

On Communication Models and Best-Achievable Security in Two-Round MPC

Aarushi Goel

Abhishek Jain

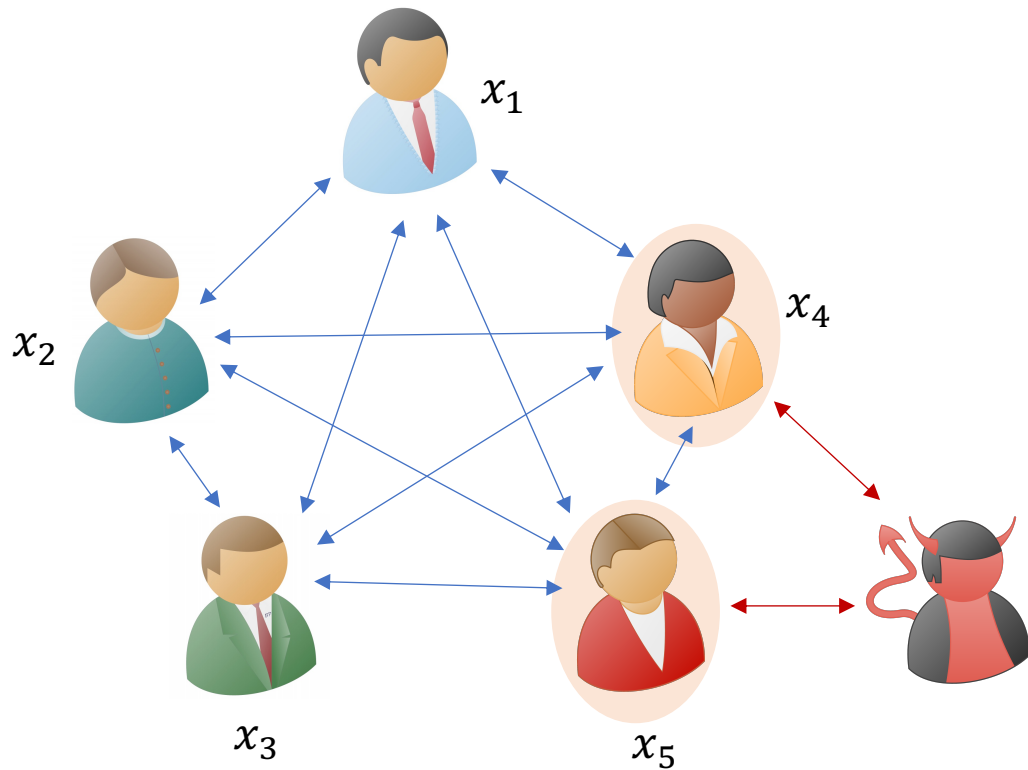
Manoj Prabhakaran

Rajeev Raghunath



Indian Institute of
Technology Bombay

Secure Multiparty Computation (MPC)

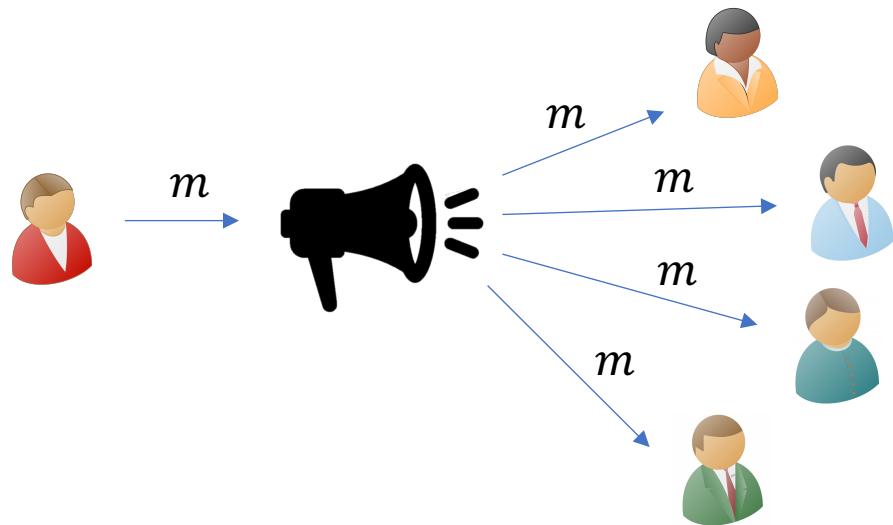


Adversary learns nothing beyond the output y

MPC protocol for computing $y = f(x_1, x_2, x_3, x_4, x_5)$

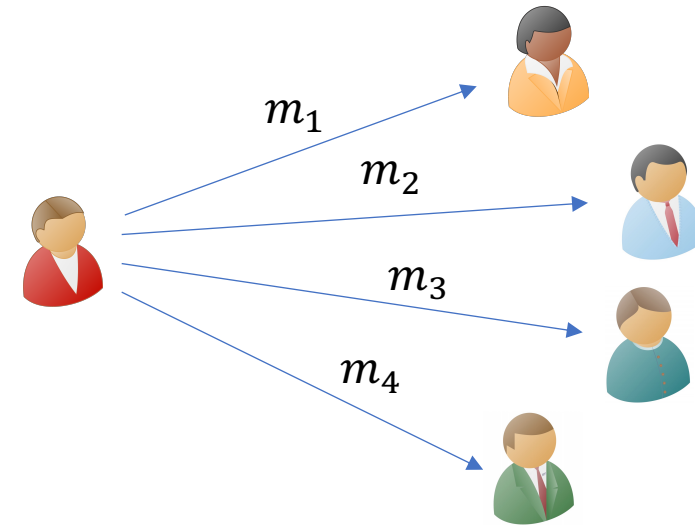
Communication Models

Broadcast Channel



Necessary for achieving security against $t > n/3$ corruptions

Private Point-to-Point (P2P) Channels



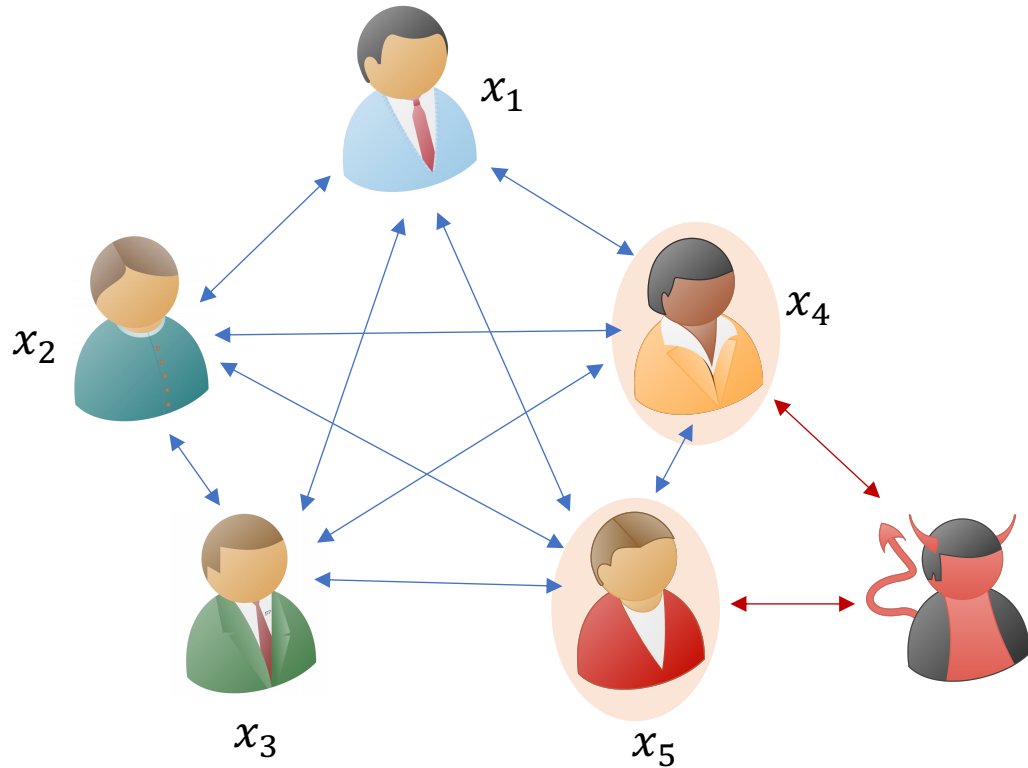
Necessary for achieving information theoretic security

Our Setting: Two-Rounds

Minimal Rounds, since one-round MPC is impossible [HLP'11]

A lot of advancement in recent years
[GS'18, BL'18, PR18, ACGJ'18, ABT'18, GIS'18, ACGJ'19, ABT'19]

Our Setting: Honest Majority [BGW88]



Advantages

Enables stronger security guarantees

Can be designed using only symmetric-key primitives

Can be designed in fewer Rounds

Often holds up in practice

Adversary corrupts a **minority** of the parties

Main Question

In two-round honest-majority MPC, in the different communication models involving broadcast and P2P channels:

What levels of security are achievable for general computation?

Under what assumptions?

In this work we focus on the plain model (no setup) and sometimes augment it to use a bare public-key infrastructure (bare PKI)

Different Security Notions

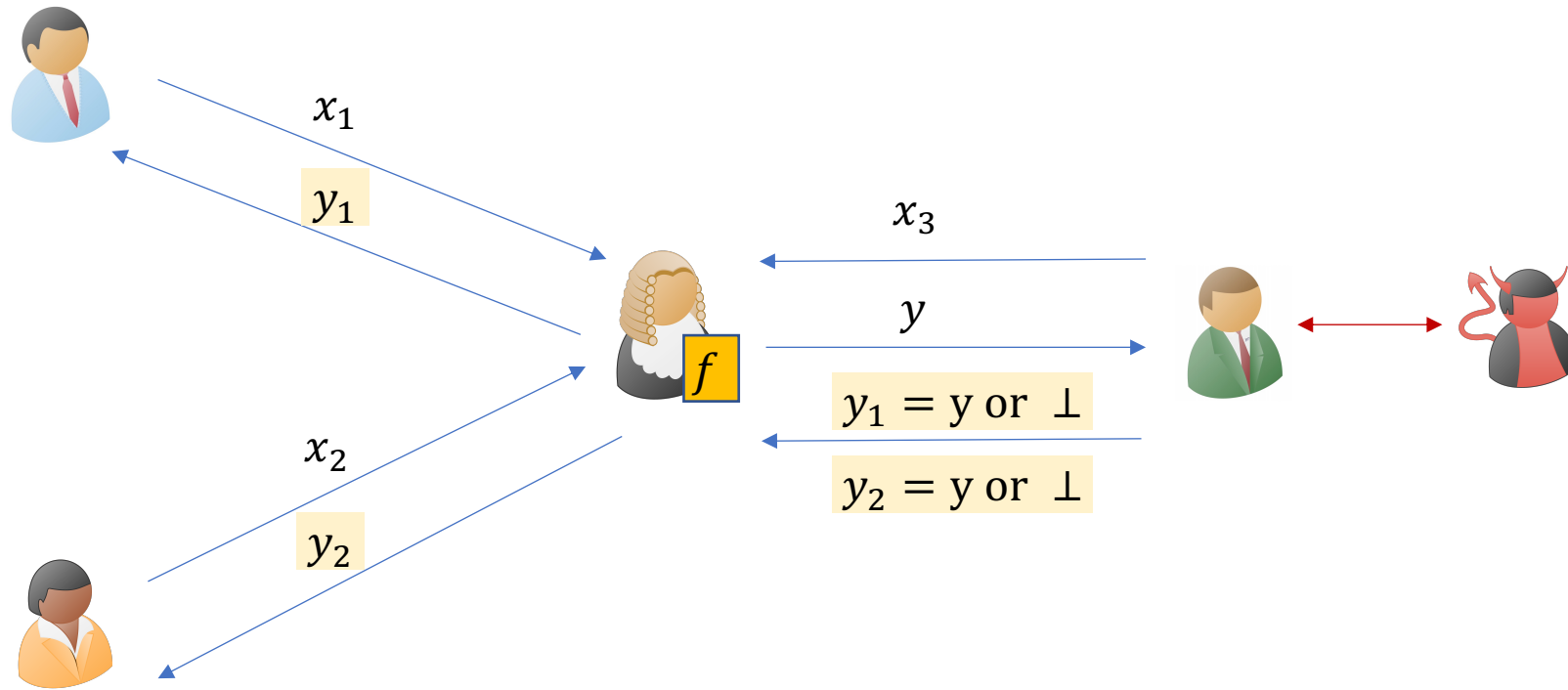
Privacy against semi-honest adversaries

Different Security Notions

Privacy against semi-honest adversaries

Security with (Selective/Unanimous/Identifiable) abort against malicious adversaries

