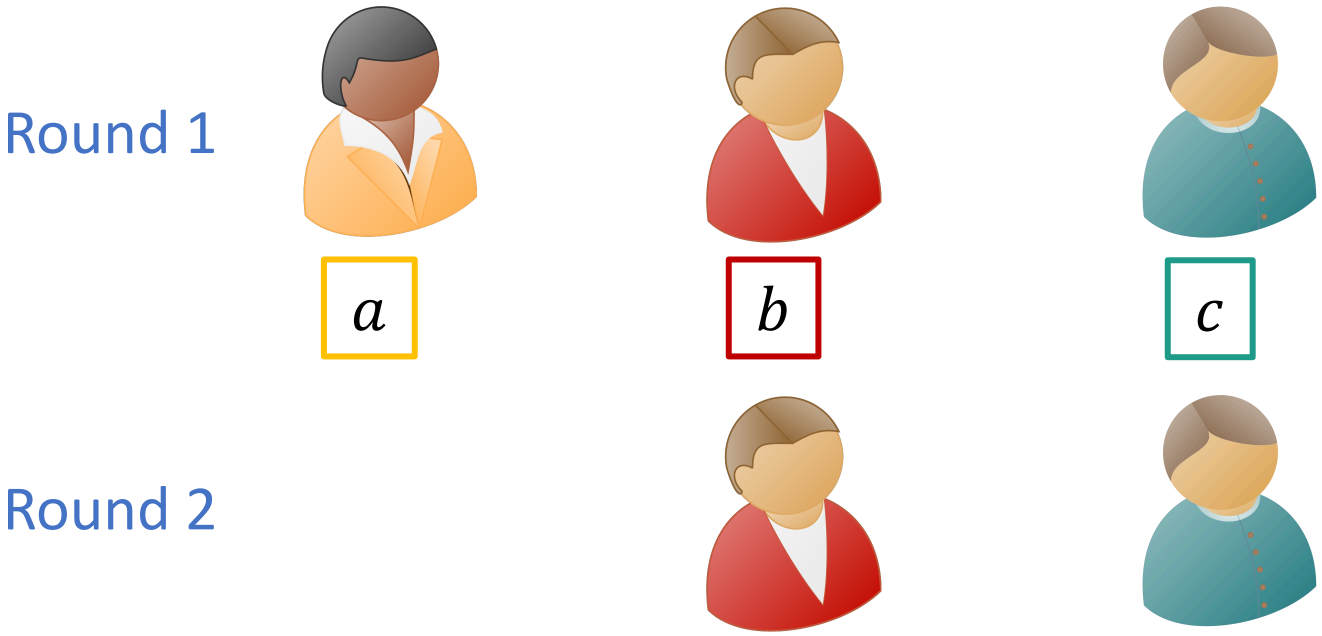
Corrupt Bob can launch an offline spoofing attack

NOT SECURE!!

Output: $y = f(a, b, c)$

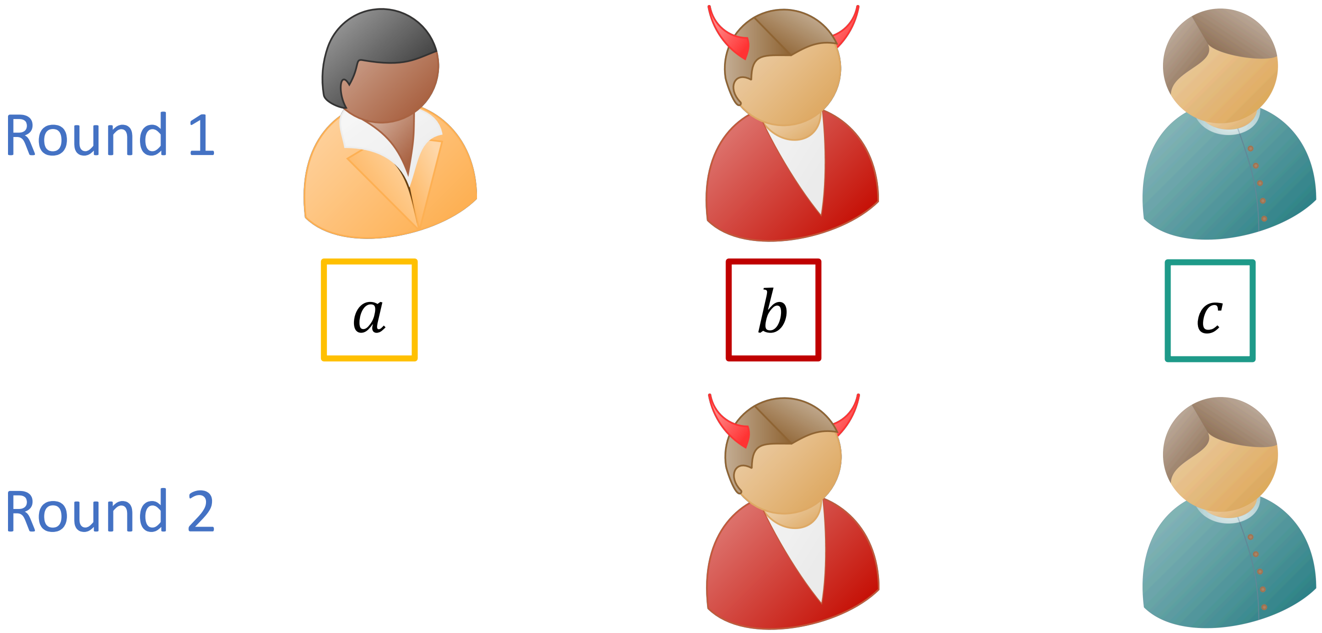
Output: $\hat{y} = f(\hat{a}, b, c)$

Seems Inherent? (Scenario 2)



