Round Optimal Secure Multiparty Computation from Minimal Assumptions

Arka Rai Choudhuri
Johns Hopkins University

Michele Ciampi
The University of Edinburgh

Vipul Goyal
Carnegie Mellon University and NTT Research

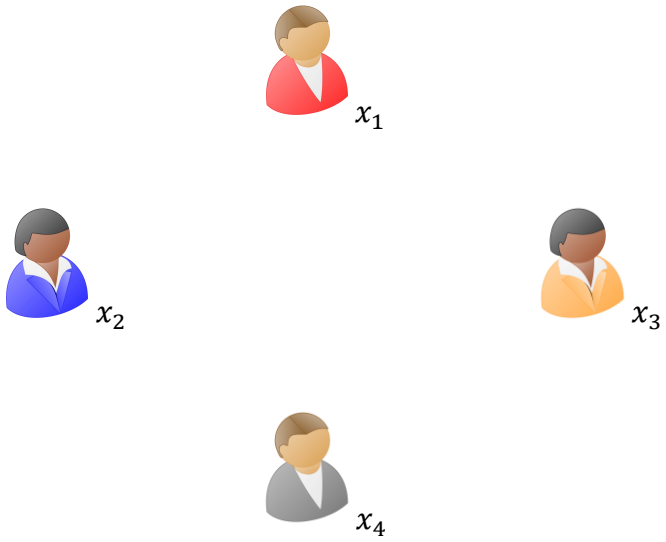
Abhishek Jain
Johns Hopkins University

Rafail Ostrovsky
University of California Los Angeles

TCC 2020

Multiparty Computation (MPC)

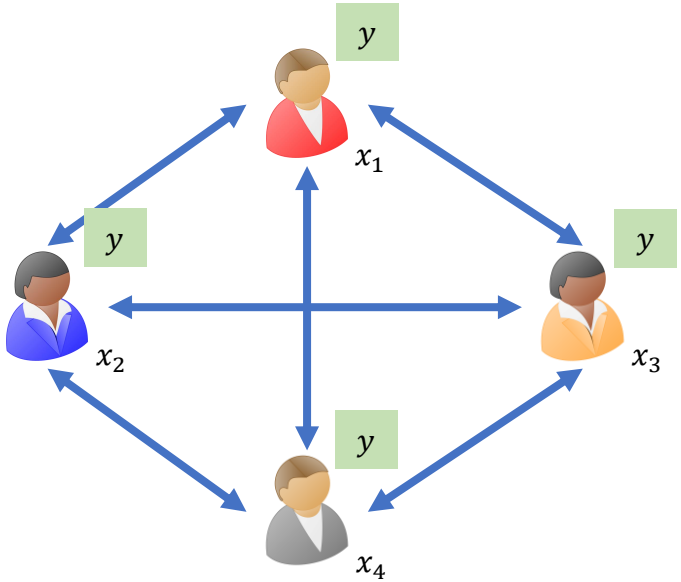
[Yao'86, Goldreich-Micali-Wigderson'87]



$y = f(x_1, x_2, x_3, x_4)$

Multiparty Computation (MPC)

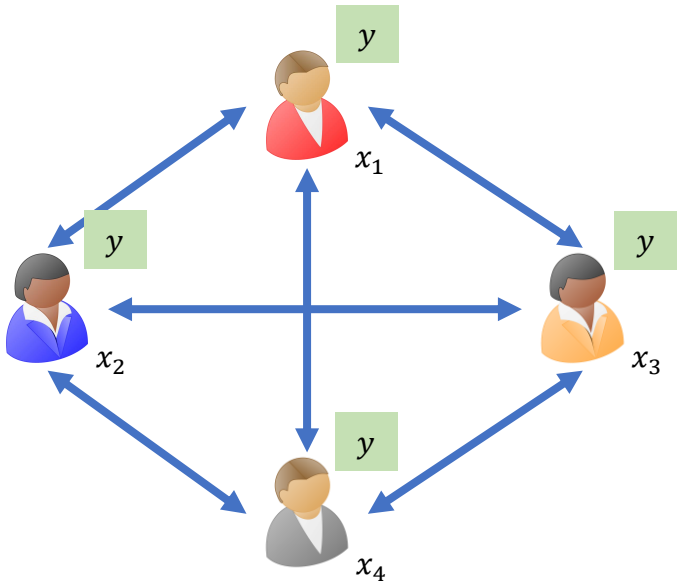
[Yao'86, Goldreich-Micali-Wigderson'87]