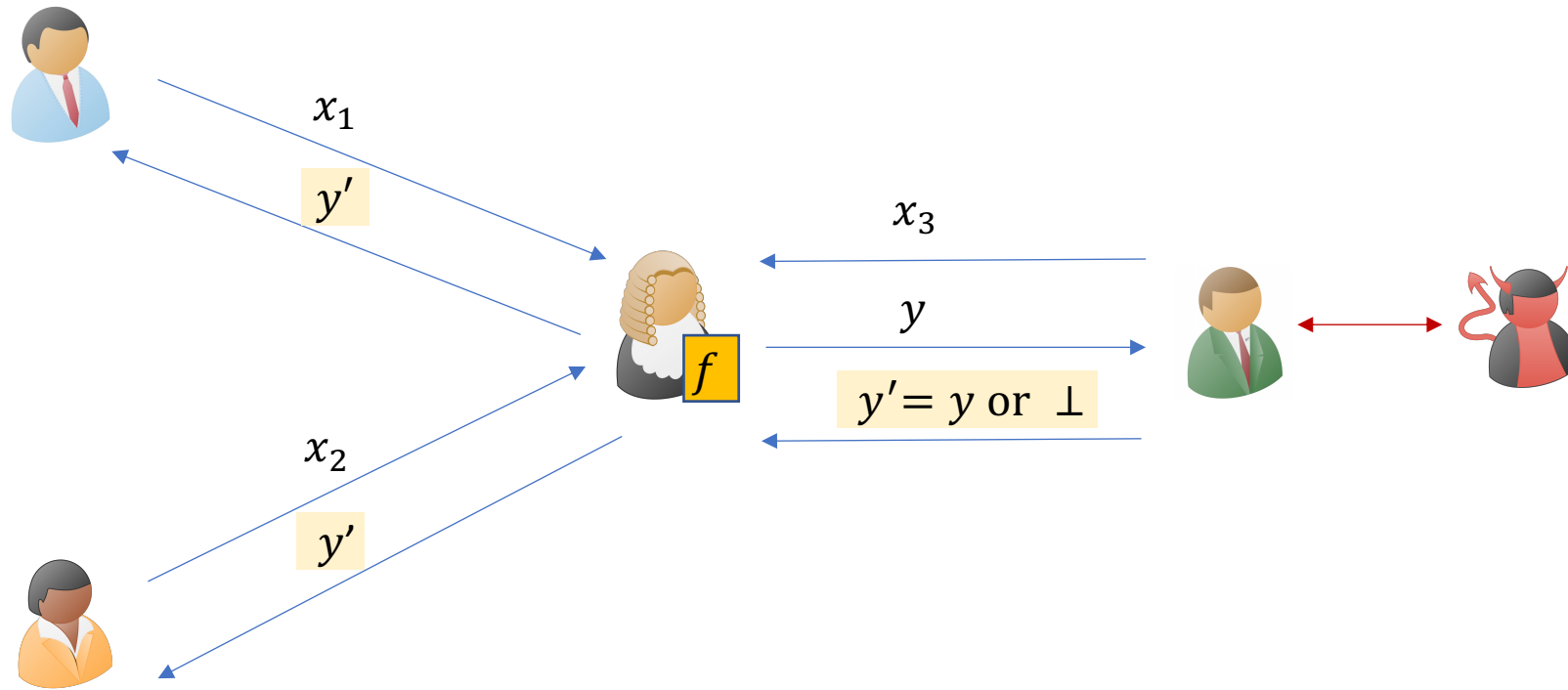
Security with Selective Abort



Honest Parties

Corrupt Party

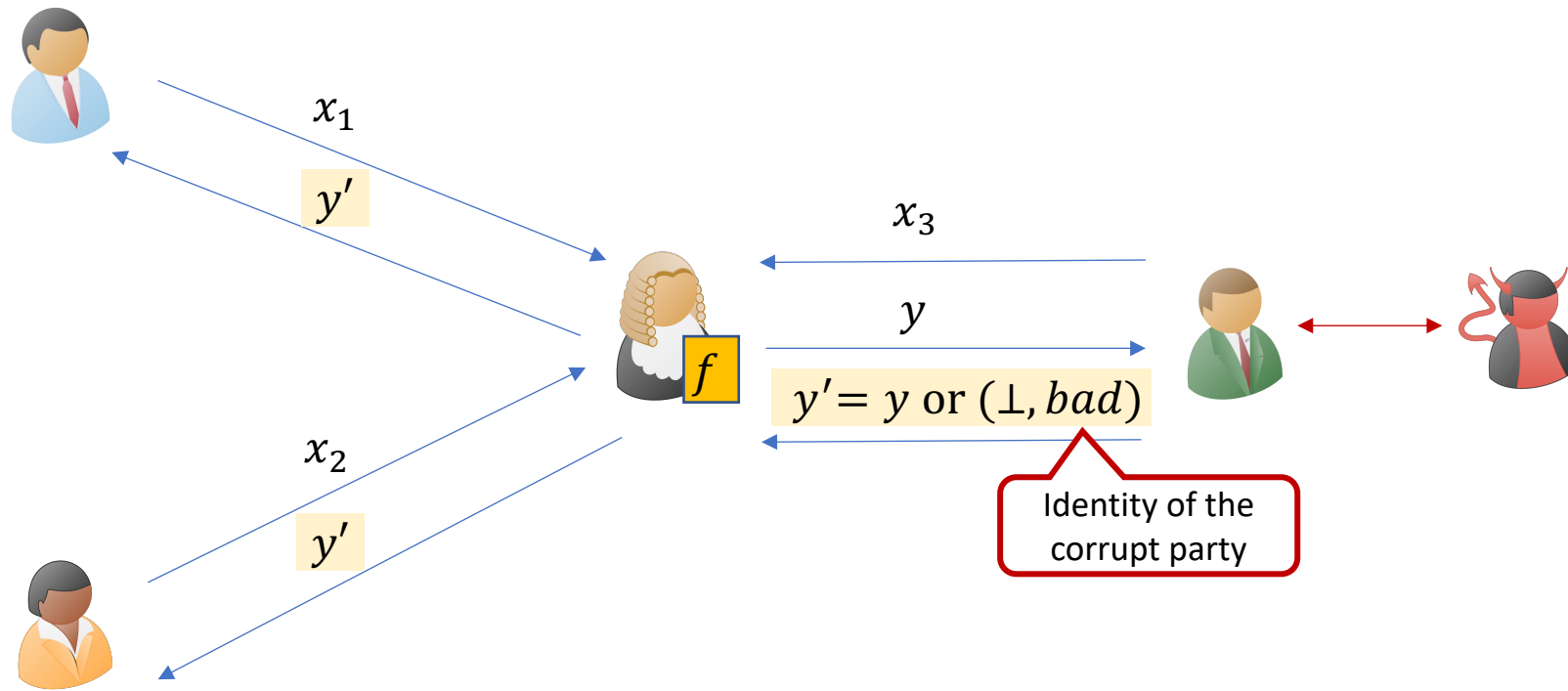
Security with Unanimous Abort



Honest Parties

Corrupt Party

Security with Identifiable Abort



Honest Parties

Corrupt Party

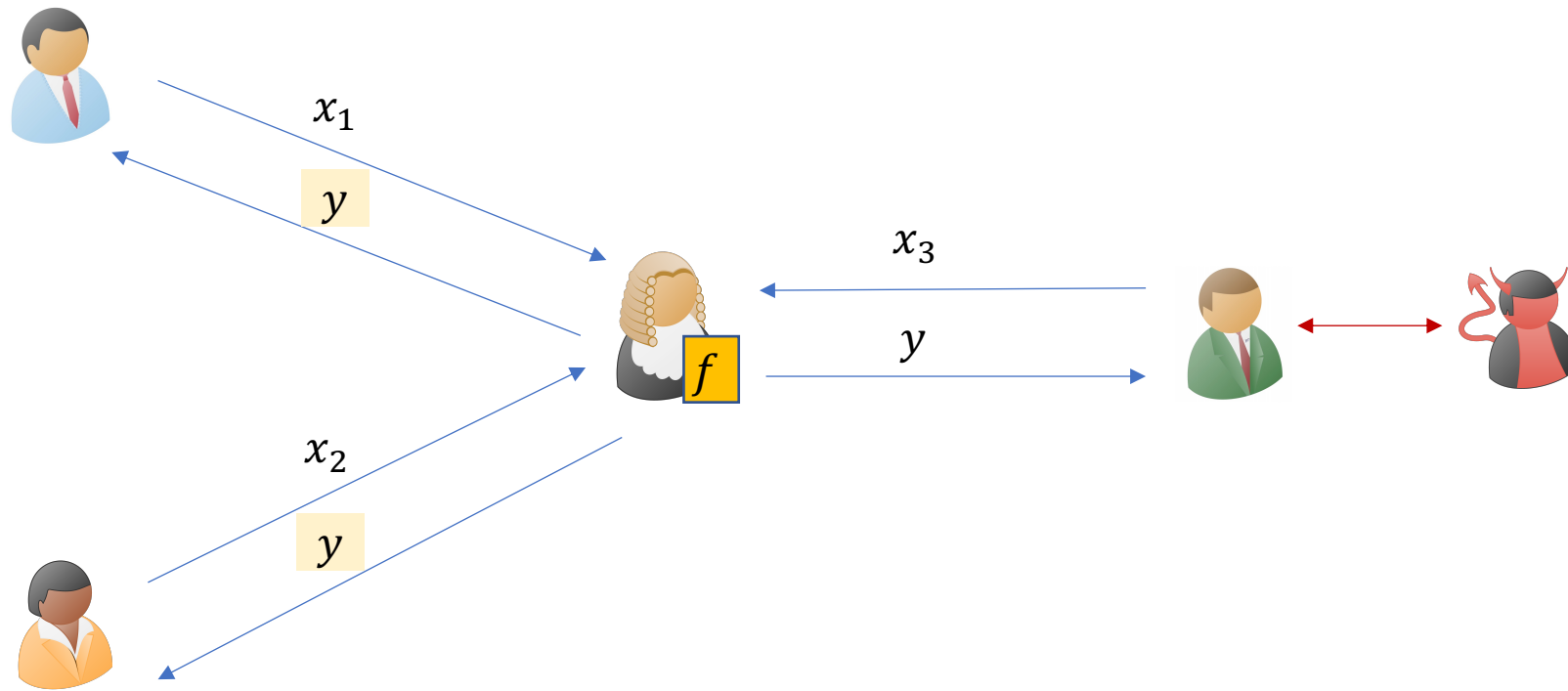
Different Security Notions

Privacy against semi-honest adversaries

Security with (**Selective/Unanimous/Identifiable**) abort against malicious adversaries

Guaranteed output delivery against (**Malicious/Fail-stop**) adversaries

Guaranteed Output Delivery

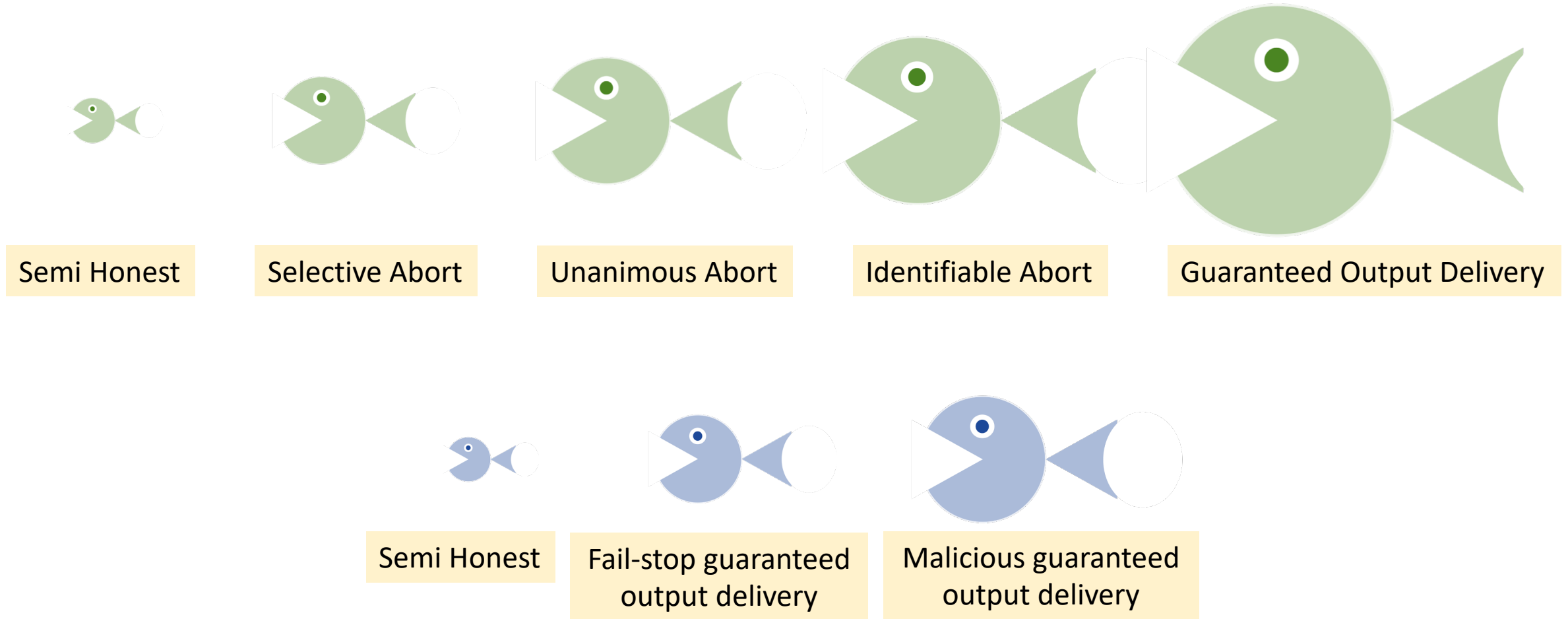


Honest Parties

Corrupt Party

Adversary is either malicious or fail-stop

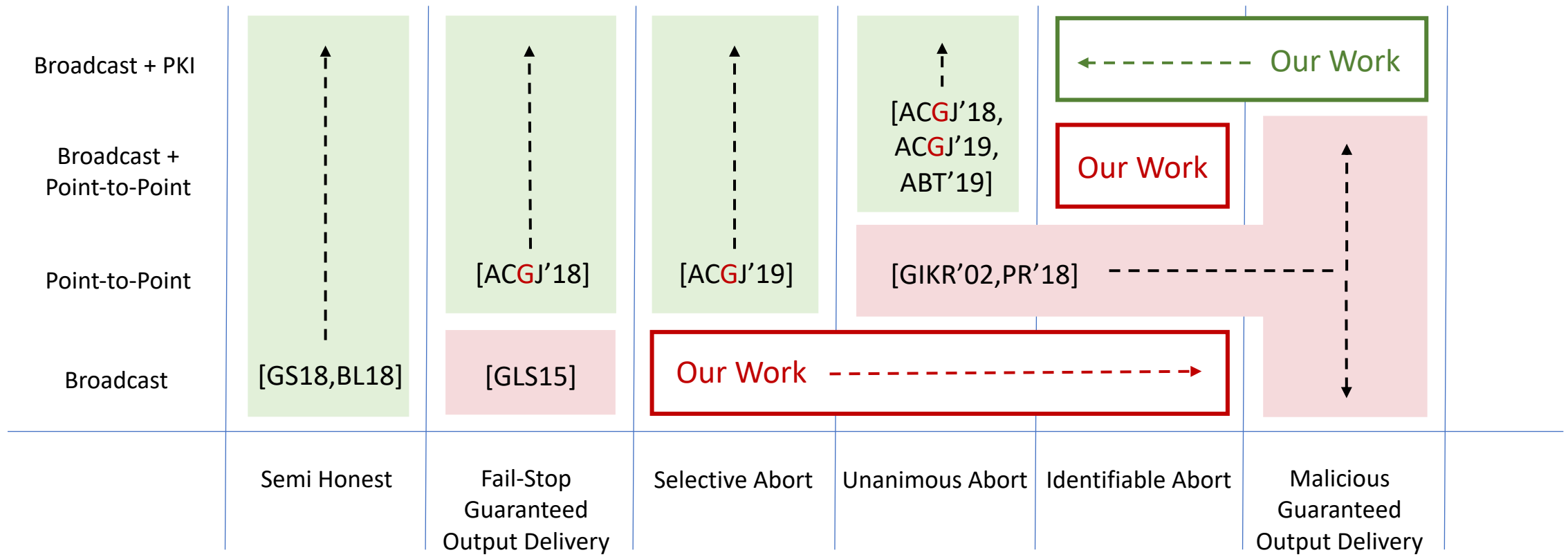
Hierarchy of Security Notions



Two-Round MPC

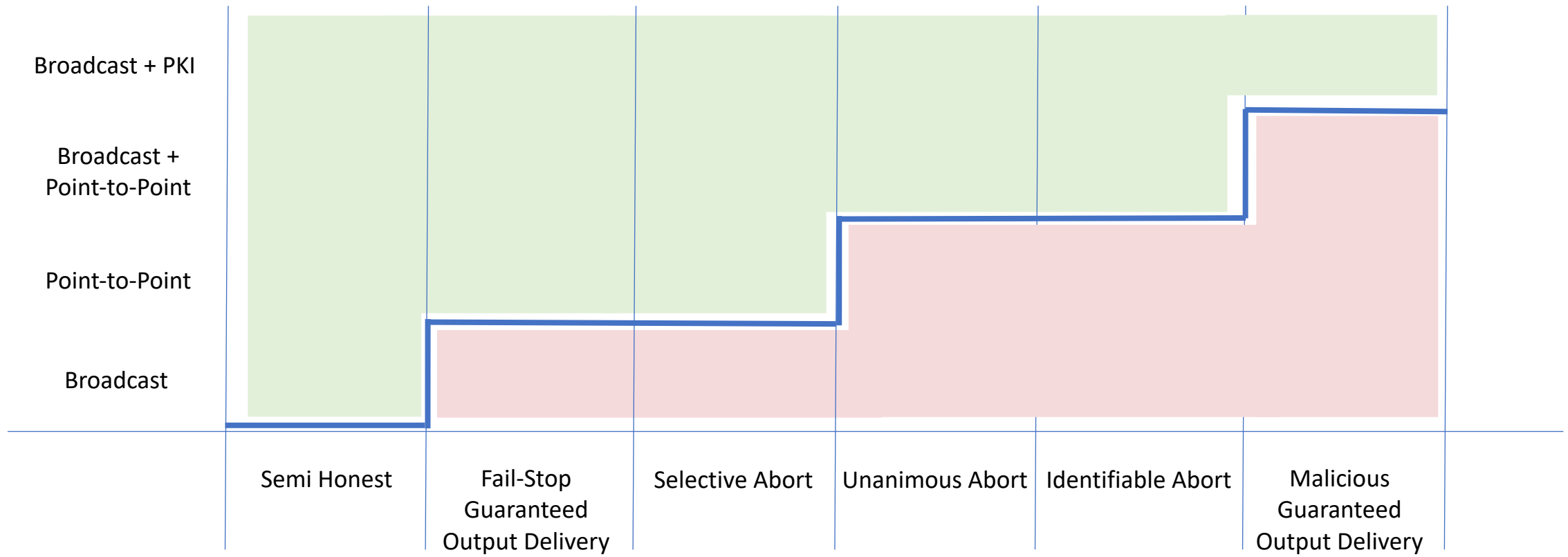
| | | | | | | |
|----------------------------|-------------|--|-----------------|---------------------------------------|--------------------|--|
| Broadcast + PKI | | | | ↑ [ACGJ'18, ACGJ'19, ABT'19] | ? | ? |
| Broadcast + Point-to-Point | | ↑ | ↑ | | ? | ↑ |
| Point-to-Point | | [ACGJ'18] | [ACGJ'19] | [GIKR'02,PR'18] | ----- | ↓ |
| Broadcast | [GS18,BL18] | [GLS15] | ? | ? | ? | |
| | Semi Honest | Fail-Stop Guaranteed Output Delivery | Selective Abort | Unanimous Abort | Identifiable Abort | Malicious Guaranteed Output Delivery |

Two-Round MPC (Completing the Picture)

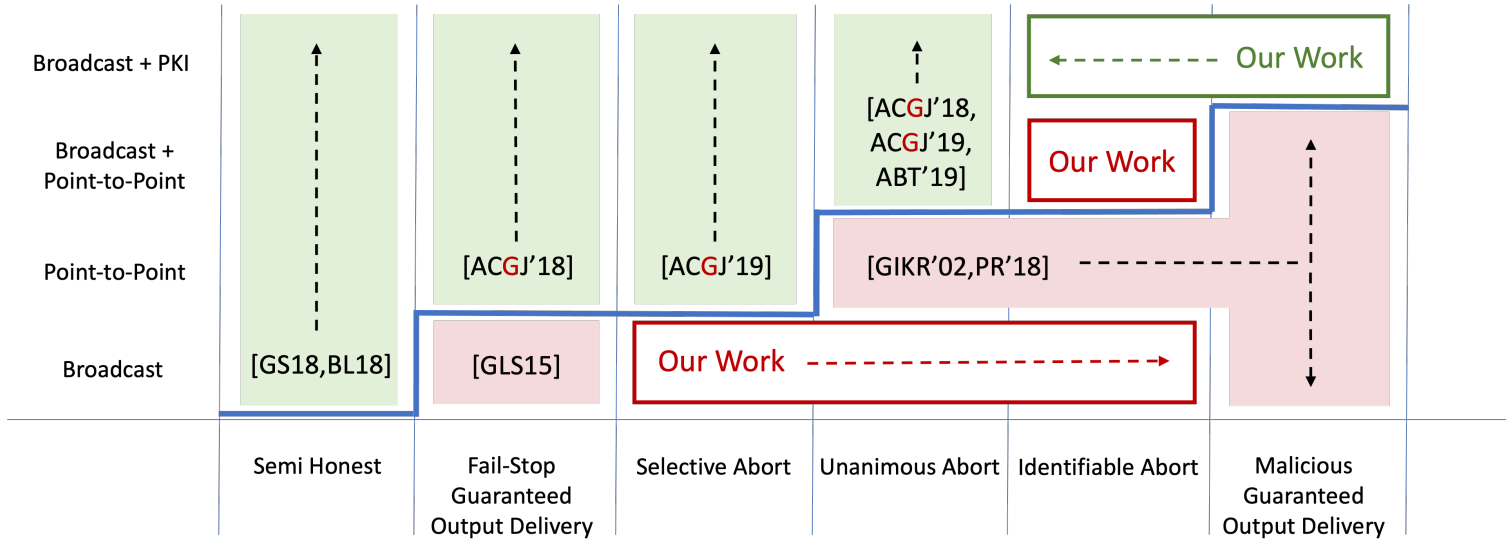


Hierarchy of Communication Models

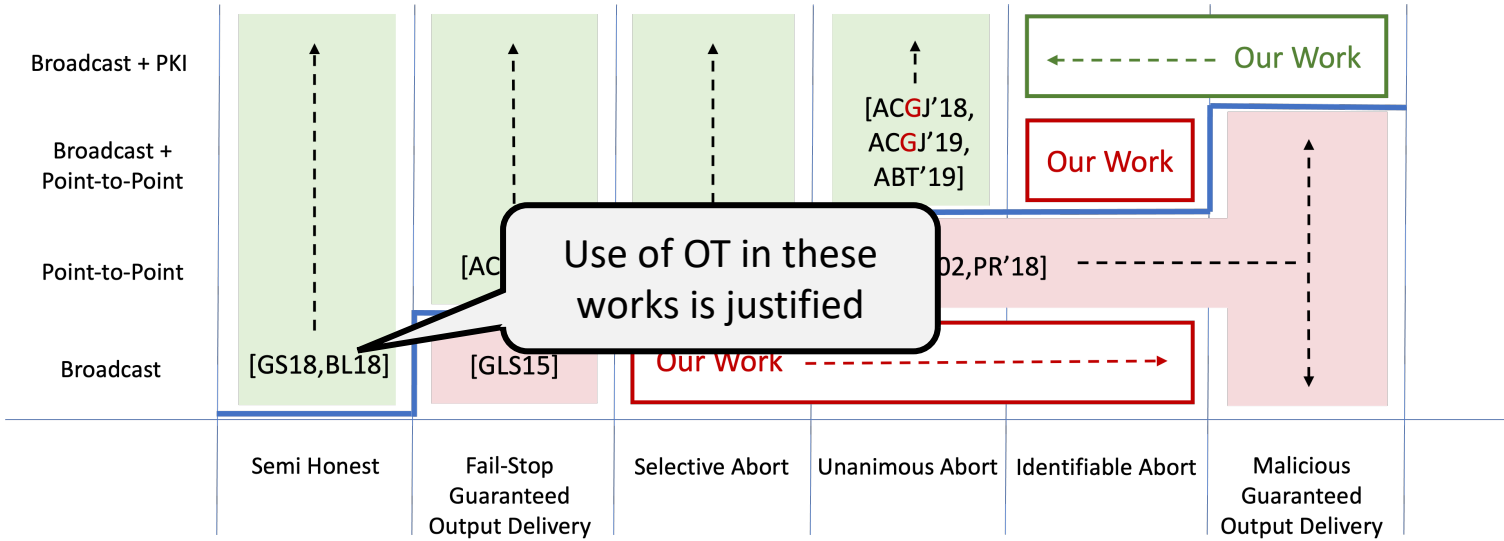
Broadcast < Point-to-Point < Broadcast + Point-to-Point < Broadcast + PKI