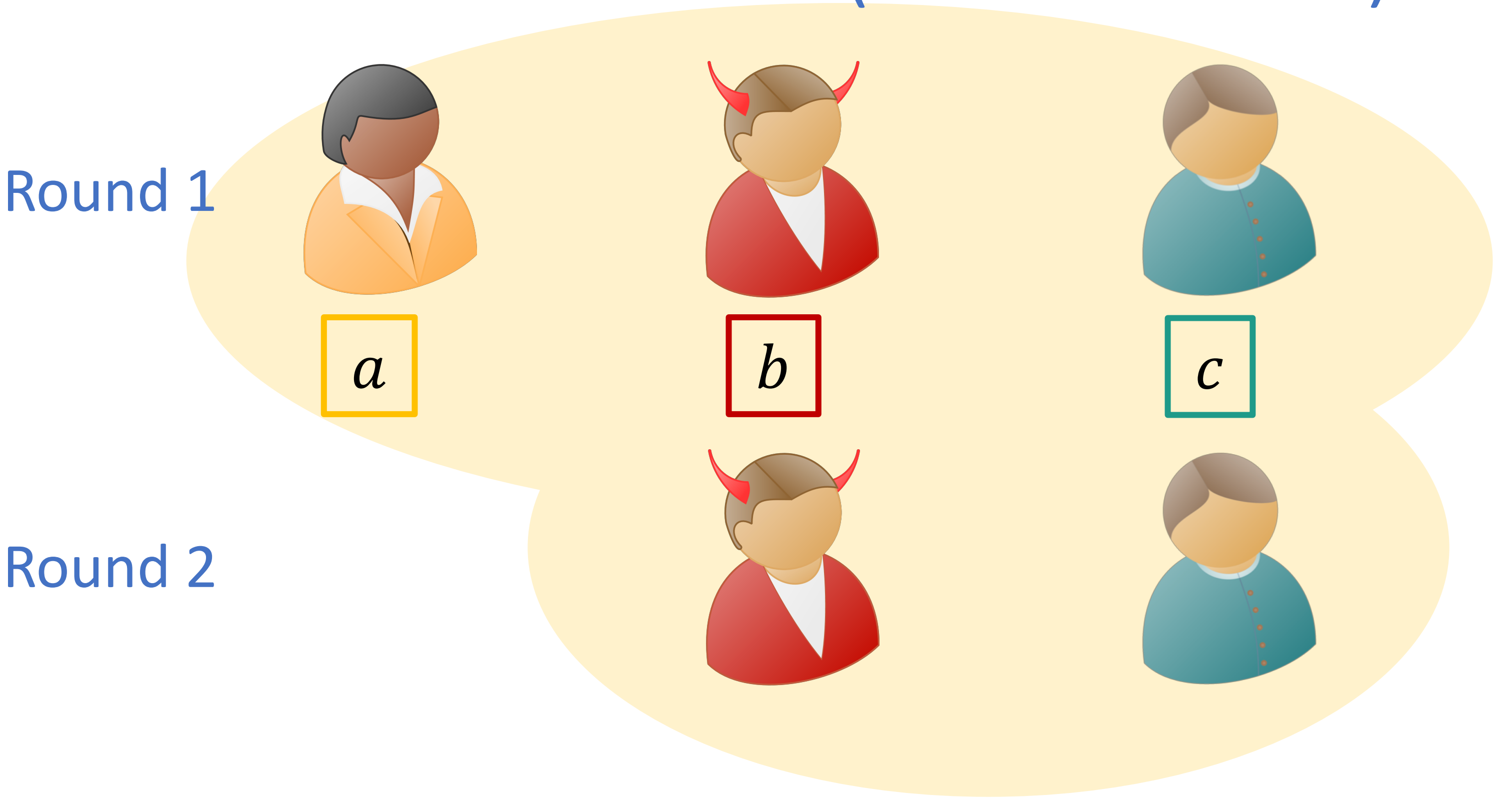
- Alice doesn’t broadcast a message in the second round

Seems Inherent? (Scenario 2)



Corrupt Bob can launch an offline residual function attack

Seems Inherent? (Scenario 2)

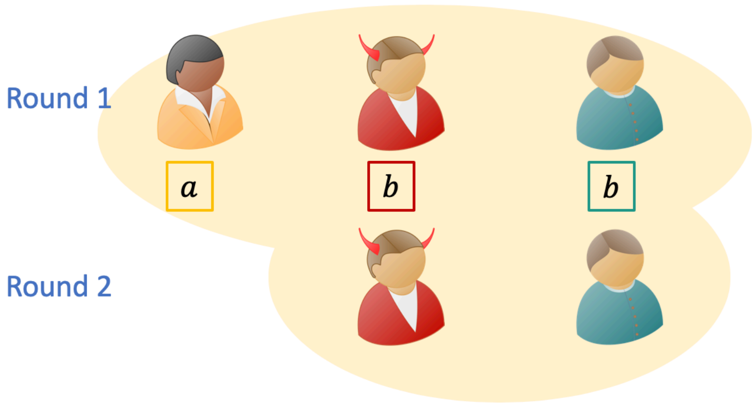


Corrupt Bob can launch an offline residual function attack

Output: $y = f(a, b, c)$

Seems Inherent? (Scenario 2)

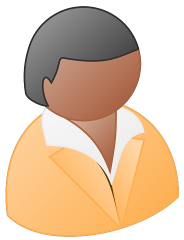
Corrupt Bob can launch an offline residual function attack



Output: $y = f(a, b, c)$

Seems Inherent? (Scenario 2)

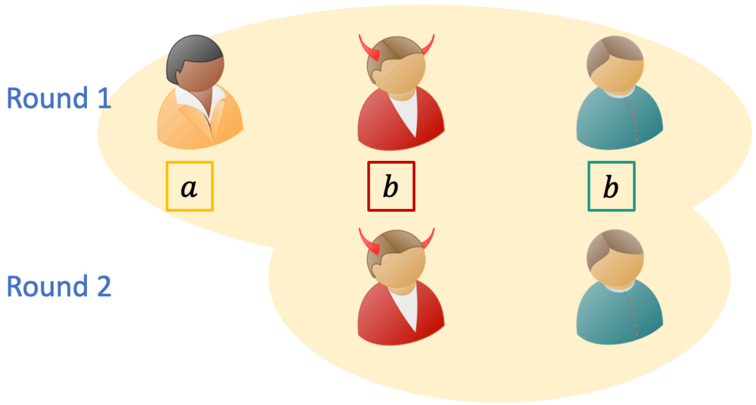
Offline Computation



a

Offline Computation

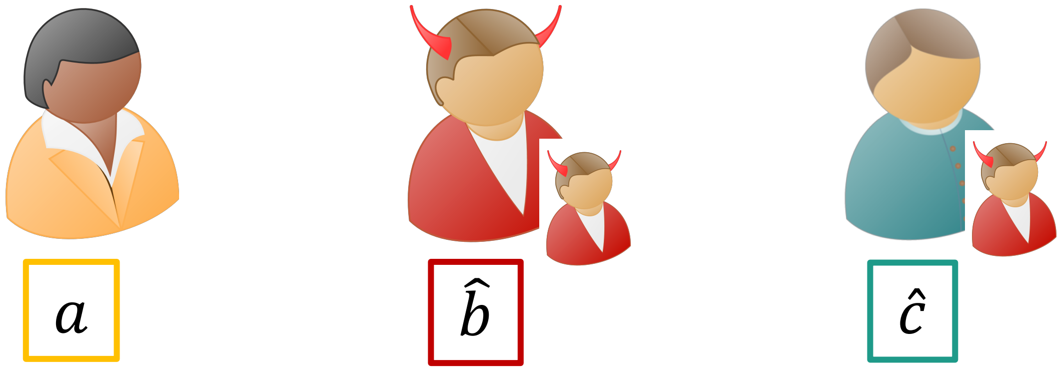
Corrupt Bob can launch an offline residual function attack