$$y = f(x_1, x_2, x_3, x_4)$$

Multiparty Computation (MPC)

[Yao'86, Goldreich-Micali-Wigderson'87]

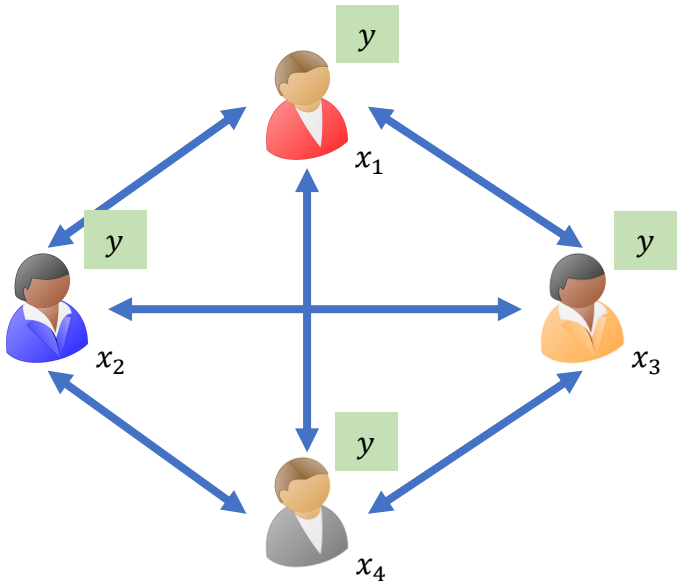


$y = f(x_1, x_2, x_3, x_4)$

A **round** constitutes of every participant sending a message.

Multiparty Computation (MPC)

[Yao'86, Goldreich-Micali-Wigderson'87]

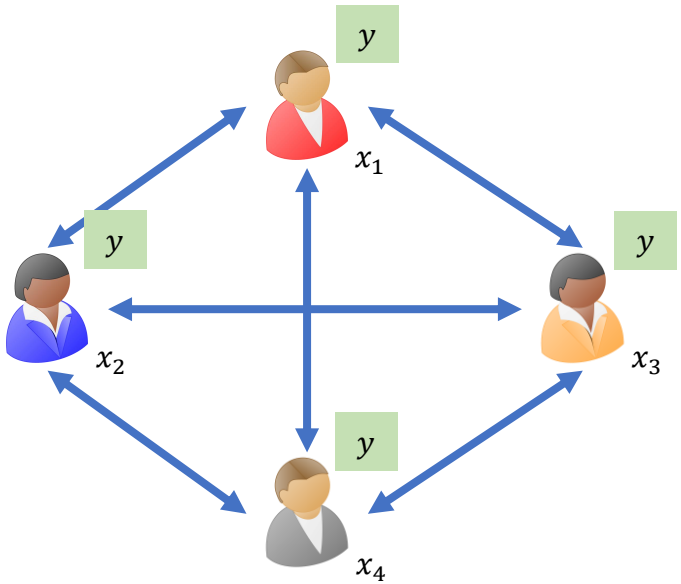


$y = f(x_1, x_2, x_3, x_4)$

A **round** constitutes of every participant sending a message.

Goal: For efficiency, **minimize rounds of interaction**.