Our Contributions



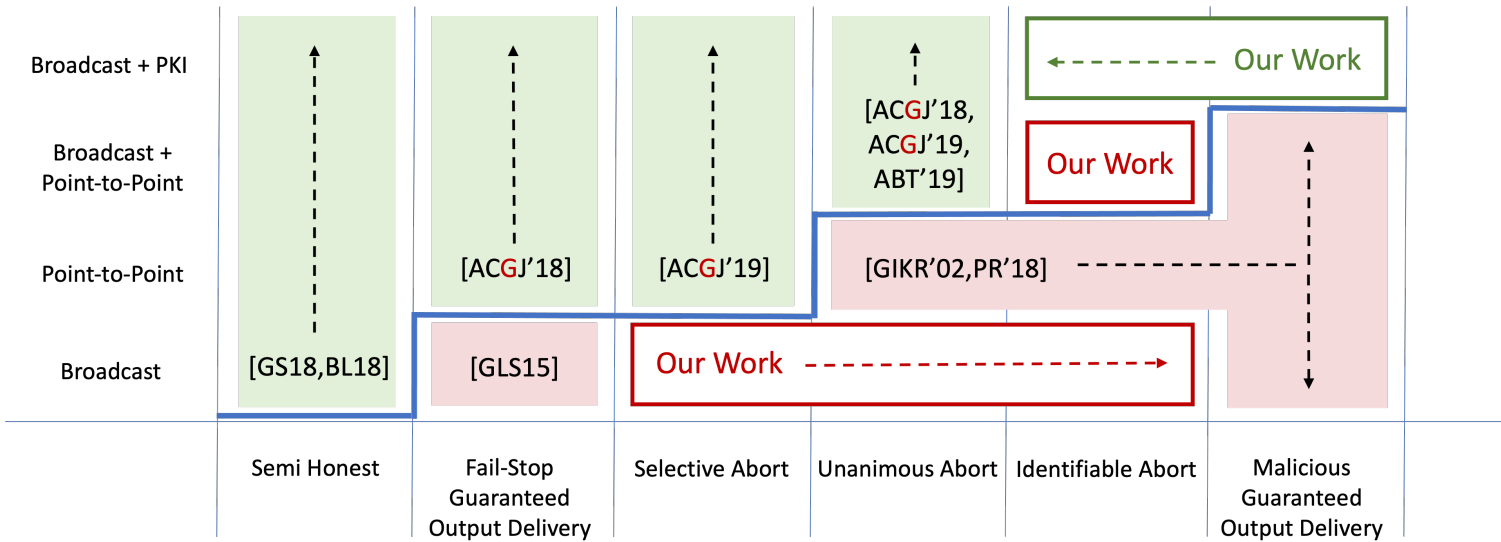
Our Contributions



Two-round honest-majority **semi-honest/malicious** MPC over broadcast channels
 ⇒ **semi-honest/malicious** two-message OT

This implication holds both in the plain and in the CRS model

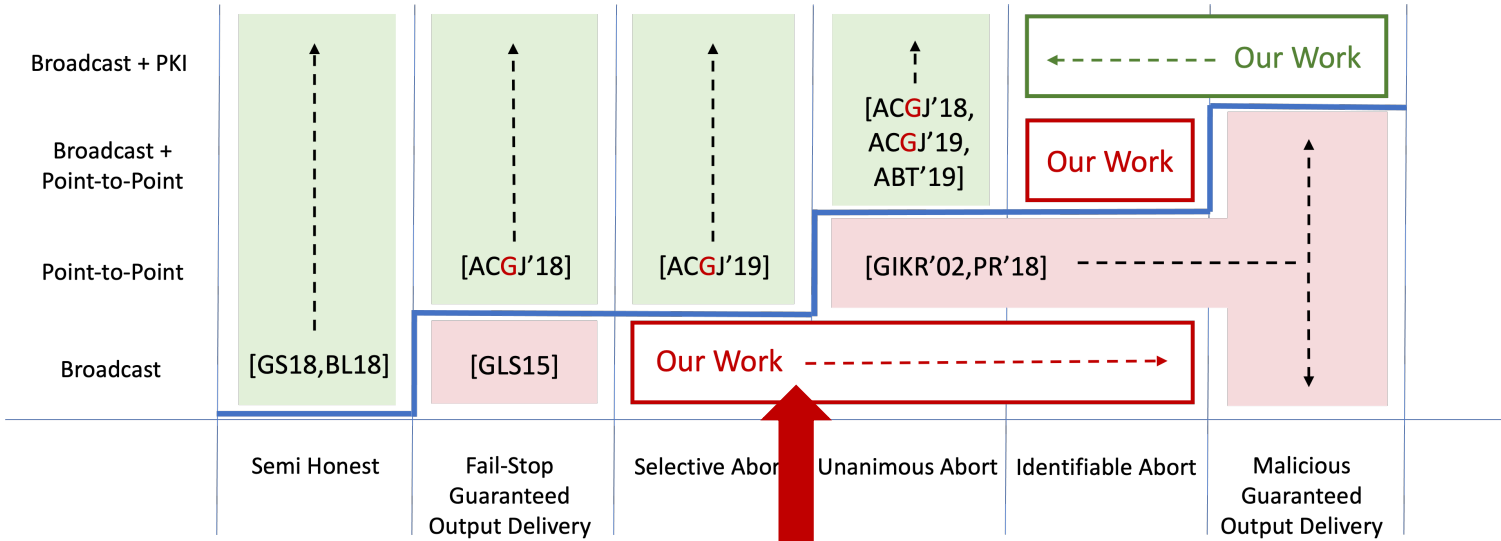
Our Contributions



Two-round honest-majority **semi-honest/malicious** MPC over broadcast channels
 ⇒ **semi-honest/malicious** two-message OT

Two-message **malicious** OT is **impossible** in the plain model

Our Contributions



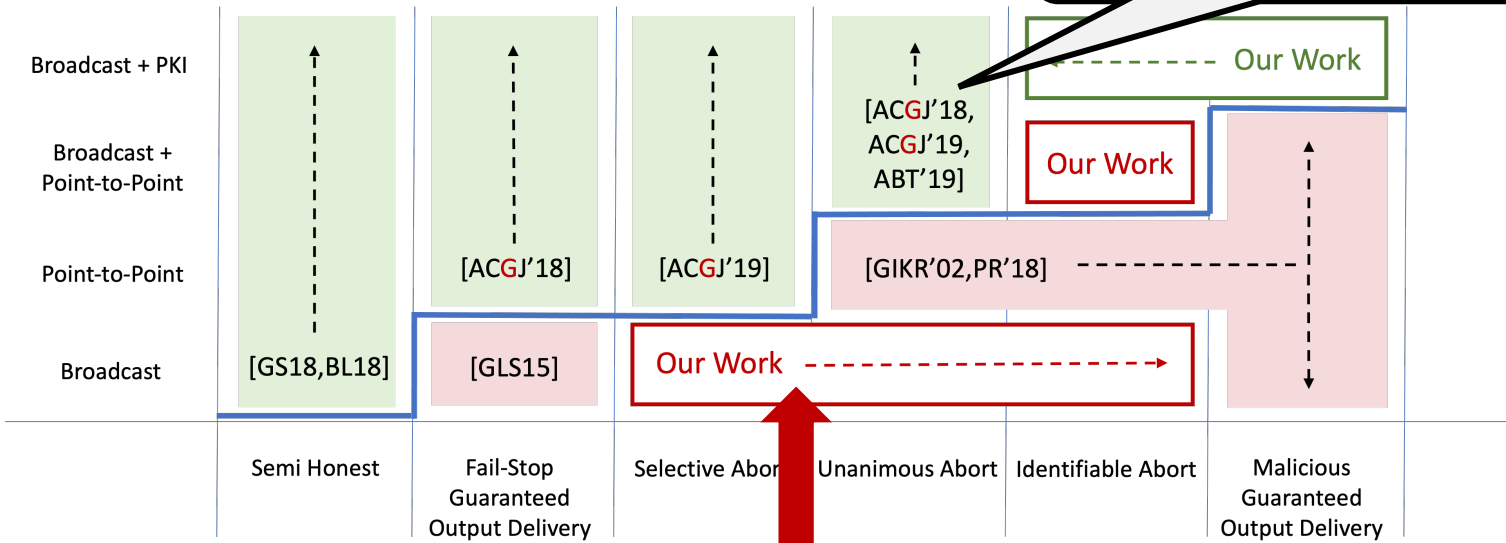
Two-round honest-majority **semi-honest/malicious** MPC over broadcast channels
 ⇒ **semi-honest/malicious** two-message OT

+

Two-message **malicious** OT is **impossible** in the plain model

Our Contributions

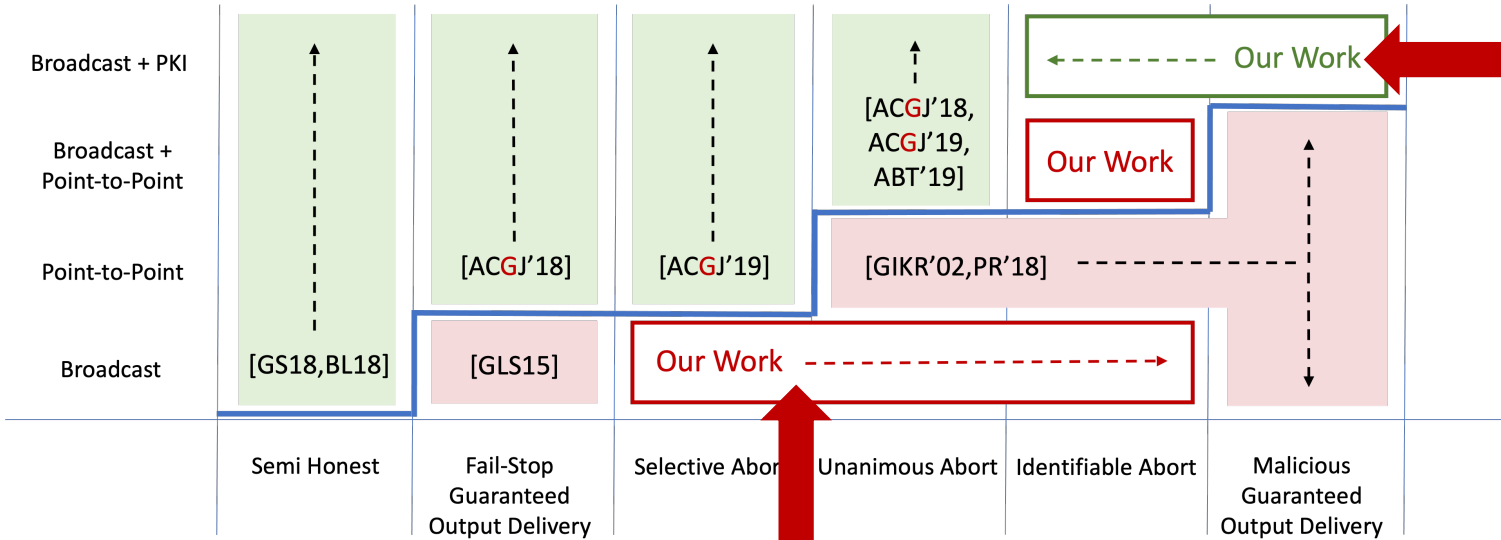
Use of P2P channels in these works was necessary



Two-round honest-majority **semi-honest/malicious** MPC over broadcast channels
 ⇒ **semi-honest/malicious** two-message OT
 +
 Two-message **malicious** OT is **impossible** in the plain model

Establishes equivalence of honest majority and dishonest majority in this setting

Our Contributions



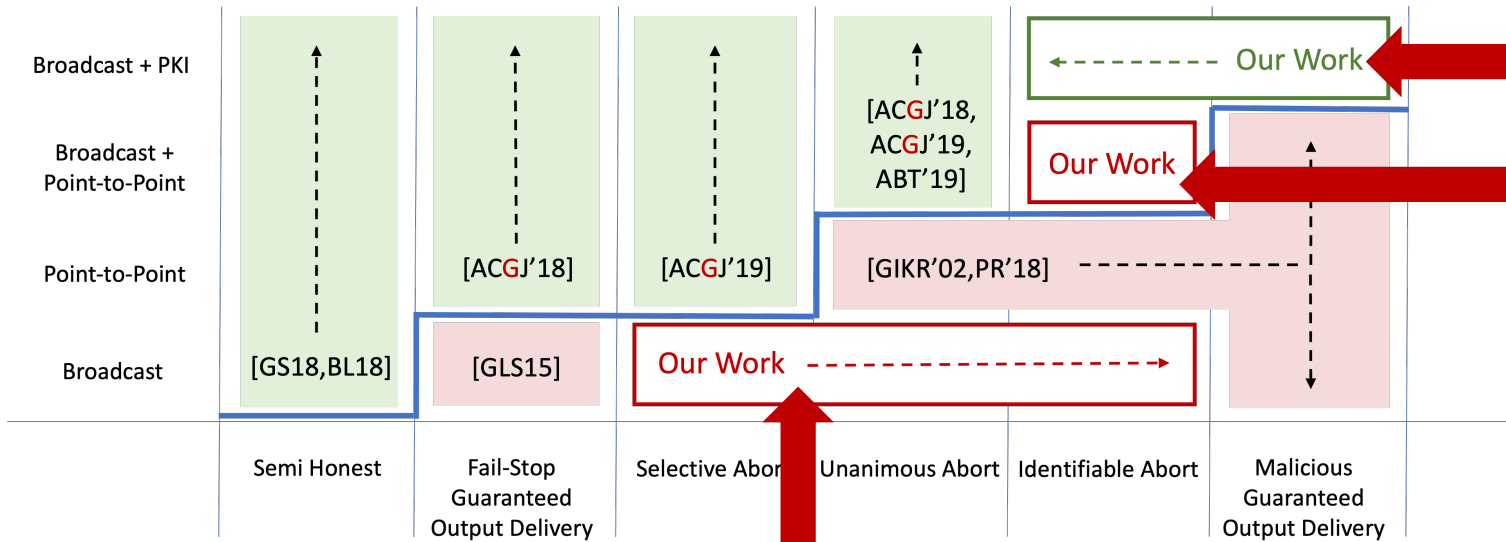
A two-round guaranteed output delivery protocol using PKE and multi-CRS NIZKs in broadcast + PKI setting for $t < n/2$

Two-round honest-majority semi-honest/malicious MPC over broadcast channels
 \Rightarrow semi-honest/malicious two-message OT

+

Two-message malicious OT is impossible in the plain model

Our Contributions



A two-round **guaranteed output delivery** protocol using **PKE** and **multi-CRS NIZKs** in **broadcast + PKI** setting for $t < n/2$

A two-round protocol with **identifiable abort** with $t < n/2$ is **impossible** over **broadcast + P2P** channels in the plain model

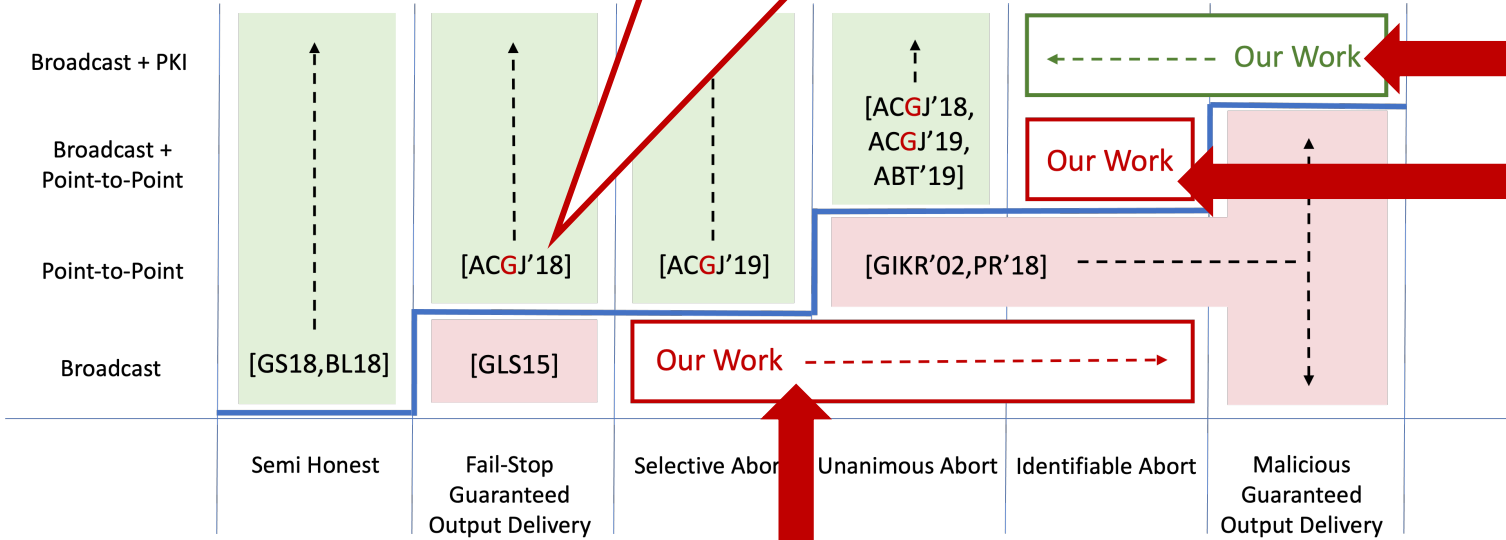
Two-round honest-majority **semi-honest/malicious** MPC over broadcast channels
 \Rightarrow **semi-honest/malicious** two-message OT

+

Two-message **malicious** OT is **impossible** in the plain model

Our Con

We also show that for $\frac{n}{3} < t < \frac{n}{2}$,
fail-stop guaranteed output
delivery implies OT!