Output: $y = f(a, b, c)$

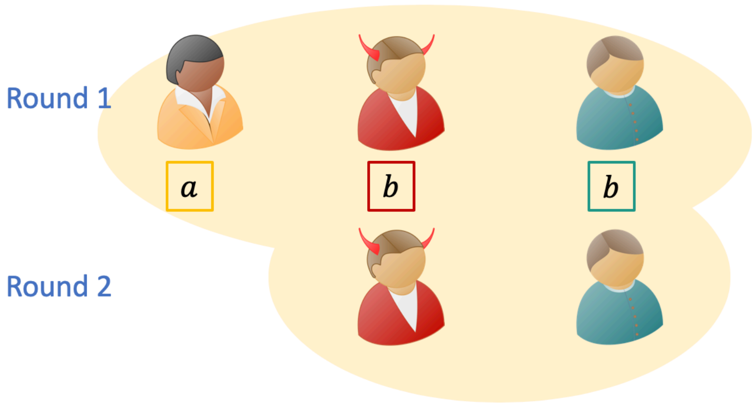
Seems Inherent? (Scenario 2)

Offline Computation



Corrupt Bob can launch an offline residual function attack

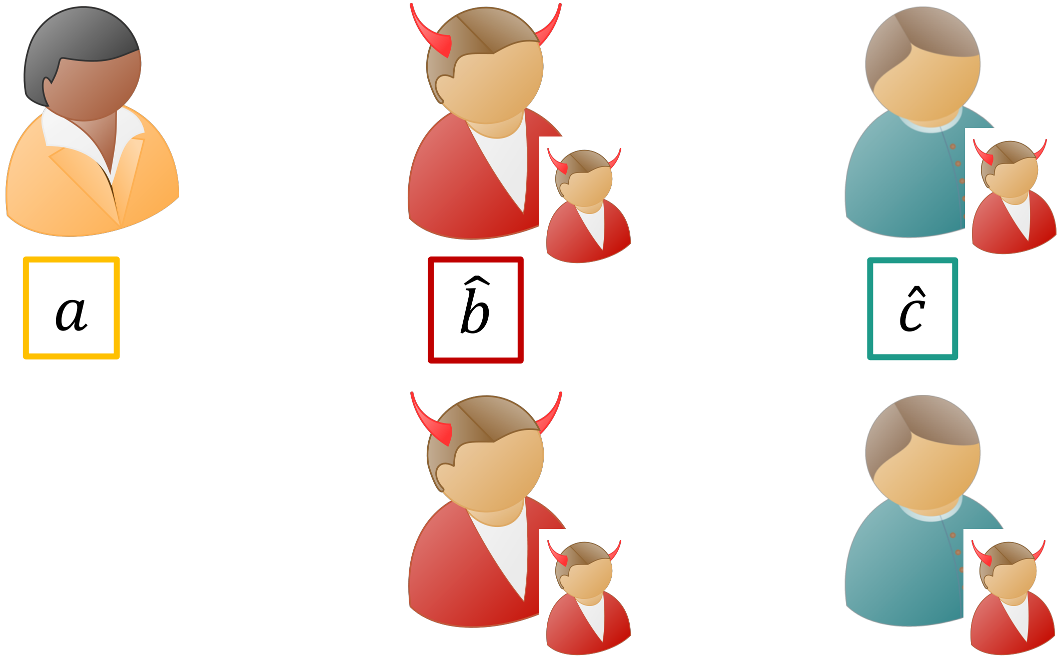
Offline Computation



Output: $y = f(a, b, c)$

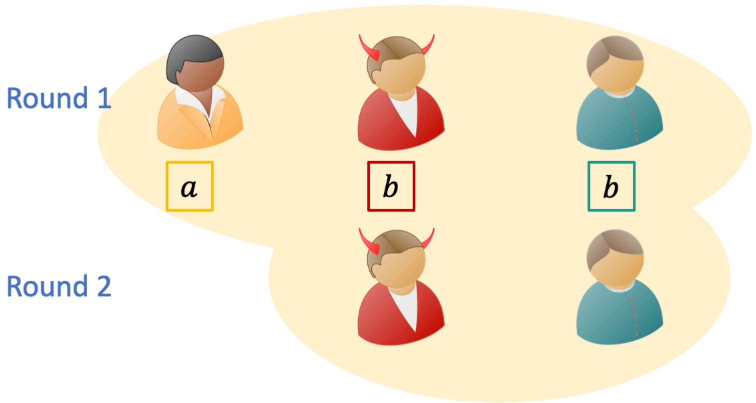
Seems Inherent? (Scenario 2)

Offline Computation



Offline Computation

Corrupt Bob can launch an offline residual function attack

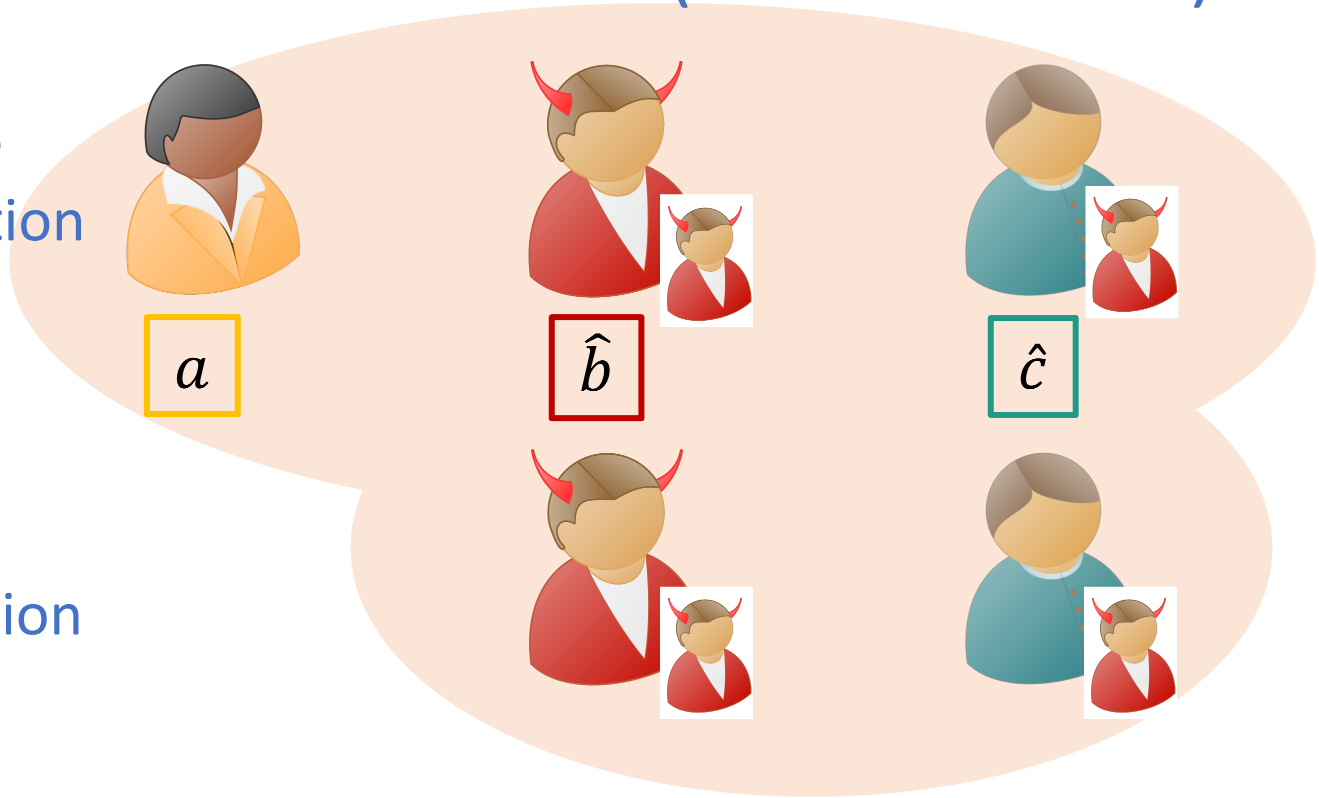


Output: $y = f(a, b, c)$

Seems Inherent? (Scenario 2)

Offline Computation

Offline Computation

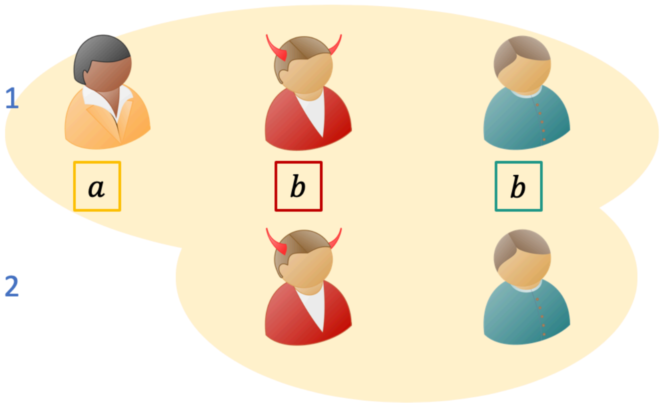


Output: $y = f(a, \hat{b}, c)$

Corrupt Bob can launch an offline residual function attack

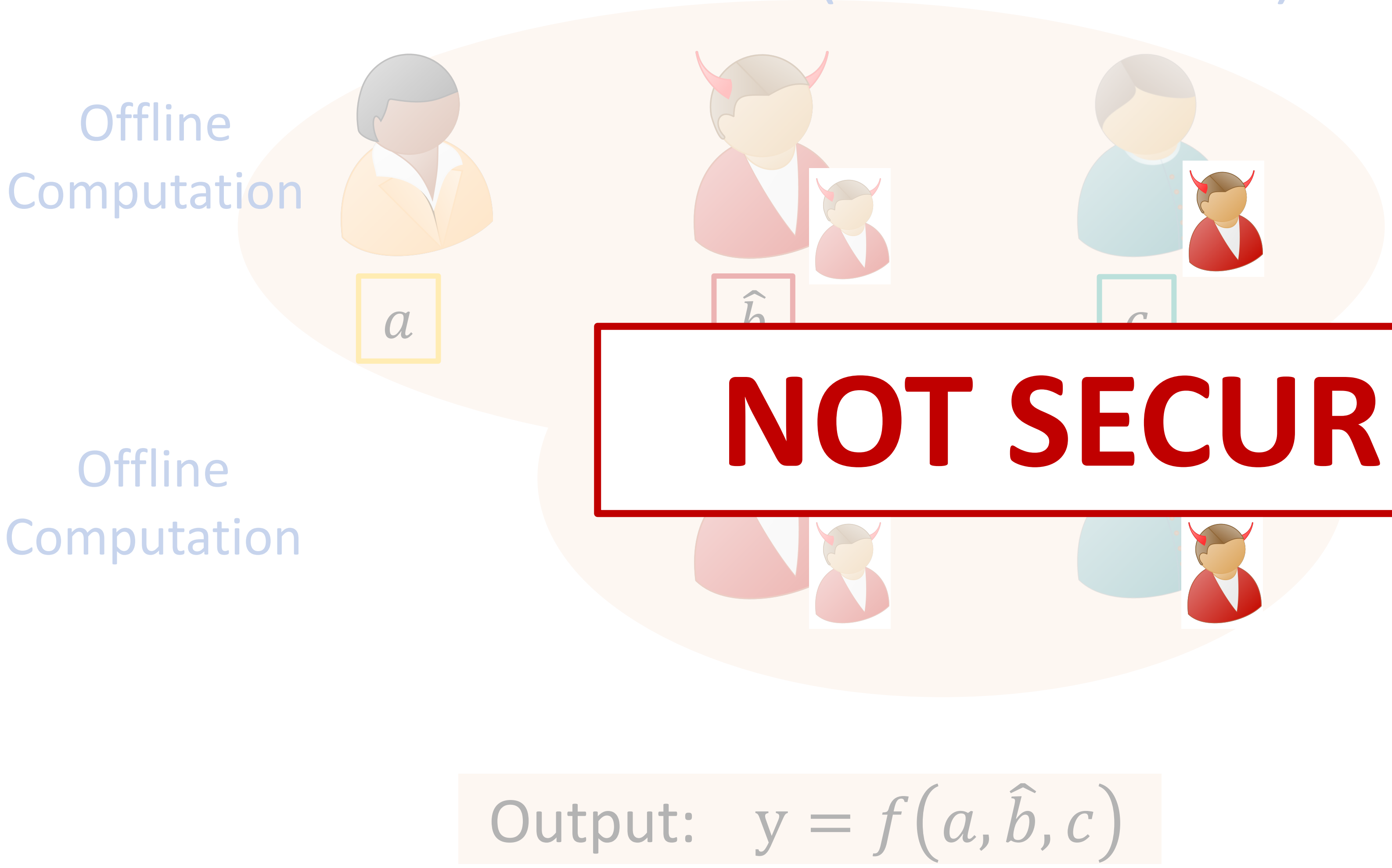
Round 1

Round 2



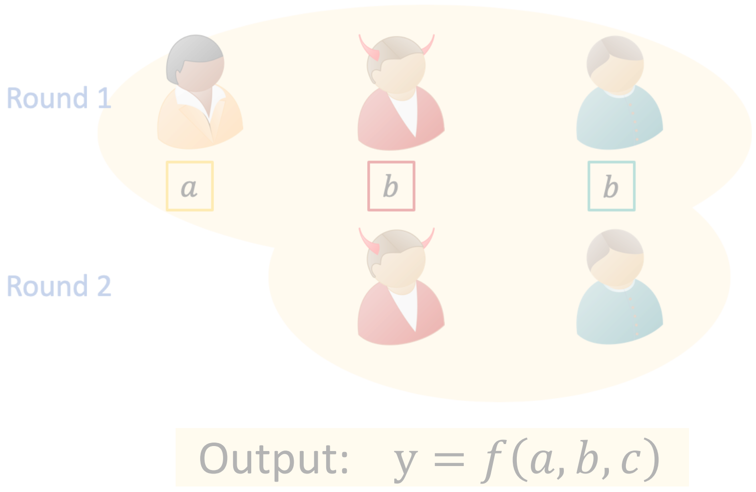
Output: $y = f(a, b, c)$

Seems Inherent? (Scenario 2)



NOT SECURE!!