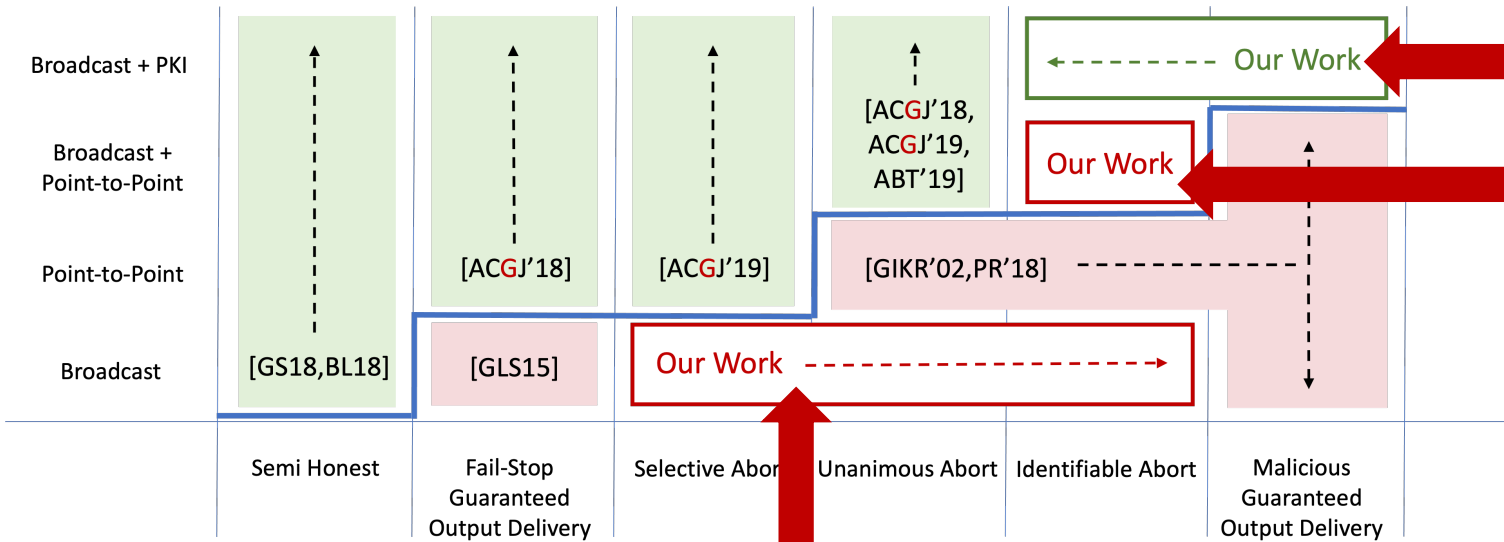


A two-round guaranteed output delivery protocol using PKE and multi-CRS NIZKs in broadcast + PKI setting for $t < n/2$

A two-round protocol with identifiable abort with $t < n/2$ is impossible over broadcast + P2P channels in the plain model

Two-round honest-majority semi-honest/malicious MPC over broadcast channels
 \Rightarrow semi-honest/malicious two-message OT
 +
 Two-message malicious OT is impossible in the plain model

Our Contributions



A two-round **guaranteed output delivery** protocol using **PKE** and **multi-CRS NIZKs** in **broadcast + PKI** setting for $t < n/2$

A two-round protocol with **identifiable abort** with $t < n/2$ is **impossible** over **broadcast + P2P** channels in the plain model

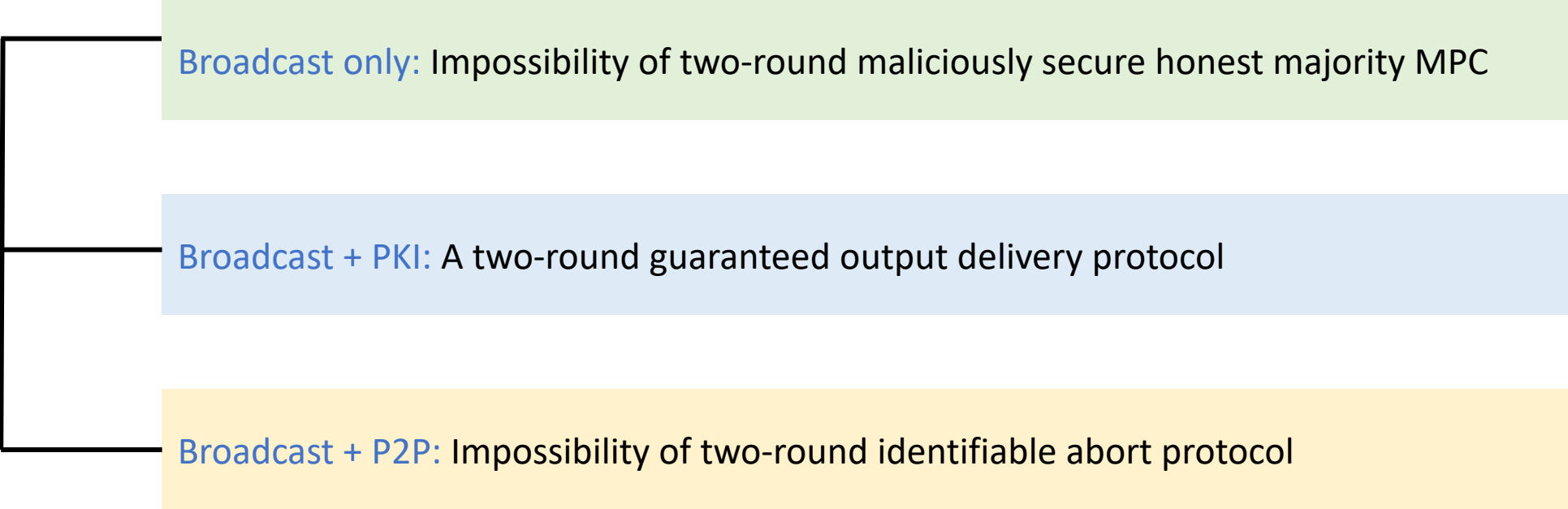
Two-round honest-majority **semi-honest/malicious** MPC over broadcast channels
 \Rightarrow **semi-honest/malicious** two-message OT

+

Two-message **malicious** OT is **impossible** in the plain model

Our Main Ideas

Talk Outline

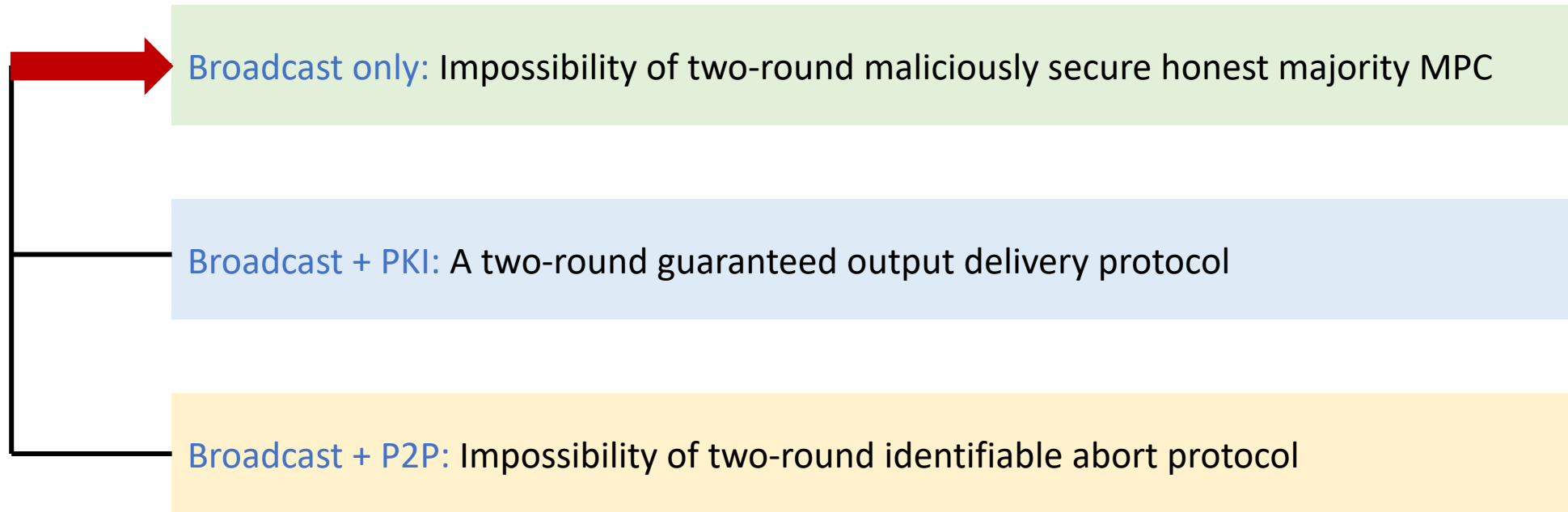


Broadcast only: Impossibility of two-round maliciously secure honest majority MPC

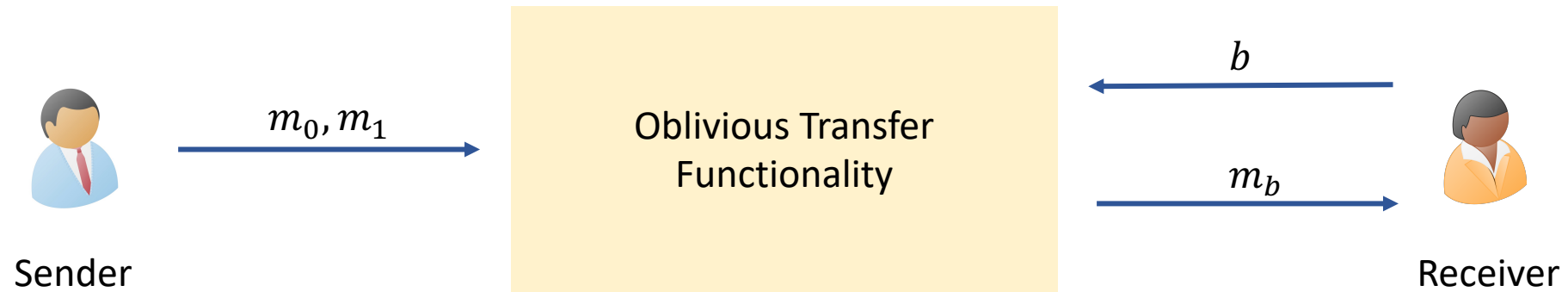
Broadcast + PKI: A two-round guaranteed output delivery protocol

Broadcast + P2P: Impossibility of two-round identifiable abort protocol

Talk Outline



Oblivious Transfer



Broadcast-Only: Two-Round MPC implies OT

Two-round broadcast-only MPC

Alice

Bob

Charlie

Round 1



Round 2



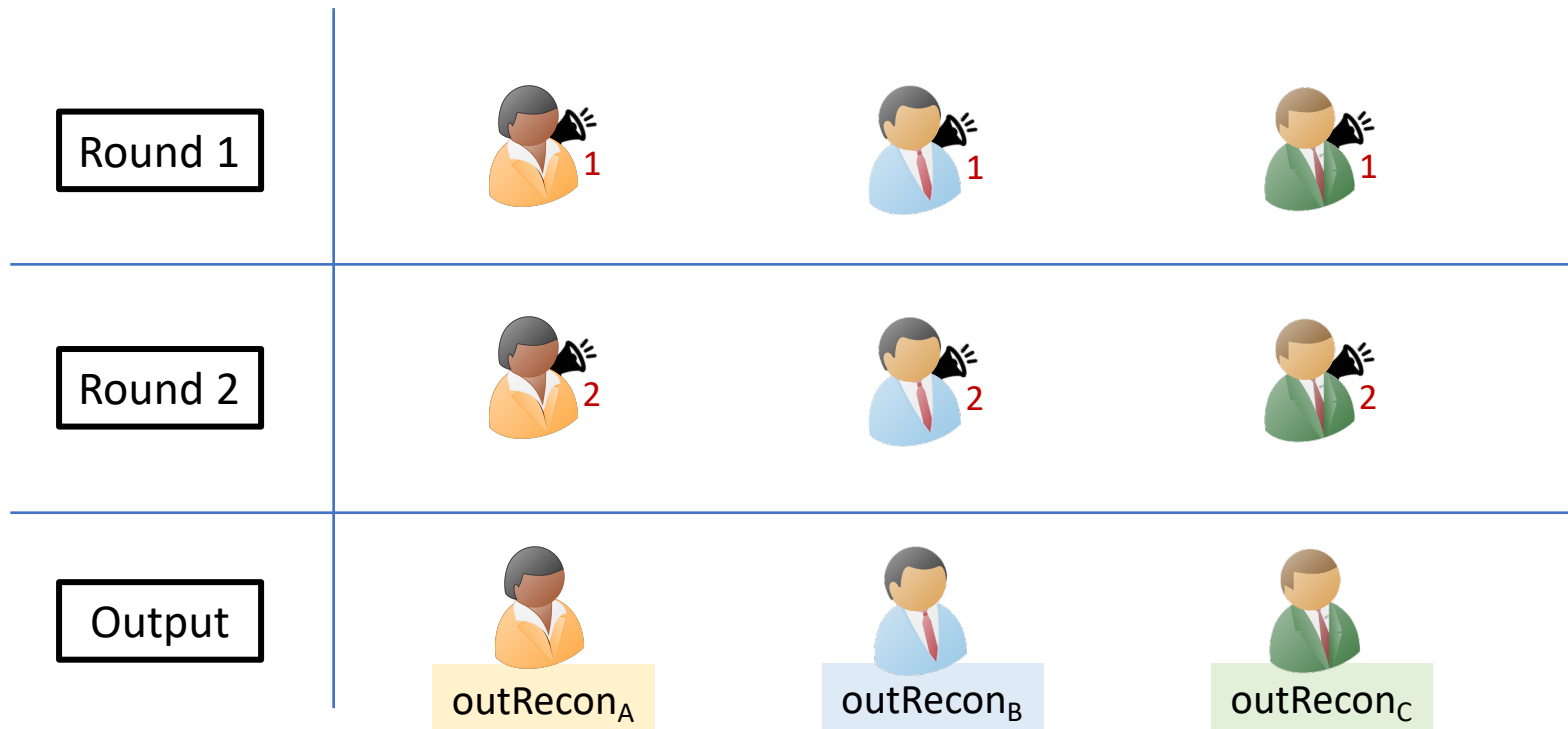
Output



Broadcast-Only: Two-Round MPC implies OT

Two-round broadcast-only MPC for

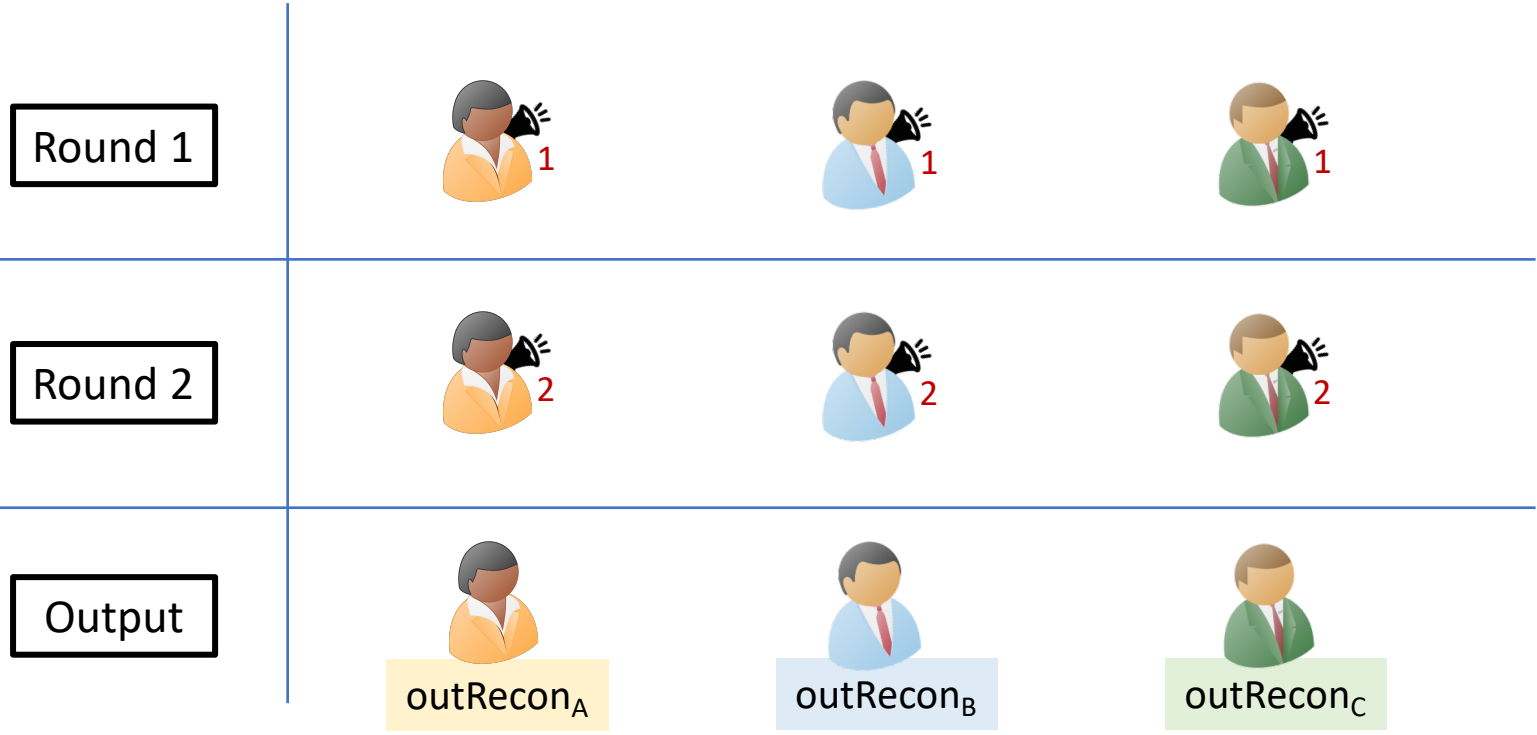
$$F\left(\begin{array}{c} \text{User A} \\ b \end{array}, \begin{array}{c} \text{User B} \\ m_0, m_1 \end{array}, \begin{array}{c} \text{User C} \\ \perp \end{array}\right) = \begin{array}{c} \text{User A} \\ m_b \end{array}, \begin{array}{c} \text{User B} \\ \perp \end{array}, \begin{array}{c} \text{User C} \\ \perp \end{array}$$



Broadcast-Only: Two-Round MPC implies OT

Receiver Sender Helper

$$F\left(\begin{array}{c} \text{Receiver} \\ b \end{array}, \begin{array}{c} \text{Sender} \\ m_0, m_1 \end{array}, \begin{array}{c} \text{Helper} \\ \perp \end{array}\right) = \begin{array}{c} \text{Receiver} \\ m_b \end{array}, \begin{array}{c} \text{Sender} \\ \perp \end{array}, \begin{array}{c} \text{Helper} \\ \perp \end{array}$$