Corrupt Bob can launch an offline residual function attack



Our Observation

Increasing round complexity

can

decrease broadcast message complexity

Our Observation

Increasing round complexity

can

decrease broadcast message complexity

Simultaneity is wasteful

Our Results

Model	Corruptions	Rounds	Output Parties	Broadcasts
Plain/CRS	$t < n - 1$		> 1	$n + t + 1$
			$= 1$	$n + t$

Our Results

Model	Corruptions	Rounds	Output Parties	Broadcasts
Plain/CRS	$t < n - 1$		> 1	$n + t + 1$
			$= 1$	$n + t$
Plain/CRS	$t = n - 1$		> 1	$2n - 1$
			$= 1$	$2n - 2$

Our Results

Model	Corruptions	Rounds	Output Parties	Broadcasts
Plain	$t < n - 1$		> 1	$n + t + 1$
			$= 1$	$n + t$
Plain	$t = n - 1$		> 1	$2n - 1$
			$= 1$	$2n - 2$
PKI	$t < n$		$> n - t$	$n + t$
			$\leq n - t$	$n + t - 1$

Our Results

Model	Corruptions	Rounds	Output Parties	Broadcasts
Plain/CRS	$t < n - 1$	3	> 1	$n + t + 1$
			$= 1$	$n + t$
Plain/CRS	$t = n - 1$	3	> 1	$2n - 1$
			$= 1$	$2n - 2$
PKI	$t < n$	3	$> n - t$	$n + t$
			$\leq n - t$	$n + t - 1$

3 rounds are necessary and sufficient for optimal broadcast message complexity

Our Results

Model	Corruptions	Rounds	Output Parties	Broadcasts
Plain/CRS	$t < n - 1$	3	> 1	$n + t + 1$
			$= 1$	$n + t$
Plain/CRS	$t = n - 1$	3	> 1	$2n - 1$
			$= 1$	$2n - 2$
PKI	$t < n$	3	$> n - t$	$n + t$
			$\leq n - t$	$n + t - 1$

Broadcast message complexity is much lower than $2n$.

This Talk: Lower Bounds

Model	Corruptions	Rounds	Output Parties	Broadcasts
Plain/CRS	$t < n - 1$	3	> 1	$n + t + 1$
			$= 1$	$n + t$
Plain/CRS	$t = n - 1$	3	> 1	$2n - 1$
			$= 1$	$2n - 2$
PKI/CRS	$t < n$	3	$> n - t$	$n + t$
			$\leq n - t$	$n + t - 1$

Message Complexity in the Plain/CRS Model

Message Complexity in the Plain/CRS Model

Obsv 1

At least t+1 parties must broadcast at least two messages each

Message Complexity in the Plain/CRS Model

Obsv 1

At least t+1 parties must broadcast at least two messages each

Obsv 2

All parties must broadcast at least one message

At least t+1 parties must broadcast at least two messages each

At least t+1 parties must broadcast at least two messages each

$\boxed{n = 5}$ $\boxed{t = 2}$

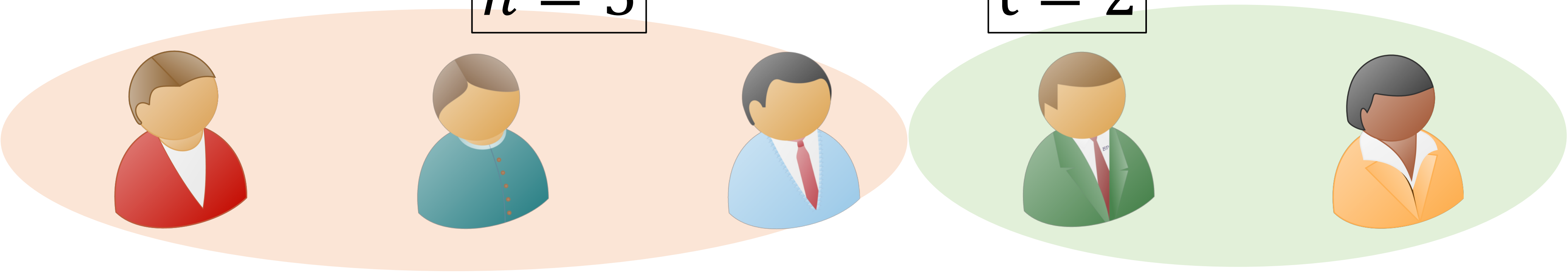
At least t+1 parties must broadcast at least two messages each

$\boxed{n = 5}$ $\boxed{t = 2}$

Assume only $t = 2$ parties broadcast at least two messages

At least t+1 parties must broadcast at least two messages each

$\boxed{n = 5}$ $\boxed{t = 2}$

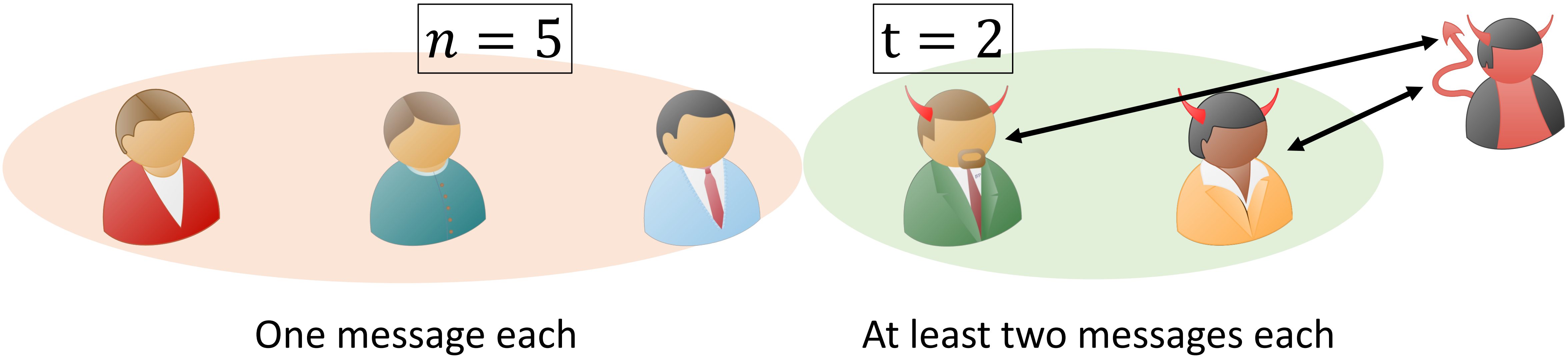


One message each

At least two messages each

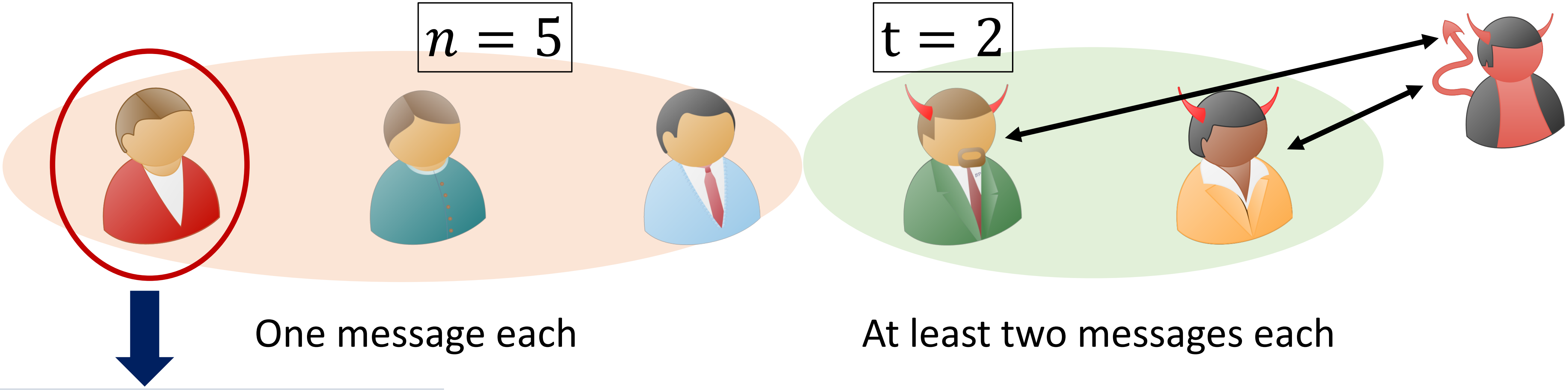
Assume only $t = 2$ parties broadcast at least two messages

At least t+1 parties must broadcast at least two messages each



Assume only $t = 2$ parties broadcast at least two messages

At least t+1 parties must broadcast at least two messages each



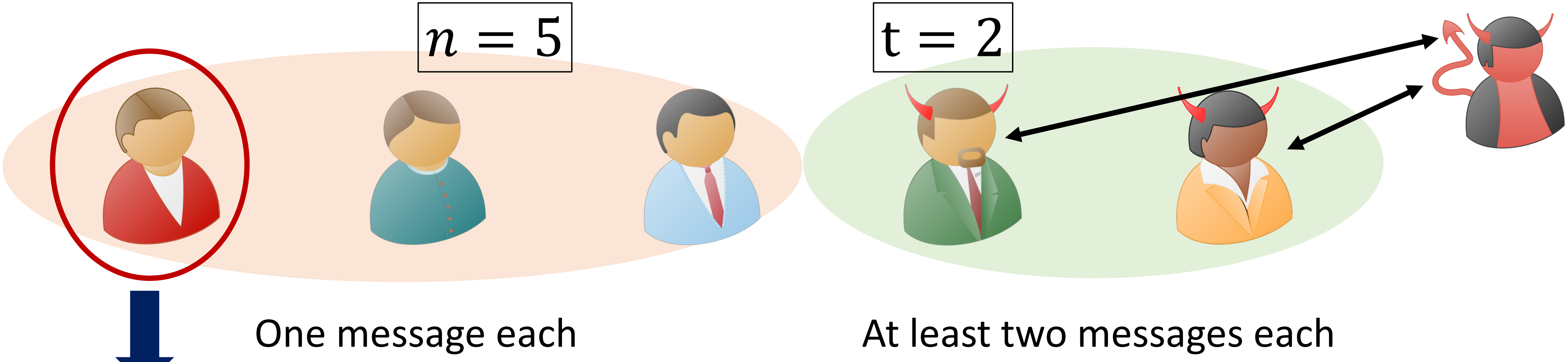
One message each

At least two messages each

First party in the orange set

Assume only $t = 2$ parties broadcast at least two messages

At least t+1 parties must broadcast at least two messages each

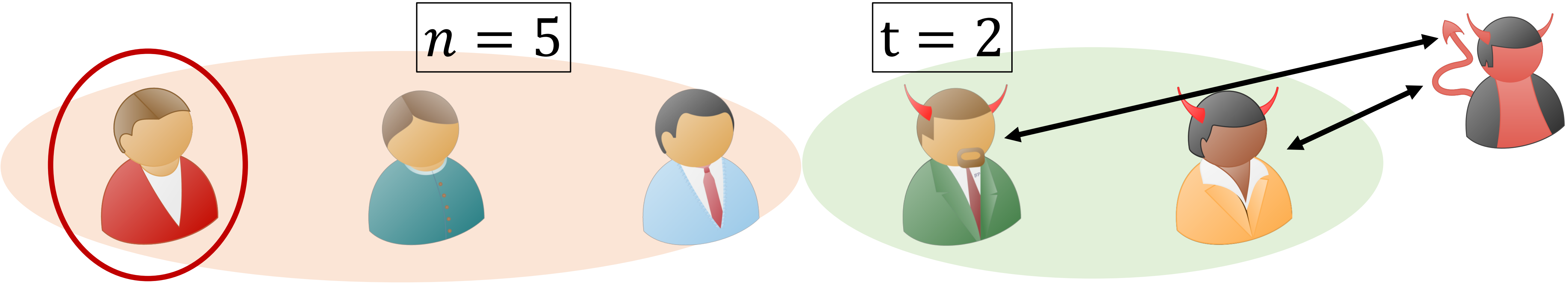


First party in the orange set

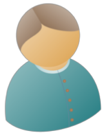
His message is independent of the inputs of other parties in the orange set