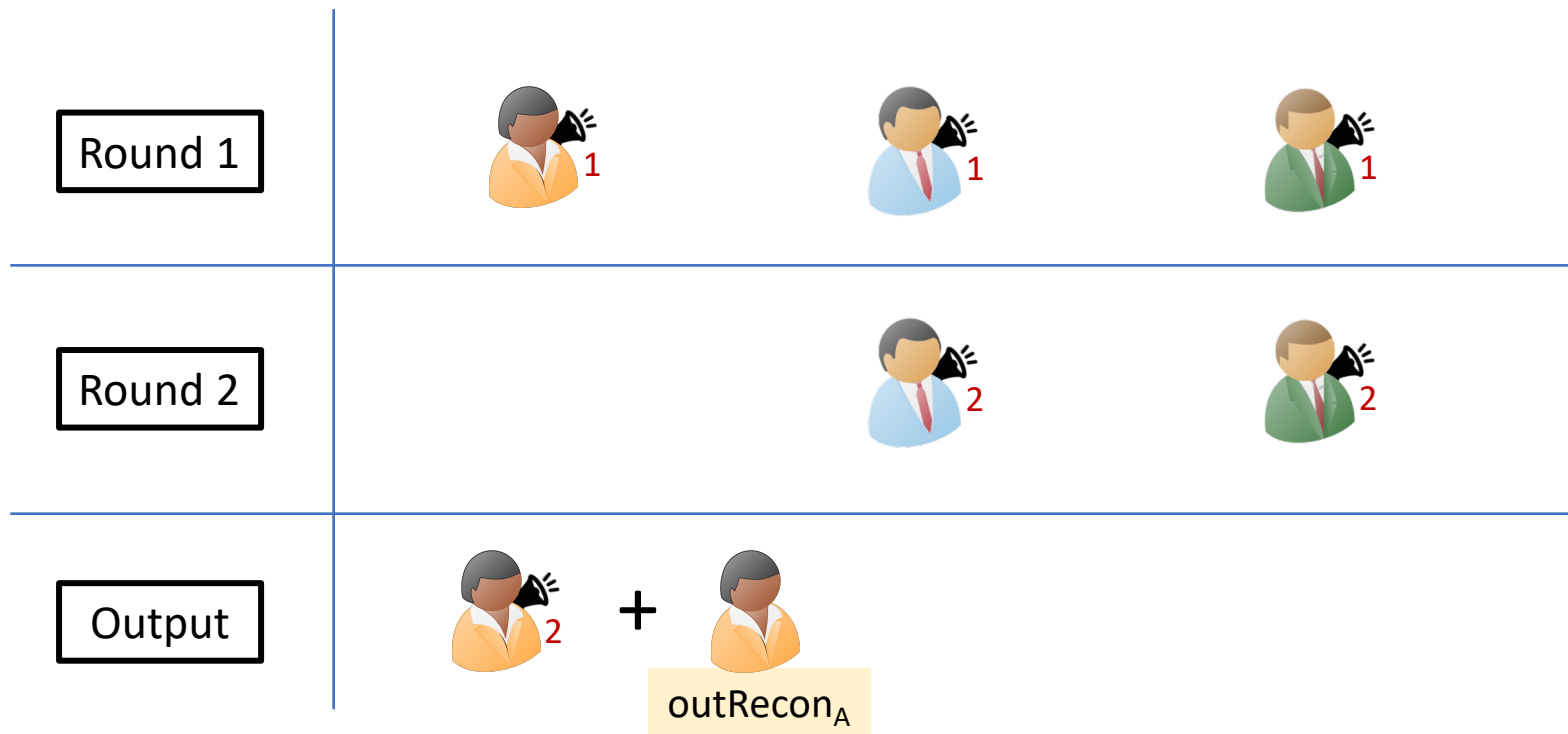


Broadcast-Only: Two-Round MPC implies OT

Two-round broadcast-only MPC for

$$F\left(\begin{array}{c} \text{Alice} \\ b \end{array}, \begin{array}{c} \text{Bob} \\ m_0, m_1 \end{array}, \begin{array}{c} \text{Charlie} \\ \perp \end{array}\right) = \begin{array}{c} \text{Alice} \\ m_b \end{array}, \begin{array}{c} \text{Bob} \\ \perp \end{array}, \begin{array}{c} \text{Charlie} \\ \perp \end{array}$$

Since Alice is the only “output-party”, it does not need to broadcast its second-round message

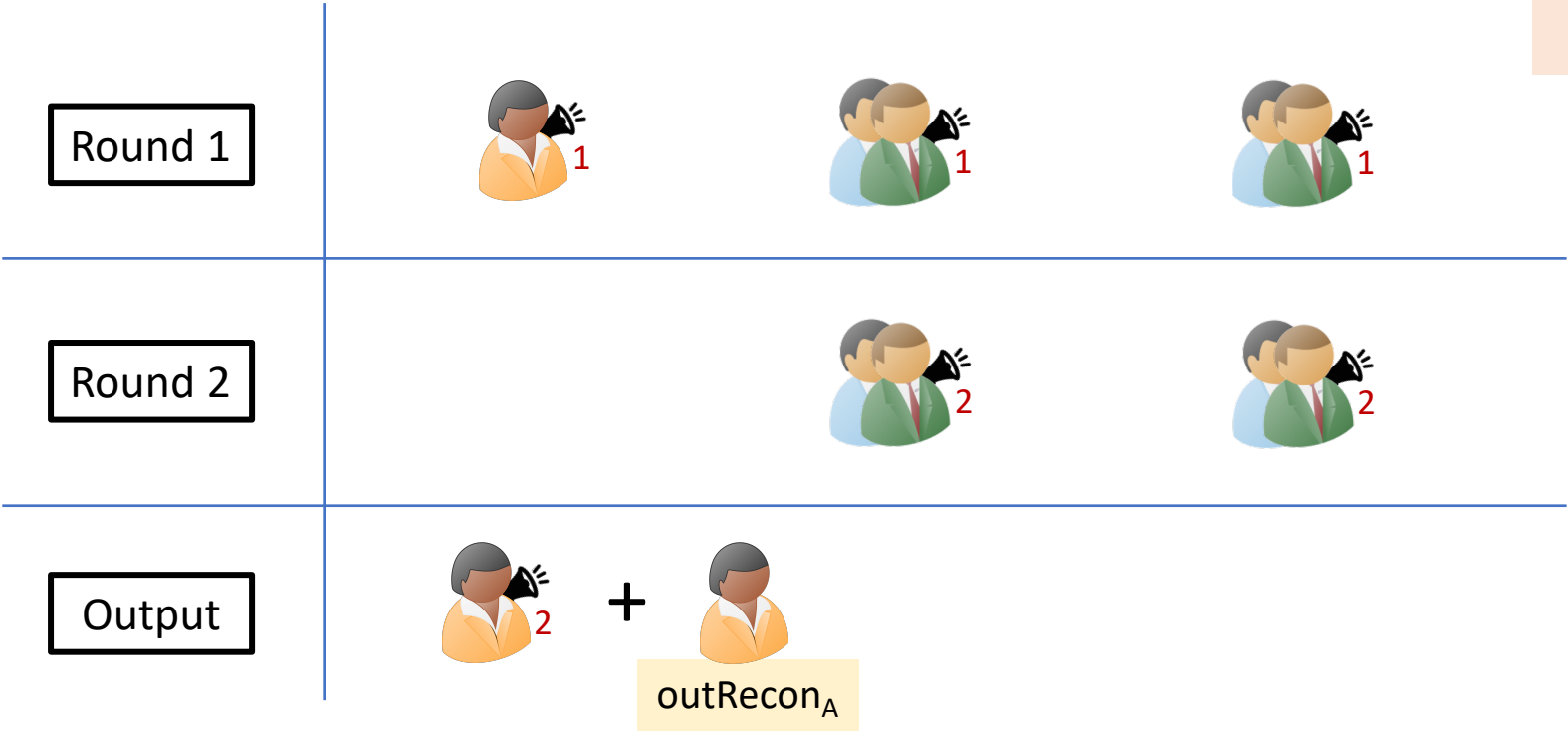


Broadcast-Only: Two-Round MPC implies OT

Two-round broadcast-only MPC for

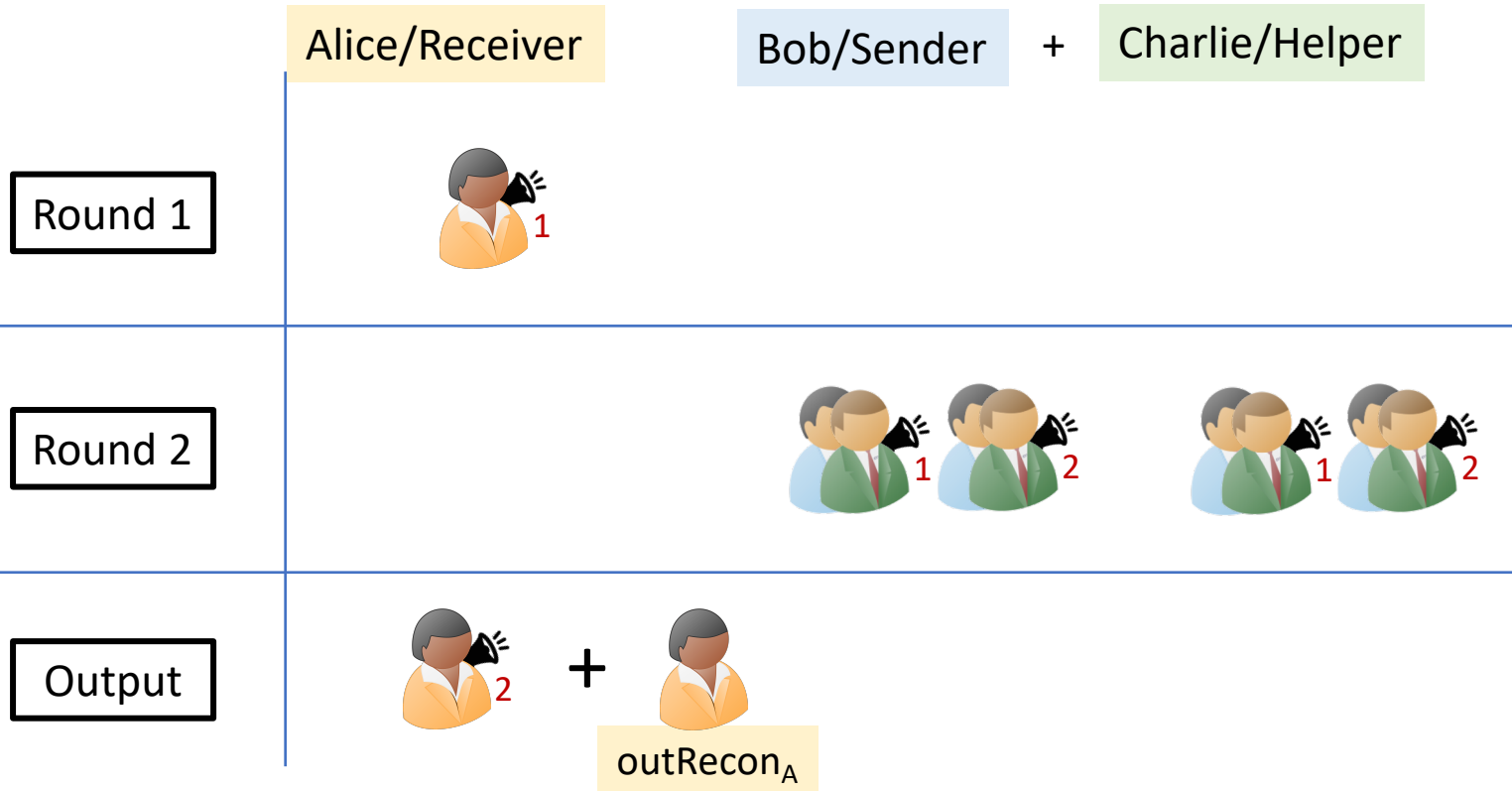
$$F\left(\begin{array}{c} \text{Alice} \\ b \end{array}, \begin{array}{c} \text{Bob, Charlie} \\ m_0, m_1 \end{array}\right) = \left(\begin{array}{c} \text{Alice} \\ m_b \end{array}, \begin{array}{c} \text{Bob, Charlie} \\ \perp \end{array}\right)$$

Modification: Bob and Charlie operate as a single party.



Two-Message OT

$$F\left(\begin{array}{c} \text{Alice} \\ b \end{array}, \begin{array}{c} \text{Bob + Charlie} \\ m_0, m_1 \end{array}\right) = \left(\begin{array}{c} \text{Alice} \\ m_b \end{array}, \begin{array}{c} \text{Bob + Charlie} \\ \perp \end{array}\right)$$



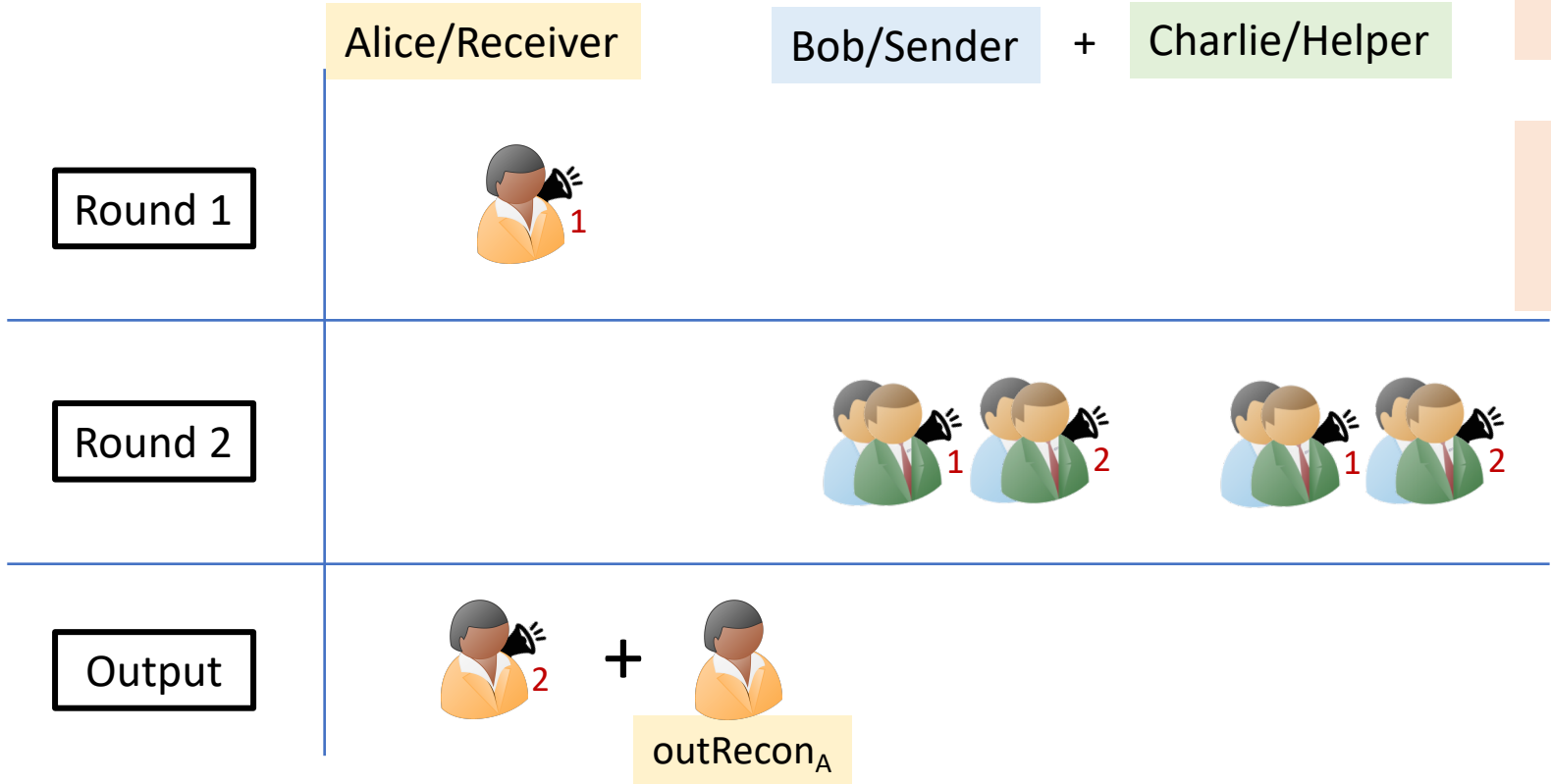
If Bob + Charlie are a single entity, they can broadcast all their messages together in the second round.

Two-Message OT: Security against Receiver

$$F\left(\begin{array}{c} \text{Alice} \\ b \end{array}, \begin{array}{c} \text{Bob, Charlie} \\ m_0, m_1 \end{array}\right) = \left(\begin{array}{c} \text{Alice} \\ m_b \end{array}, \begin{array}{c} \text{Bob, Charlie} \\ \perp \end{array}\right)$$

Security against receiver follows from security of the original two-round MPC

If the original MPC protocol was *semi-honest/malicious*, we get security against *semi-honest/malicious* receiver



Two-Message OT: Security against **Sender**

$$F\left(\begin{array}{c} \text{Alice} \\ b \end{array}, \begin{array}{c} \text{Bob} \\ m_0, m_1 \end{array}\right) = \left(\begin{array}{c} \text{Alice} \\ m_b \end{array}, \begin{array}{c} \text{Bob} \\ \perp \end{array}\right)$$

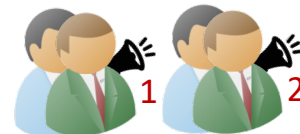
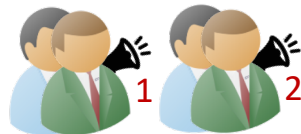
Charlie did not have an input in the original function

Alice/Receiver Bob/Sender + Charlie/Helper

Round 1

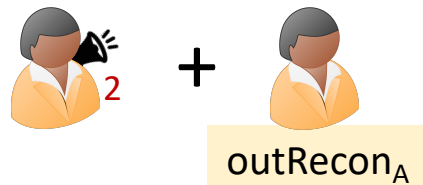


Round 2



If the adversary only corrupts Bob in the original protocol, it can obtain the same view as in this transformed 2-party protocol, by internally simulating Charlie.