Assume only $t = 2$ parties broadcast at least two messages

At least t+1 parties must broadcast at least two messages each

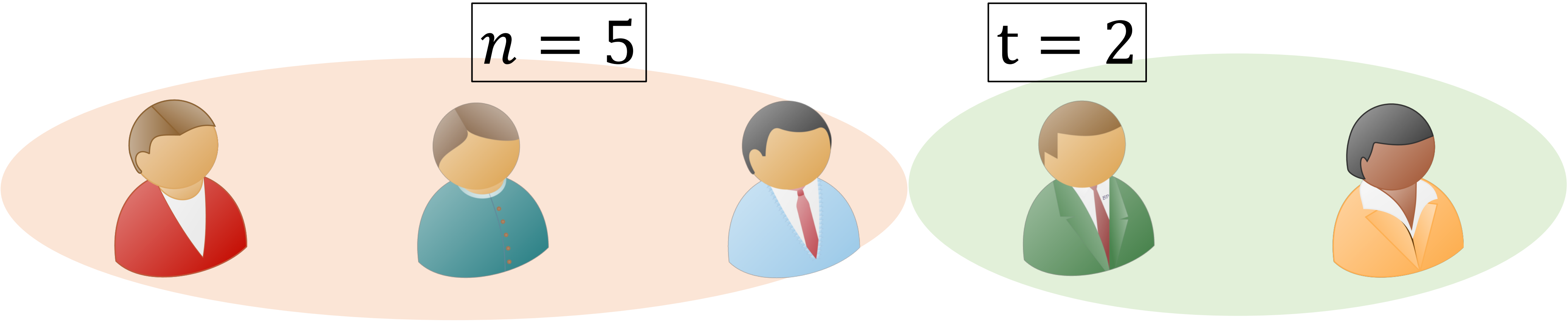


Residual Function Attack by Spoofing

 can recompute messages of  and  on different inputs by spoofing as them.

Assume only $t = 2$ parties broadcast at least two messages

At least t+1 parties must broadcast at least two messages each



One message each

At least two messages each

$\boxed{\text{Not Secure !!}}$

Assume only $t = 2$ parties broadcast at least two messages

Message Complexity in the Plain/CRS Model

Obsv 1

At least t+1 parties must broadcast at least two messages each

Obsv 2

All parties must broadcast at least one message

Message Complexity in the Plain/CRS Model

Obsv 1

At least t+1 parties must broadcast at least two messages each

Obsv 2

All parties must broadcast at least one message

Important for considering their inputs.

Message Complexity in the Plain/CRS Model

Obsv 1

At least t+1 parties must broadcast at least two messages each

Obsv 2

All parties must broadcast at least one message

Message Complexity in the Plain/CRS Model

Obsv 1

At least t+1 parties must broadcast at least two messages each

$2\times(t+1)$ messages

Obsv 2

All parties must broadcast at least one message

$1\times(n-(t+1))$ messages

$2\times(t+1)+1\times(n-(t+1))=n+t+1$ messages

Communication Pattern in the Plain/CRS Model

Communication Pattern in the Plain/CRS Model

Minimum Round Complexity: 3

Communication Pattern in the Plain/CRS Model

Minimum Round Complexity: 3

There is a unique communication pattern.

Communication Pattern in the Plain/CRS Model

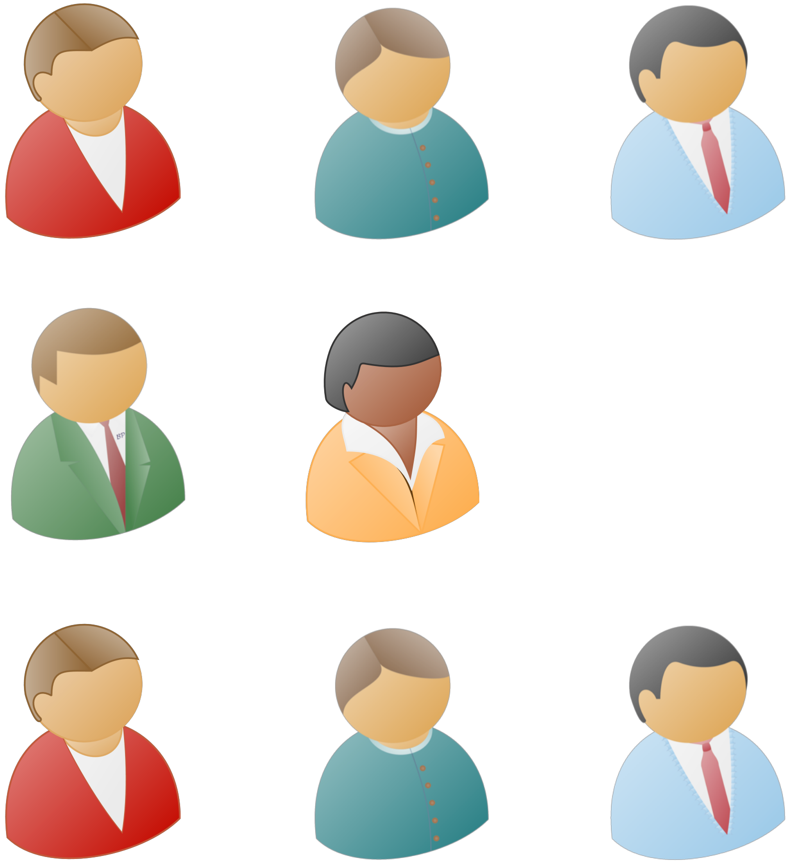
Minimum Round Complexity: 3

There is a unique communication pattern.

Round 1

Round 2

Round 3



Communication Pattern in the Plain/CRS Model

Message Complexity in the PKI Model

Obsv 1

At least t parties must broadcast at least two messages each

Message Complexity in the PKI Model

Obsv 1

At least t parties must broadcast at least two messages each

This is in contrast to the requirement in the plain model

Spoofing attacks are not possible in the PKI model

Message Complexity in the PKI Model

Obsv 1

At least t parties must broadcast at least two messages each

Obsv 2

All parties must broadcast at least one message

Message Complexity in the PKI Model

Obsv 1	At least t parties must broadcast at least two messages each
Obsv 2	All parties must broadcast at least one message