Output



We get security against **semi-honest sender**

Two-Message OT

$$F\left(\begin{array}{c} \text{Alice} \\ b \end{array}, \begin{array}{c} \text{Bob} \\ m_0, m_1 \end{array}\right) = \left(\begin{array}{c} \text{Alice} \\ m_b \end{array}, \begin{array}{c} \text{Bob} \\ \perp \end{array}\right)$$

Alice/Receiver

Bob/Sender

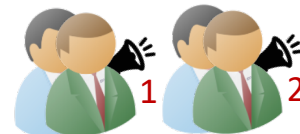
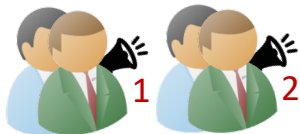
+

Charlie/Helper

Round 1



Round 2



Output



+



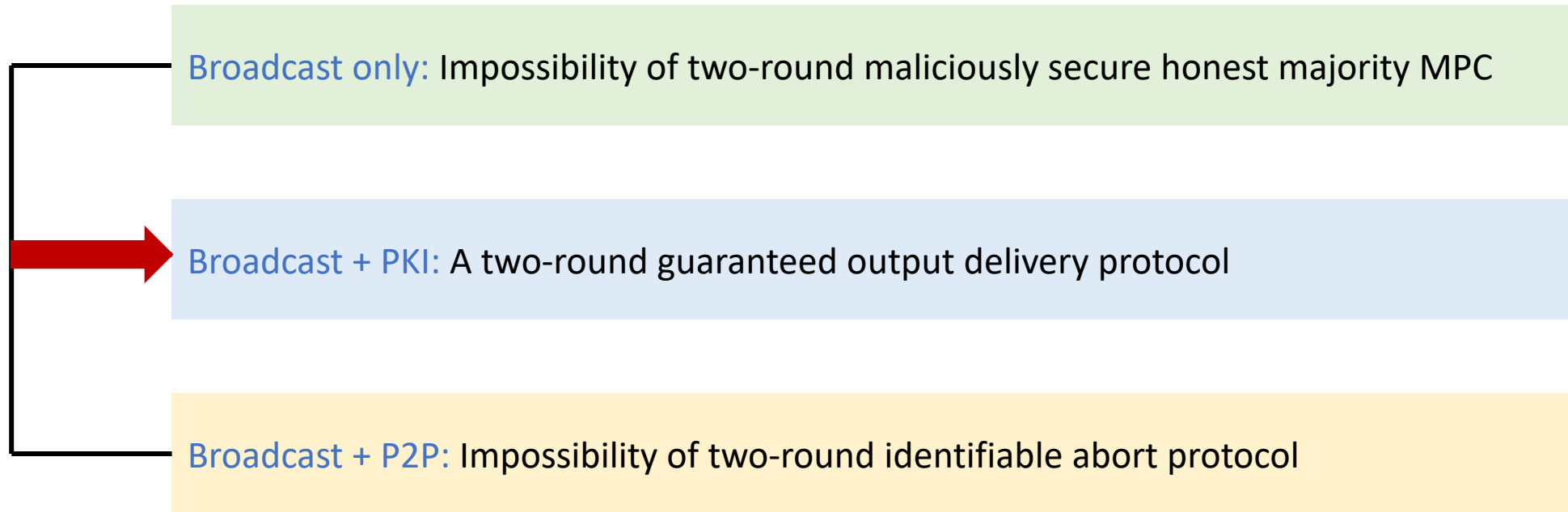
outRecon_A

A maliciously secure broadcast-only two-round MPC
⇒ Two-message malicious receiver OT

We show that a two-message malicious receiver OT is impossible

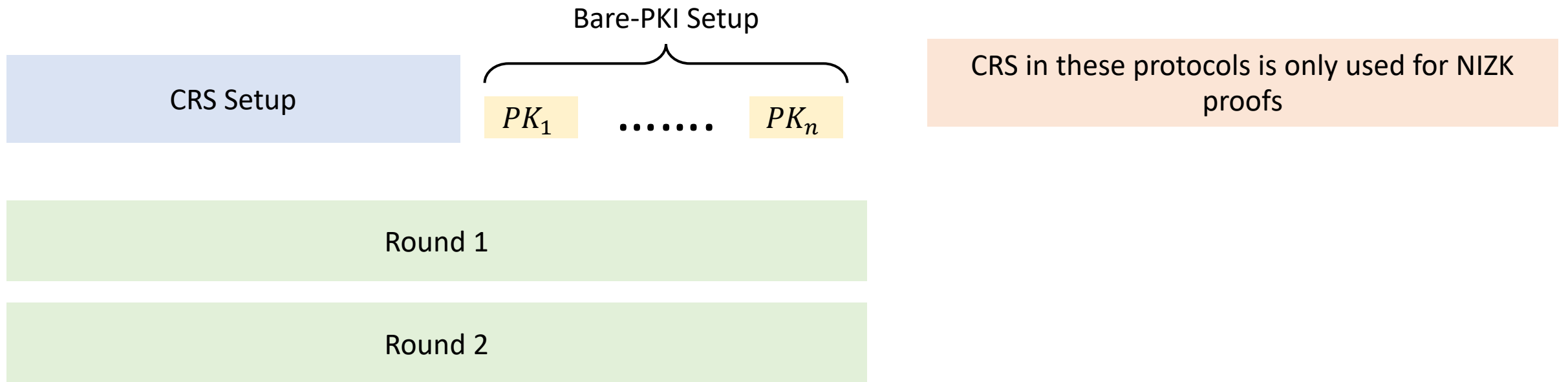
Hence, a maliciously secure broadcast-only two-round MPC is **impossible!**

Talk Outline



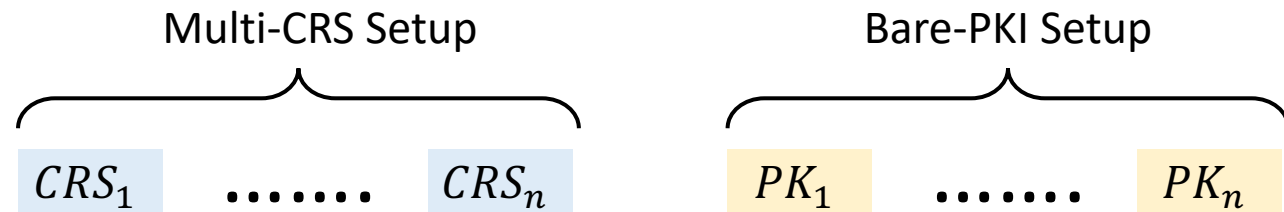
Broadcast + PKI: Guaranteed Output Delivery

Existing guaranteed output delivery protocols (e.g. [GLS'18]) in the broadcast + PKI setting, rely on a trusted CRS setup



Broadcast + PKI: Guaranteed Output Delivery

Existing guaranteed output delivery protocols (e.g. [GLS'18]) in the broadcast + PKI setting, rely on a trusted CRS setup



Round 1

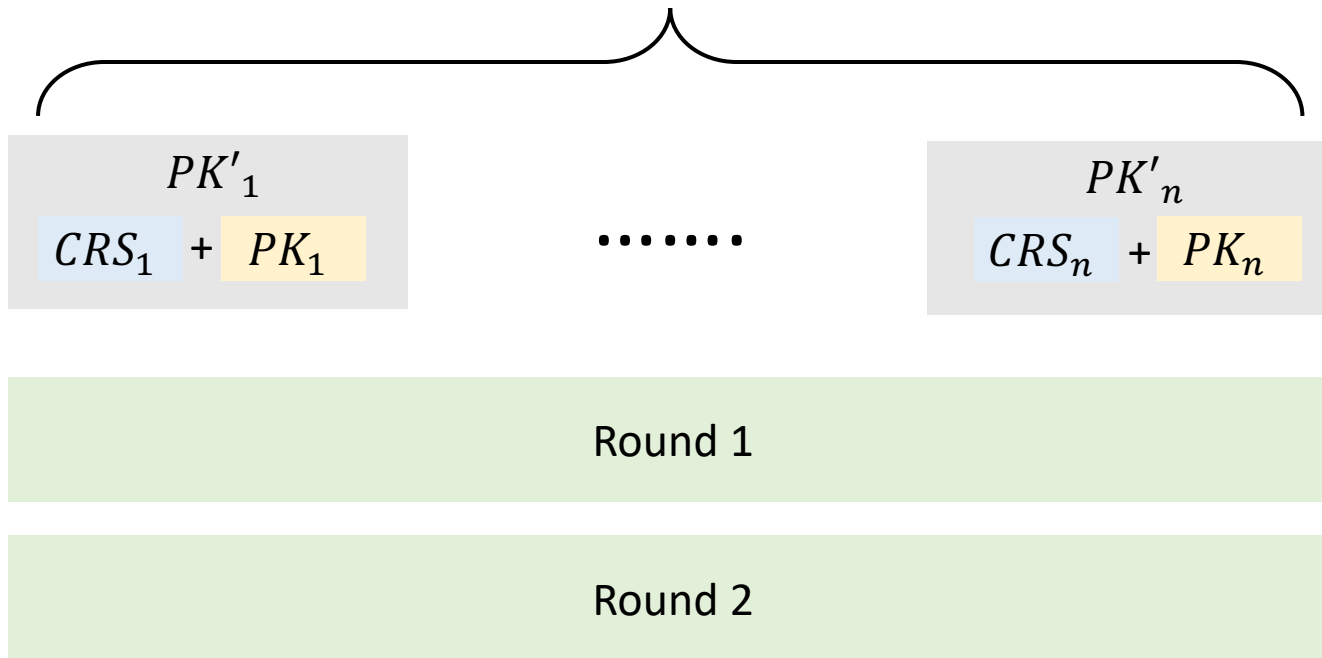
Round 2

CRS in these protocols is only used for NIZK proofs

NIZKs in the honest majority setting can be replaced with multi-CRS NIZKs [GO'07]

Broadcast + PKI: Guaranteed Output Delivery

Existing guaranteed output delivery protocols (e.g. [GLS'18]) in the broadcast + PKI setting, rely on a trusted CRS setup



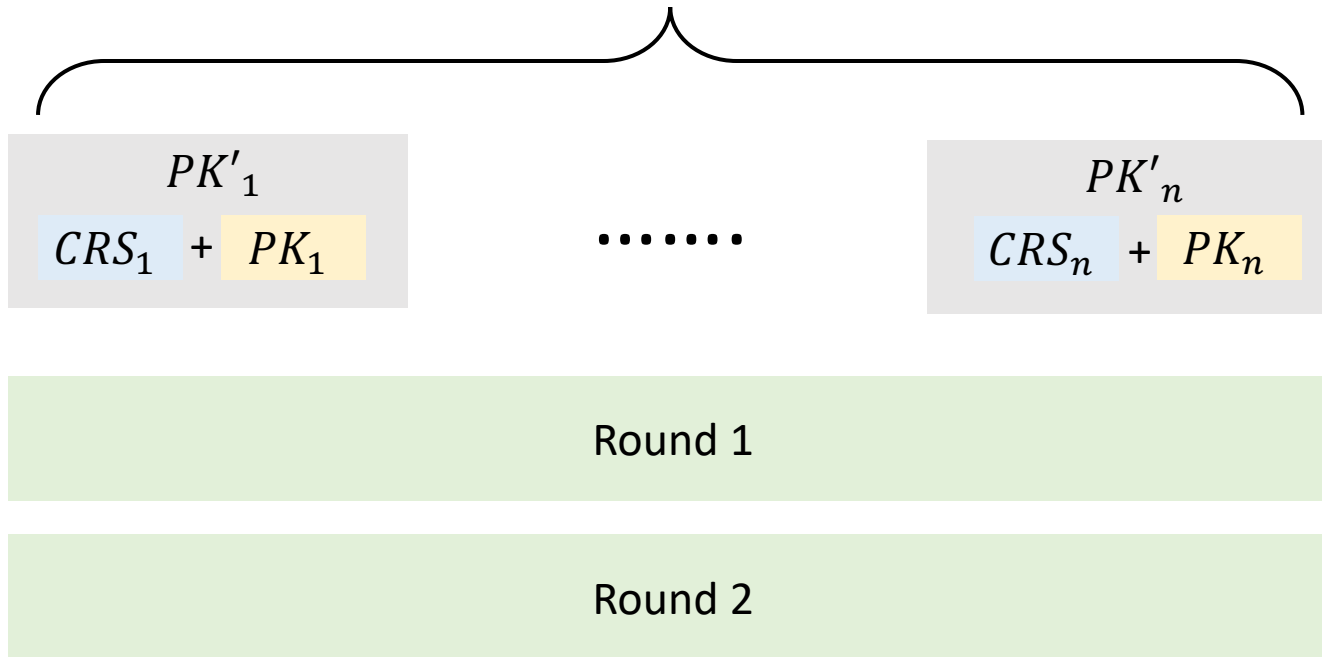
CRS in these protocols is only used for NIZK proofs

NIZKs in the honest majority setting can be replaced with multi-CRS NIZKs [GO'07]

Multi-CRS can be embedded inside the bare-PKI setup

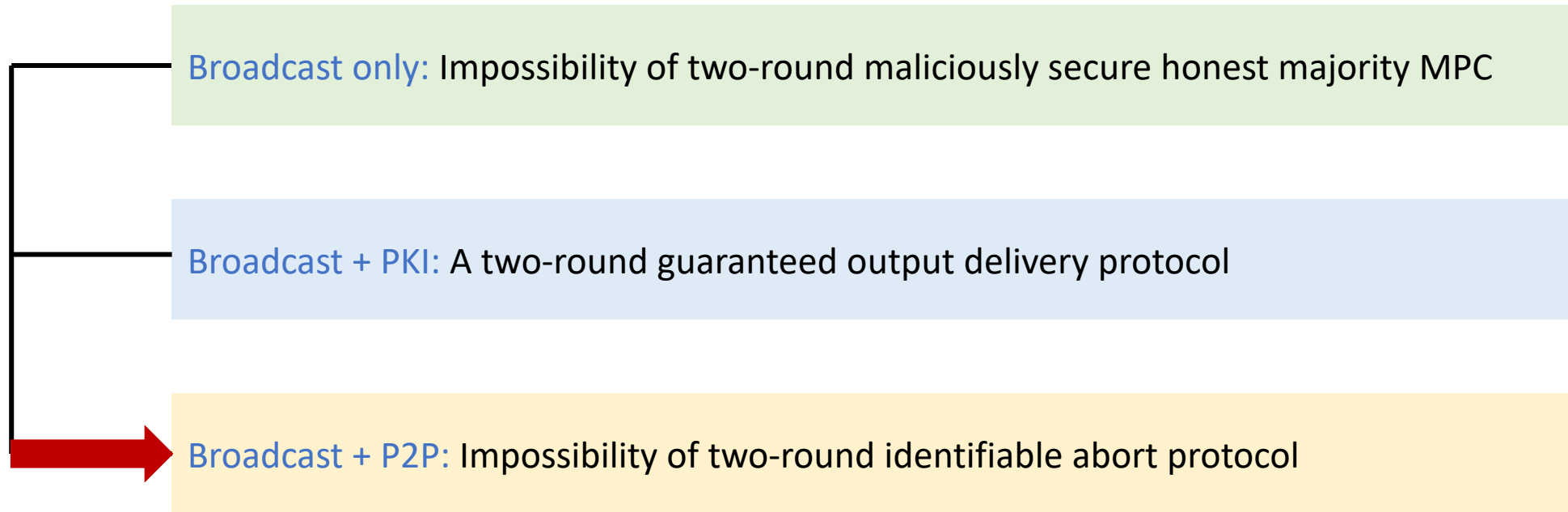
Broadcast + PKI: Guaranteed Output Delivery

Bare-PKI Setup



This gives us a two-round guaranteed output delivery protocol without CRS!

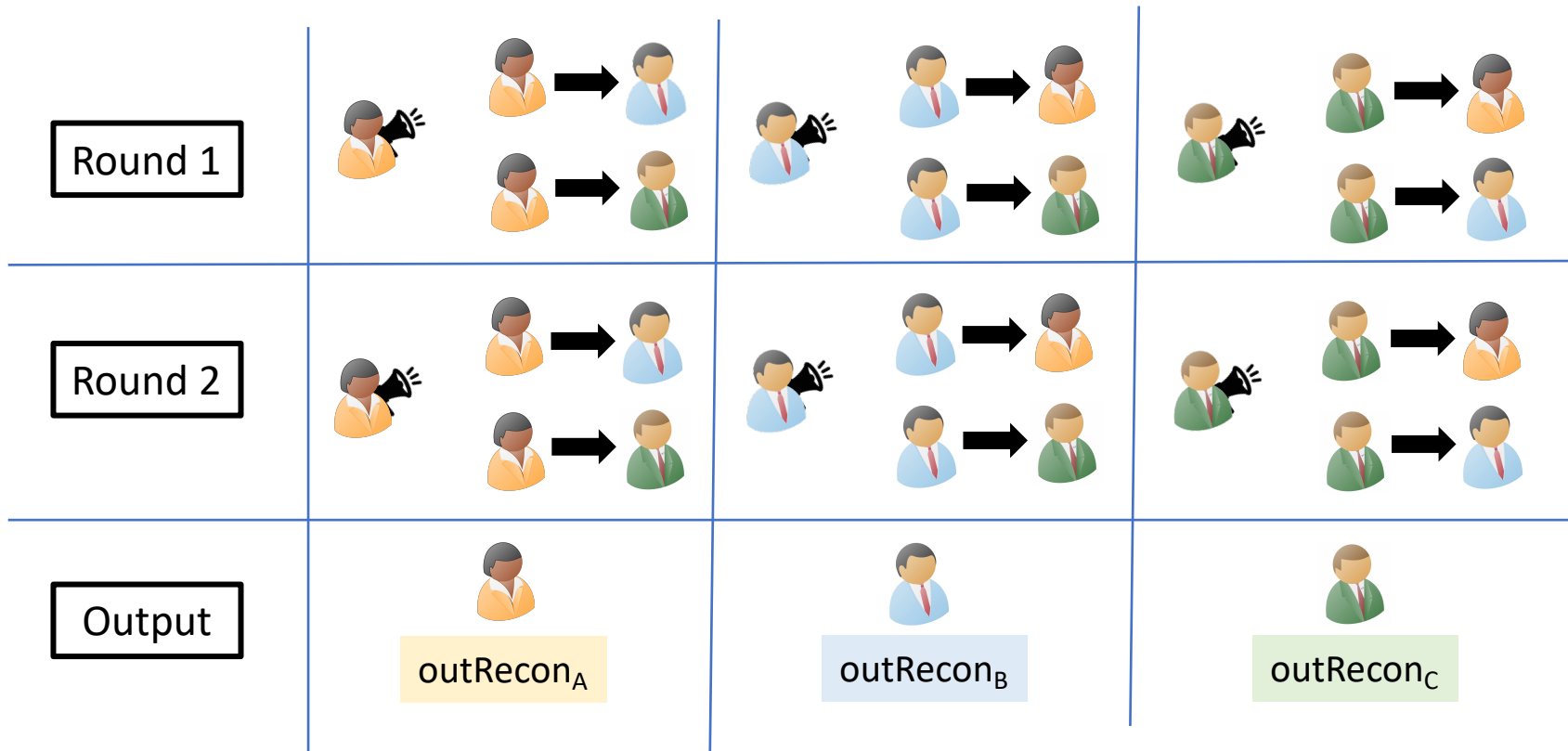
Talk Outline



Broadcast + P2P: Identifiable Abort is Impossible

Assume FSOC, \exists a two-round identifiable abort protocol for

$$F\left(\begin{array}{c} \text{A} \\ b \end{array}, \begin{array}{c} \text{B} \\ m_0, m_1 \end{array}, \begin{array}{c} \text{C} \\ \perp \end{array}\right) = \left(\begin{array}{c} \text{A} \\ \perp \end{array}, \begin{array}{c} \text{B} \\ \perp \end{array}, \begin{array}{c} \text{C} \\ m_b \end{array}\right)$$