At least t parties must broadcast at least two messages each

At least t parties must broadcast at least two messages each

$\boxed{n = 5}$ $\boxed{\mathrm{t} = 2}$

At least t parties must broadcast at least two messages each

$\boxed{n = 5}$ $\boxed{t = 2}$

Assume only $t - 1 = 1$ parties broadcast at least two messages

At least t parties must broadcast at least two messages each

$n = 5$ $\quad$ $t = 2$

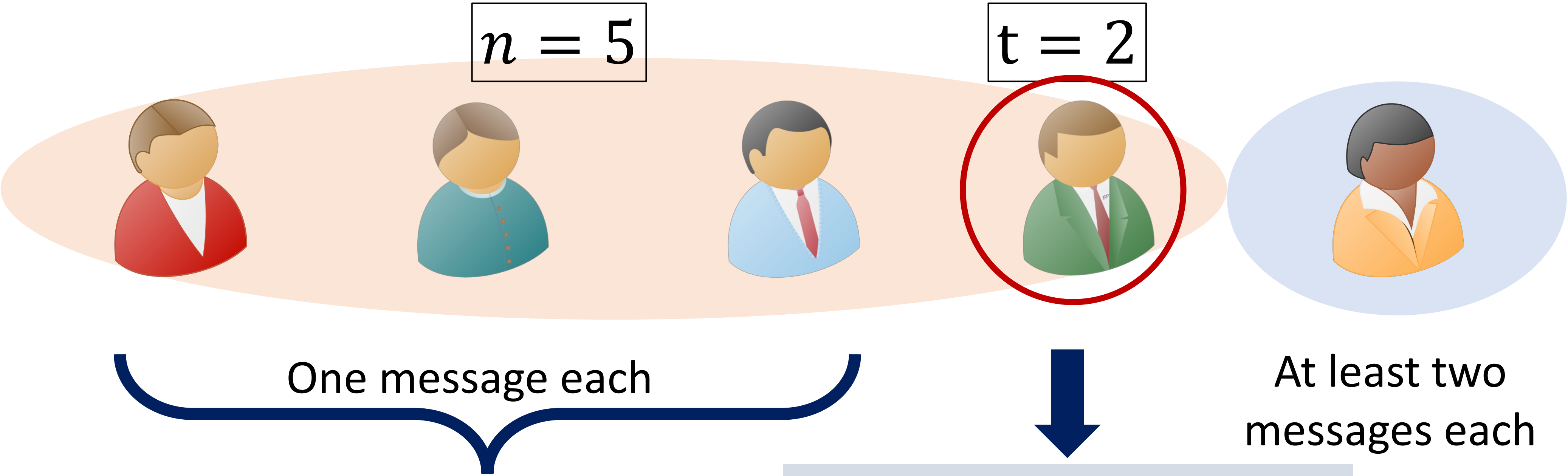
One message each

At least two messages each

Last party in the orange set

Assume only $t - 1 = 1$ parties broadcast at least two messages

At least t parties must broadcast at least two messages each

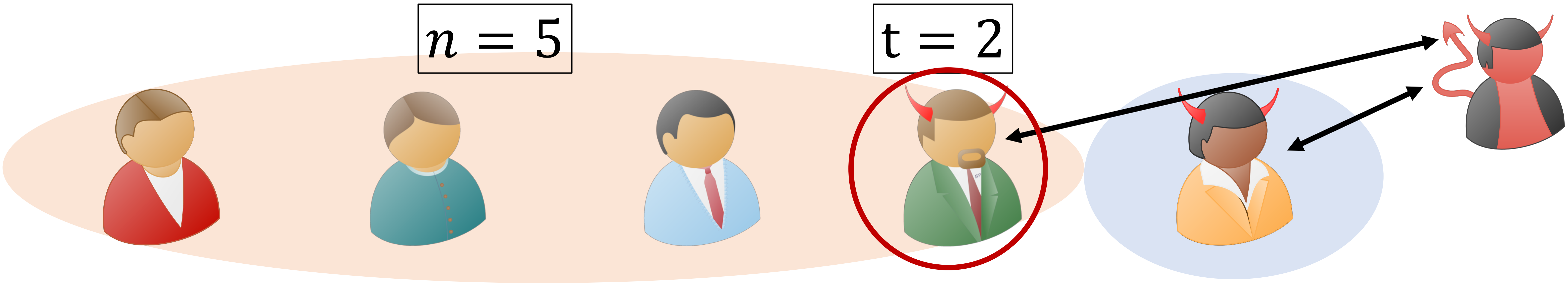


Messages of these parties are independent of the last party's input

Last party in the orange set

Assume only $t - 1 = 1$ parties broadcast at least two messages

At least t parties must broadcast at least two messages each



One message each

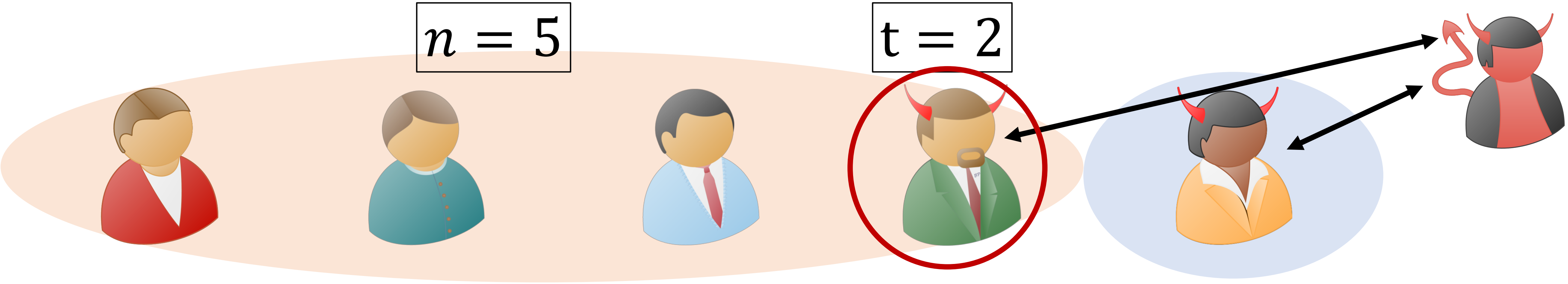
Messages of these parties are independent of the last party's input

Last party in the orange set

At least two messages each

Assume only $t - 1 = 1$ parties broadcast at least two messages

At least t parties must broadcast at least two messages each



Residual Function Attack without Spoofing

Re-compute the message of  on different inputs.

Assume only $t - 1 = 1$ parties broadcast at least two messages

At least t parties must broadcast at least two messages each

$n = 5$ $\quad$ $t = 2$

Not Secure !!

Assume only $t - 1 = 1$ parties broadcast at least two messages

Message Complexity in the PKI Model

STEP 1

At least t parties must broadcast at least two messages each

STEP 2

All parties must broadcast at least one message

Message Complexity in the PKI Model

STEP 1

At least t parties must broadcast at least two messages each

$2 \times t$ messages

STEP 2

All parties must broadcast at least one message

$1 \times (n - t)$ messages

$(2 \times t) + (1 \times (n - t)) = n + t$ messages

Communication Pattern in the PKI Model

Minimum Round Complexity: 3

There is a restricted class of admissible communication patterns.

Summary

- Initiate the study of broadcast message complexity in MPC.

Summary

- Initiate the study of broadcast message complexity in MPC.
- Provide tight bounds for semi-honest corruptions in the PKI, plain and CRS models.

Summary

- Initiate the study of broadcast message complexity in MPC.
- Provide tight bounds for semi-honest corruptions in the PKI, plain and CRS models.
- Show that 3 rounds are necessary and sufficient for optimal message complexity.

Summary

- Initiate the study of broadcast message complexity in MPC.
- Provide tight bounds for semi-honest corruptions in the PKI, plain and CRS models.
- Show that 3 rounds are necessary and sufficient for optimal message complexity.
- Show which communication patterns are feasible for achieving optimal message complexity.

Thank You.

aarushig@cs.jhu.edu