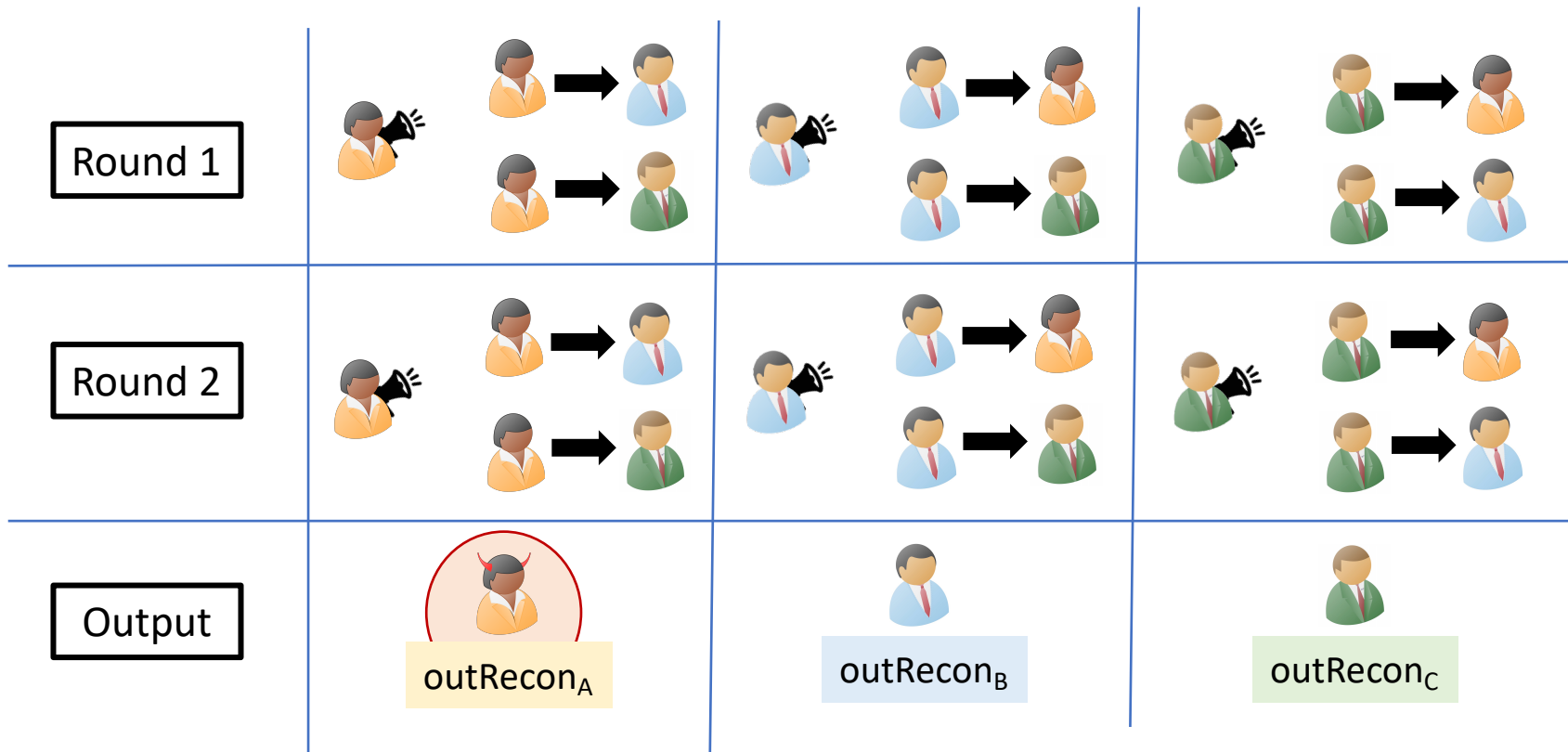


Broadcast + P2P: Identifiable Abort is Impossible

Assume FSOC, \exists a two-round identifiable abort protocol for

$$F\left(\begin{array}{c} \text{Alice} \\ b \end{array}, \begin{array}{c} \text{Bob} \\ m_0, m_1 \end{array}, \begin{array}{c} \text{Charlie} \\ \perp \end{array}\right) = \left(\begin{array}{c} \text{Alice} \\ \perp \end{array}, \begin{array}{c} \text{Bob} \\ \perp \end{array}, \begin{array}{c} \text{Charlie} \\ m_b \end{array}\right)$$

Adversary corrupts Alice



Broadcast + P2P: Identifiable Abort is Impossible

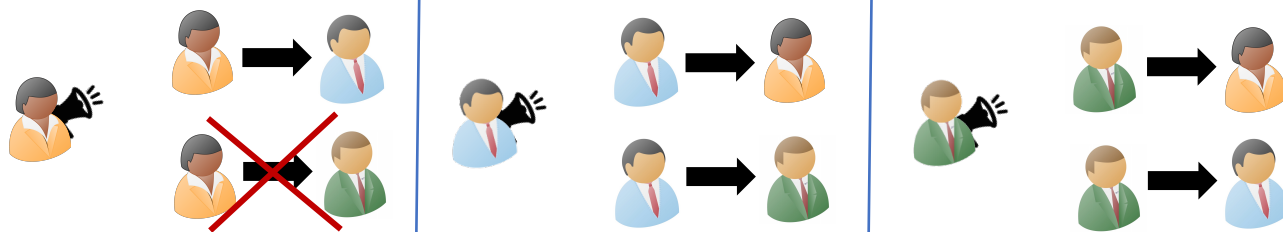
Assume FSOC, \exists a two-round identifiable abort protocol for

$$F\left(\begin{array}{c} \text{Alice} \\ b \end{array}, \begin{array}{c} \text{Bob} \\ m_0, m_1 \end{array}, \begin{array}{c} \text{Charlie} \\ \perp \end{array}\right) = \left(\begin{array}{c} \text{Alice} \\ \perp \end{array}, \begin{array}{c} \text{Bob} \\ \perp \end{array}, \begin{array}{c} \text{Charlie} \\ m_b \end{array}\right)$$

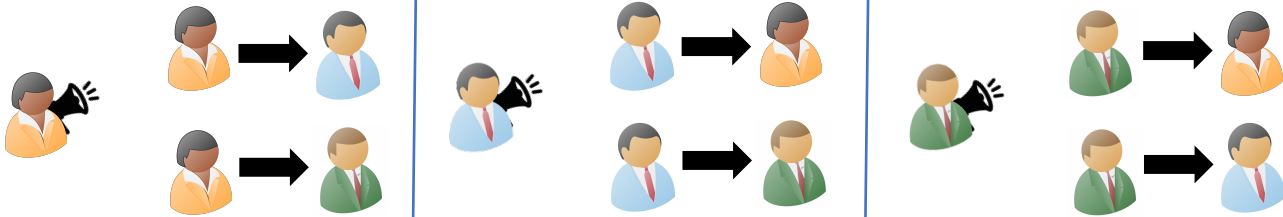
Adversary corrupts Alice

Alice doesn't send private message to Charlie

Round 1



Round 2



Output



Broadcast + P2P: Identifiable Abort is Impossible

Assume FSOC, \exists a two-round identifiable abort protocol for

$$F\left(\begin{array}{c} \text{Alice} \\ b \end{array}, \begin{array}{c} \text{Bob} \\ m_0, m_1 \end{array}, \begin{array}{c} \text{Charlie} \\ \perp \end{array}\right) = \left(\begin{array}{c} \text{Alice} \\ \perp \end{array}, \begin{array}{c} \text{Bob} \\ \perp \end{array}, \begin{array}{c} \text{Charlie} \\ m_b \end{array}\right)$$

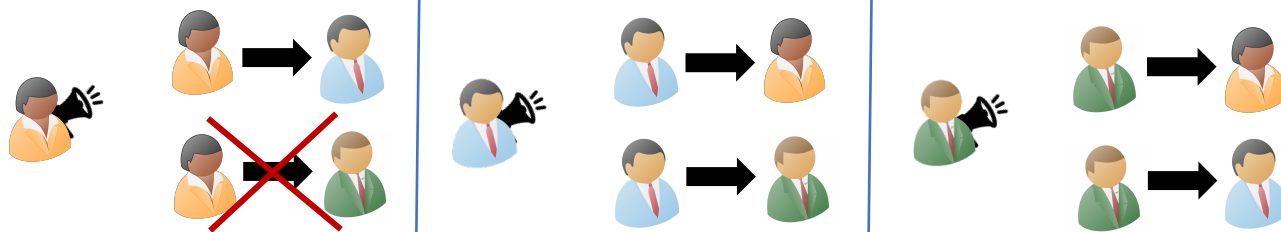
Adversary corrupts Alice

Alice doesn't send private message to Charlie

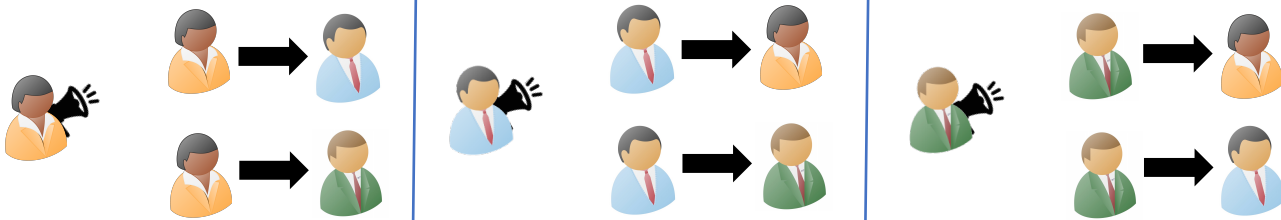
Honest parties should :

1. Either abort and identify the corrupt party
2. Or do not abort

Round 1



Round 2



Output



Broadcast + P2P: Identifiable Abort is Impossible

Assume FSOC, \exists a two-round identifiable abort protocol for

$$F\left(\begin{array}{c} \text{Person A} \\ b \end{array}, \begin{array}{c} \text{Person B} \\ m_0, m_1 \end{array}, \begin{array}{c} \text{Person C} \\ \perp \end{array}\right) = \left(\begin{array}{c} \text{Person A} \\ \perp \end{array}, \begin{array}{c} \text{Person B} \\ \perp \end{array}, \begin{array}{c} \text{Person C} \\ m_b \end{array}\right)$$

| | | | |
|---------|-----------------------------|-----------------------------|-----------------------------|
| Round 1 | | | |
| Round 2 | | | |
| Output | <p>outRecon_A</p> | <p>outRecon_B</p> | <p>outRecon_C</p> |

Case 1: Lets assume the honest parties abort

If outputs \perp , then all honest parties should identify as corrupt.

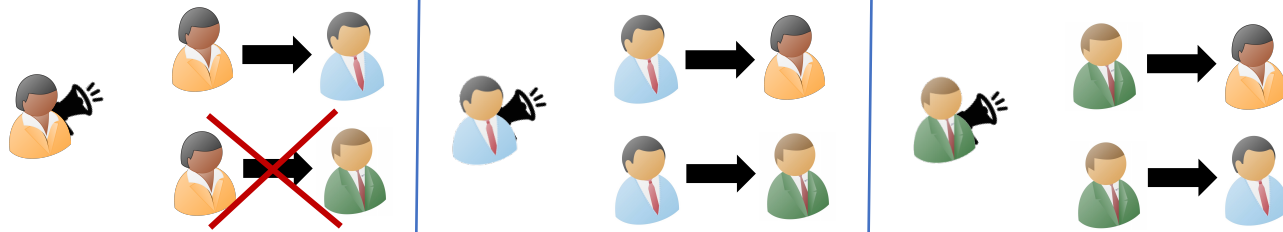
But has no reason to believe why would be corrupt.

Broadcast + P2P: Identifiable Abort is Impossible

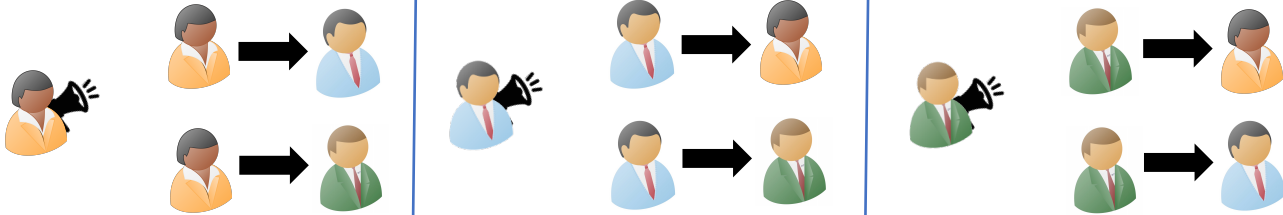
Assume FSOC, \exists a two-round identifiable abort protocol for

$$F\left(\begin{array}{c} \text{Person A} \\ b \end{array}, \begin{array}{c} \text{Person B} \\ m_0, m_1 \end{array}, \begin{array}{c} \text{Person C} \\ \perp \end{array}\right) = \left(\begin{array}{c} \text{Person A} \\ \perp \end{array}, \begin{array}{c} \text{Person B} \\ \perp \end{array}, \begin{array}{c} \text{Person C} \\ m_b \end{array}\right)$$

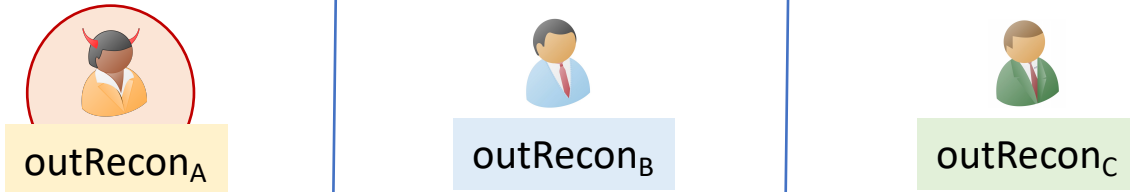
Round 1



Round 2



Output



~~Case 1:~~ Lets assume the honest parties abort

If Person C outputs \perp , then all honest parties should identify Person A as corrupt.

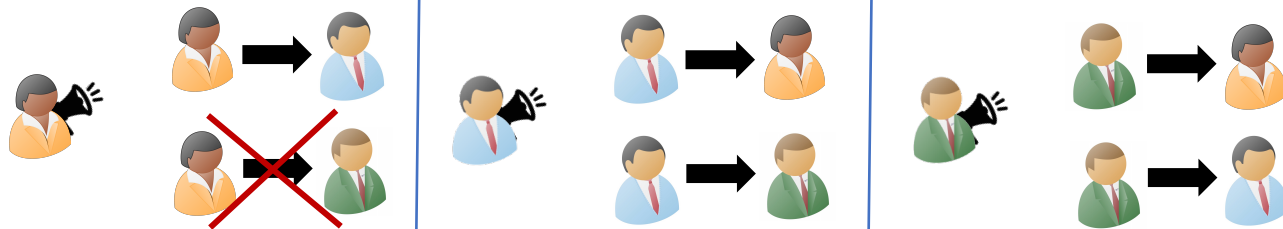
But Person B has no reason to believe why Person A would be corrupt.

Broadcast + P2P: Identifiable Abort is Impossible

$$F\left(\begin{array}{c} \text{Person A} \\ b \end{array}, \begin{array}{c} \text{Person B} \\ m_0, m_1 \end{array}, \begin{array}{c} \text{Person C} \\ \perp \end{array}\right) = \left(\begin{array}{c} \text{Person A} \\ \perp \end{array}, \begin{array}{c} \text{Person B} \\ \perp \end{array}, \begin{array}{c} \text{Person C} \\ m_b \end{array}\right)$$

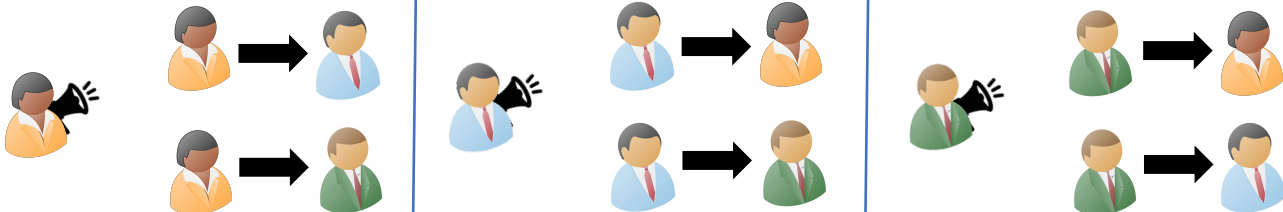
Case 2: Lets assume the honest parties **do not** abort

Round 1



1. The simulator extracts b as Person A's input.

Round 2



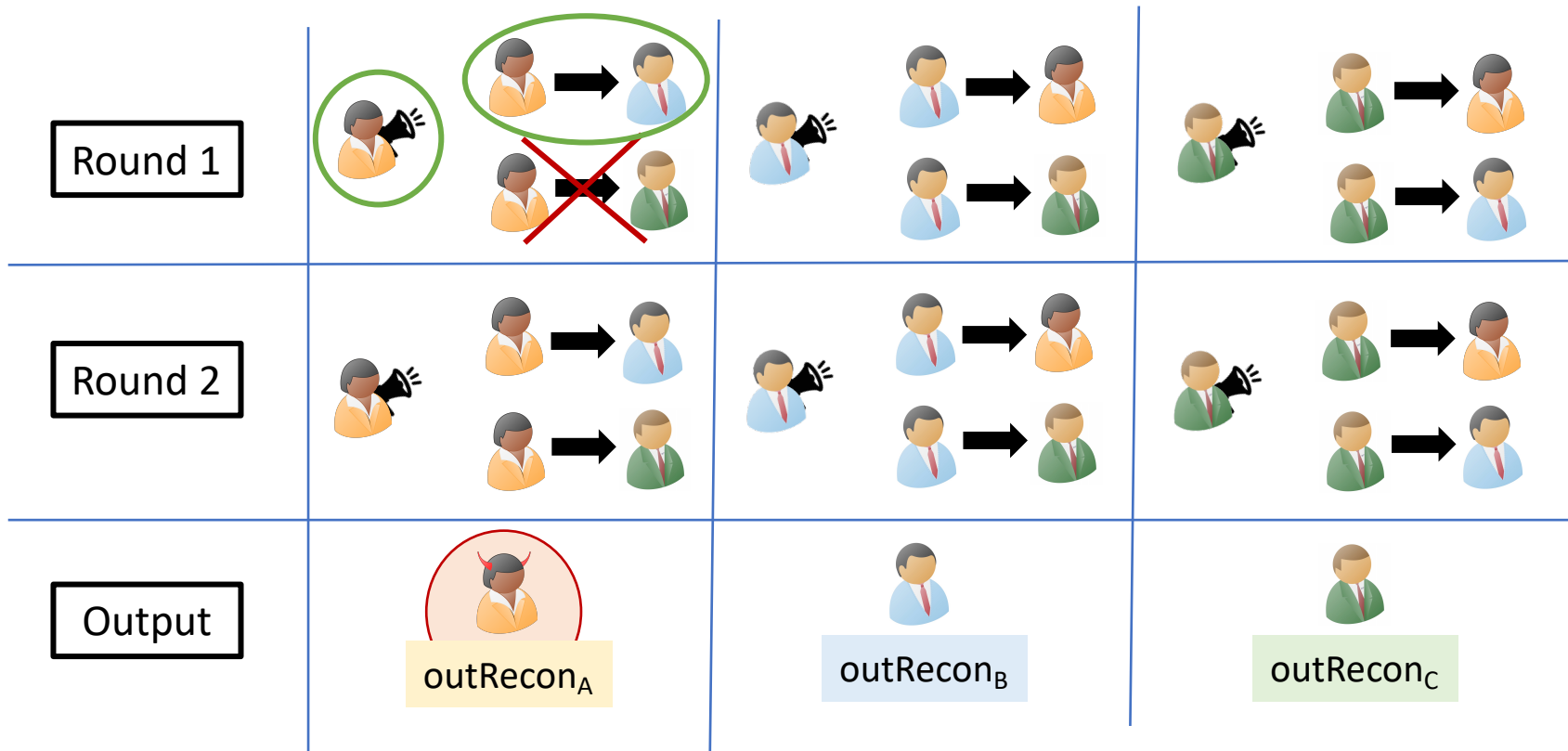
2. The simulator extracts $1 - b$ as Person A's input.

Output



Broadcast + P2P: Identifiable Abort is Impossible

$$F\left(\begin{matrix} \text{Person A} \\ b \end{matrix}, \begin{matrix} \text{Person B} \\ m_0, m_1 \end{matrix}, \begin{matrix} \text{Person C} \\ \perp \end{matrix}\right) = \left(\begin{matrix} \text{Person A} \\ \perp \end{matrix}, \begin{matrix} \text{Person B} \\ \perp \end{matrix}, \begin{matrix} \text{Person C} \\ m_b \end{matrix}\right)$$



Case 2: Lets assume the honest parties **do not** abort

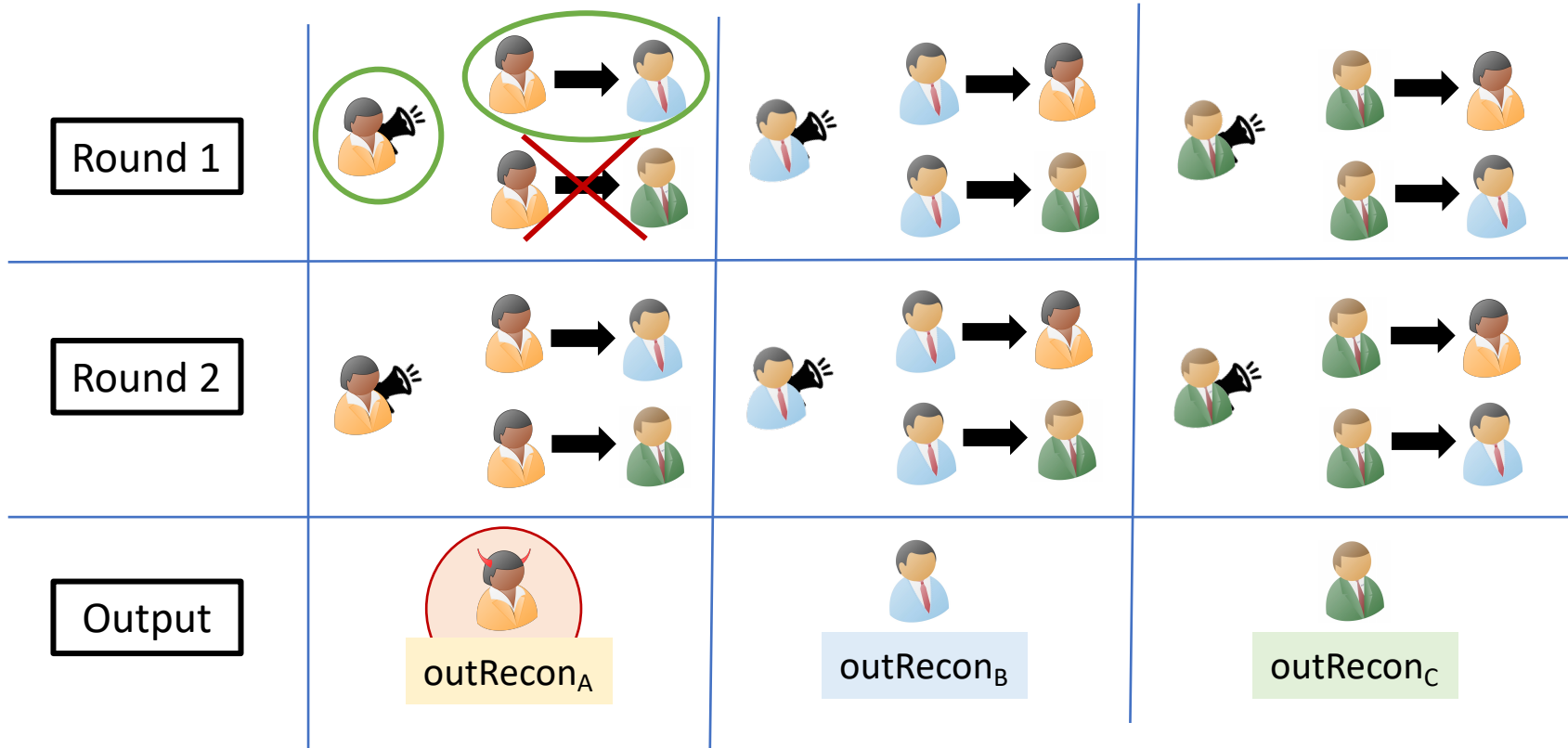
1. The simulator extracts b as Person A's input.

A corrupt Person B can use the same simulator algorithm to violate Person A's privacy


2. The simulator extracts $1 - b$ as Person A's input.



Broadcast + P2P: Identifiable Abort is Impossible


$$F\left(\begin{matrix} \text{Person A} \\ b \end{matrix}, \begin{matrix} \text{Person B} \\ m_0, m_1 \end{matrix}, \begin{matrix} \text{Person C} \\ \perp \end{matrix}\right) = \left(\begin{matrix} \text{Person A} \\ \perp \end{matrix}, \begin{matrix} \text{Person B} \\ \perp \end{matrix}, \begin{matrix} \text{Person C} \\ m_b \end{matrix}\right)$$



Case 2: Lets assume the honest parties **do not** abort

1. ~~The simulator extracts b as 's input.~~

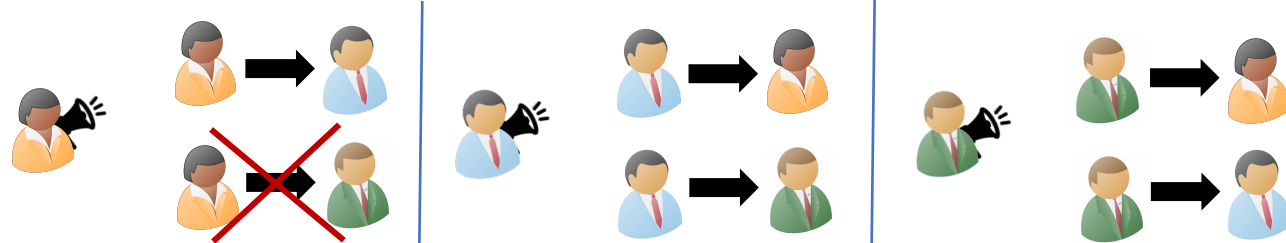
A corrupt  can use the same simulator algorithm to violate 's privacy

2. The simulator extracts $1 - b$ as 's input.

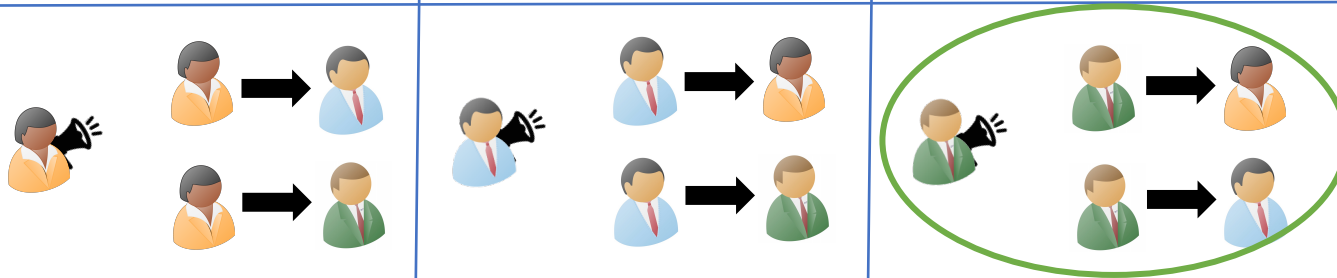
Broadcast + P2P: Identifiable Abort is Impossible

$$F\left(\begin{matrix} \text{Person A} \\ b \end{matrix}, \begin{matrix} \text{Person B} \\ m_0, m_1 \end{matrix}, \begin{matrix} \text{Person C} \\ \perp \end{matrix}\right) = \left(\begin{matrix} \text{Person A} \\ \perp \end{matrix}, \begin{matrix} \text{Person B} \\ \perp \end{matrix}, \begin{matrix} \text{Person C} \\ m_b \end{matrix}\right)$$

Round 1



Round 2



Output



Case 2: Lets assume the honest parties **do not** abort

1. ~~The simulator extracts b as Person A's input.~~

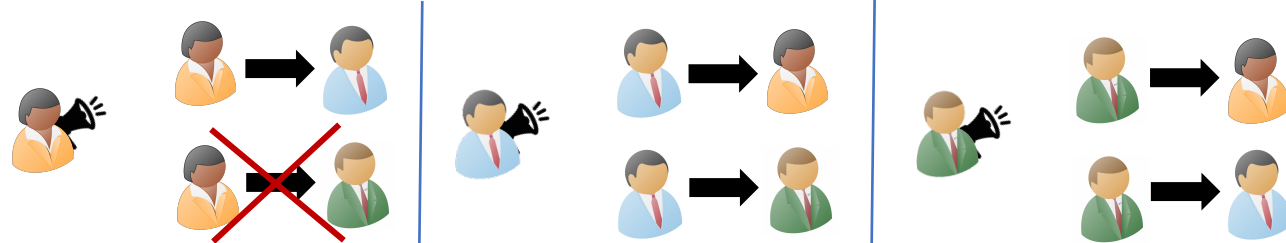
2. The simulator extracts $1 - b$ as Person A's input.

A corrupt Person C can launch a residual function attack to violate Person A's privacy

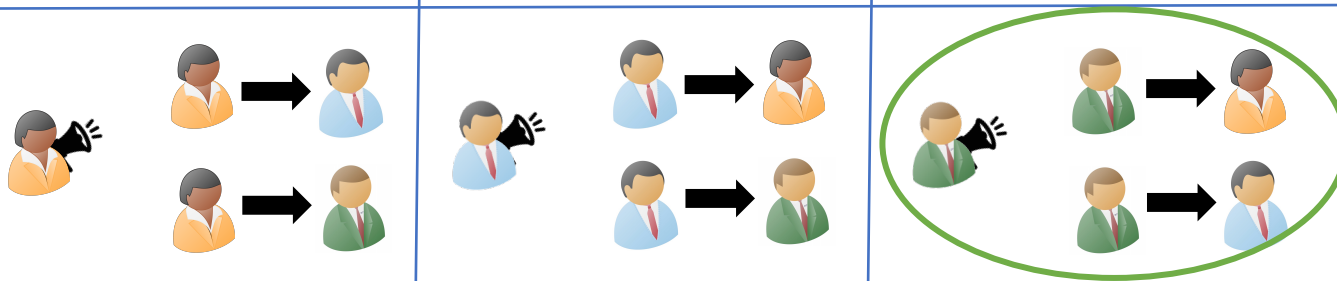
Broadcast + P2P: Identifiable Abort is Impossible

$$F\left(\begin{matrix} \text{Person A} \\ b \end{matrix}, \begin{matrix} \text{Person B} \\ m_0, m_1 \end{matrix}, \begin{matrix} \text{Person C} \\ \perp \end{matrix}\right) = \left(\begin{matrix} \text{Person A} \\ \perp \end{matrix}, \begin{matrix} \text{Person B} \\ \perp \end{matrix}, \begin{matrix} \text{Person C} \\ m_b \end{matrix}\right)$$

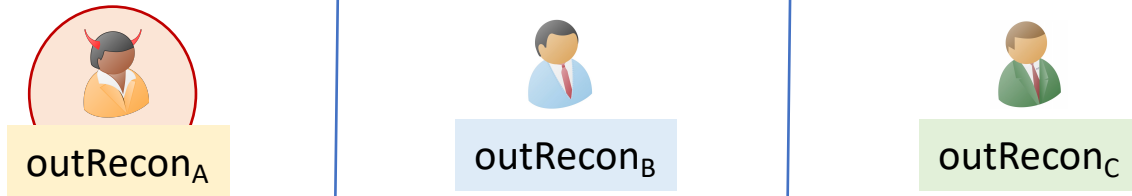
Round 1



Round 2



Output



Case 2: Lets assume the honest parties **do not** abort

~~1. The simulator extracts b as 's input.~~

~~2. The simulator extracts $1 - b$ as 's input.~~

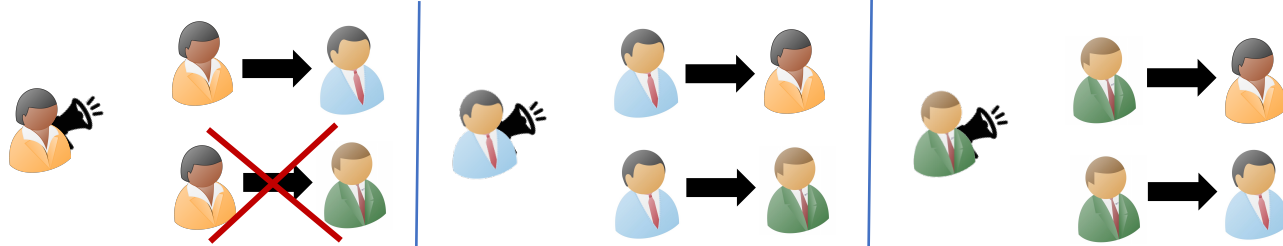
A corrupt can launch a residual function attack to violate 's privacy

Broadcast + P2P: Identifiable Abort is Impossible

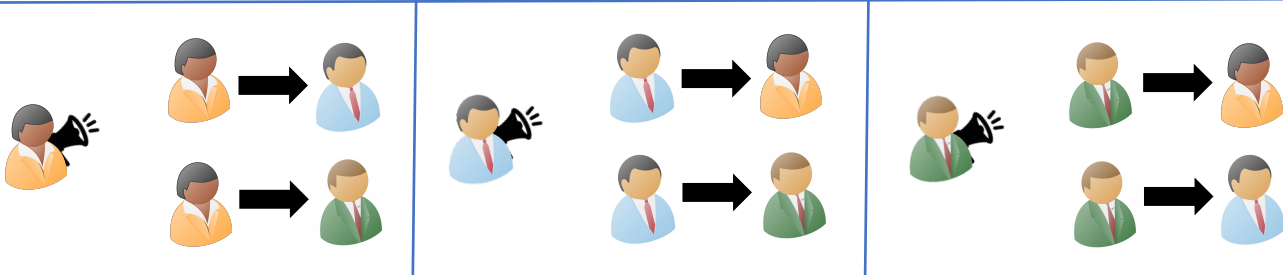
Assume FSOC, \exists a two-round identifiable abort protocol for

$$F\left(\begin{array}{c} \text{Alice} \\ b \end{array}, \begin{array}{c} \text{Bob} \\ m_0, m_1 \end{array}, \begin{array}{c} \text{Charlie} \\ \perp \end{array}\right) = \left(\begin{array}{c} \text{Alice} \\ \perp \end{array}, \begin{array}{c} \text{Bob} \\ \perp \end{array}, \begin{array}{c} \text{Charlie} \\ m_b \end{array}\right)$$

Round 1



Round 2



Output



Adversary corrupts Alice

Alice doesn't send private message to Charlie

Honest parties should :

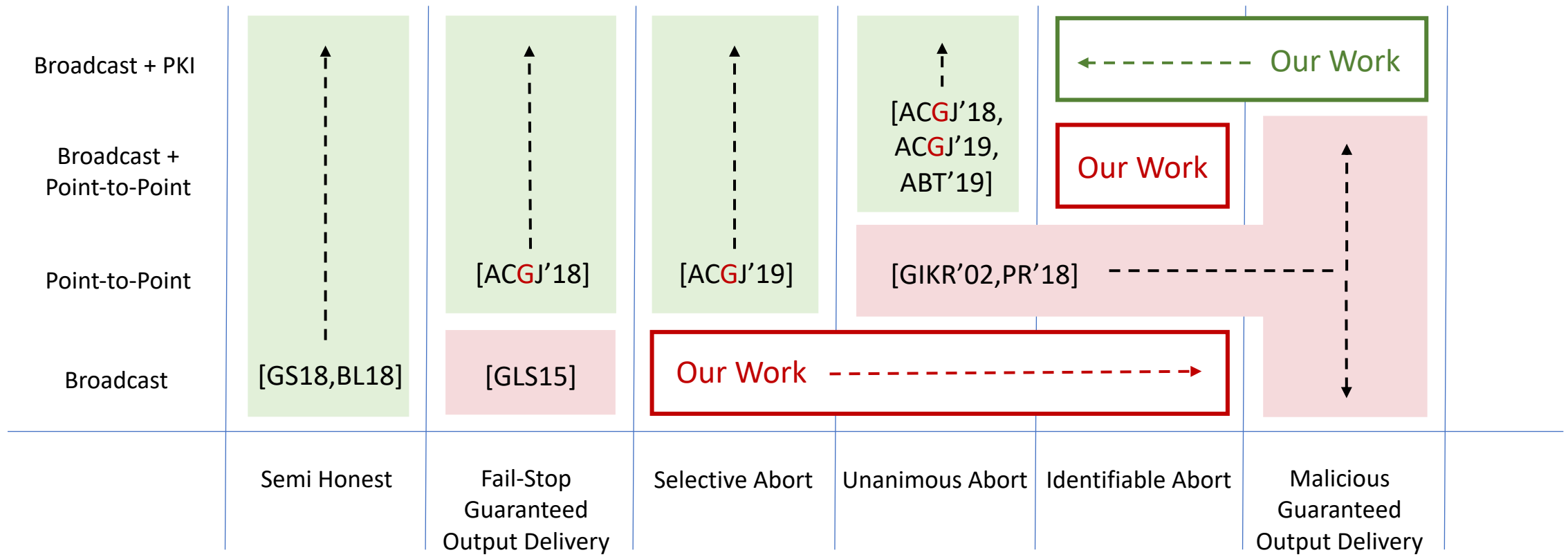
1. Either abort and identify the corrupt party
2. Or do not abort

Neither of these cases are true!

No such identifiable abort protocol exists!

Conclusion: Two-Round MPC

Broadcast < Point-to-Point < Broadcast + Point-to-Point < Broadcast + PKI



<https://eprint.iacr.org/2021/690>

Thank You!