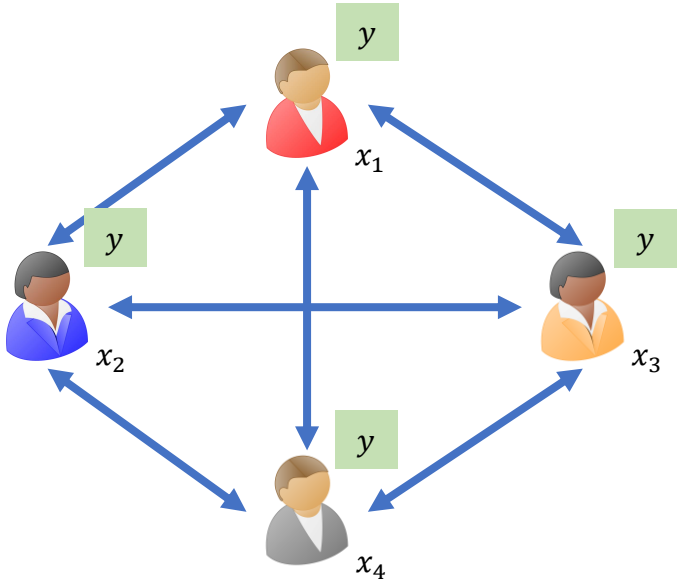
Security



$y = f(x_1, x_2, x_3, x_4)$

Misbehaving participants should not learn anything beyond the output of the function.

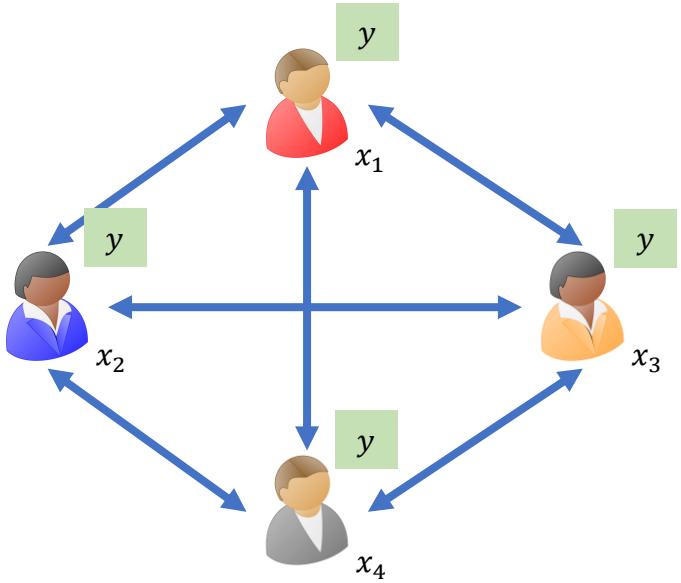
Security



$$y = f(x_1, x_2, x_3, x_4)$$

Security

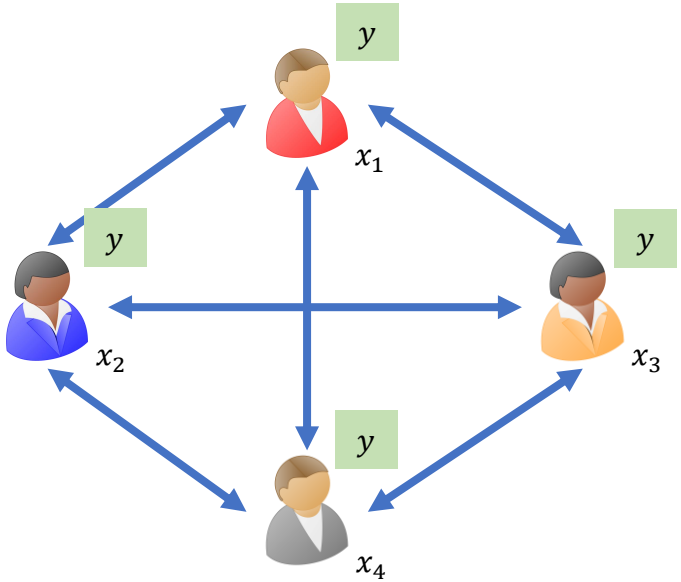
real world



$$y = f(x_1, x_2, x_3, x_4)$$

Security

real world

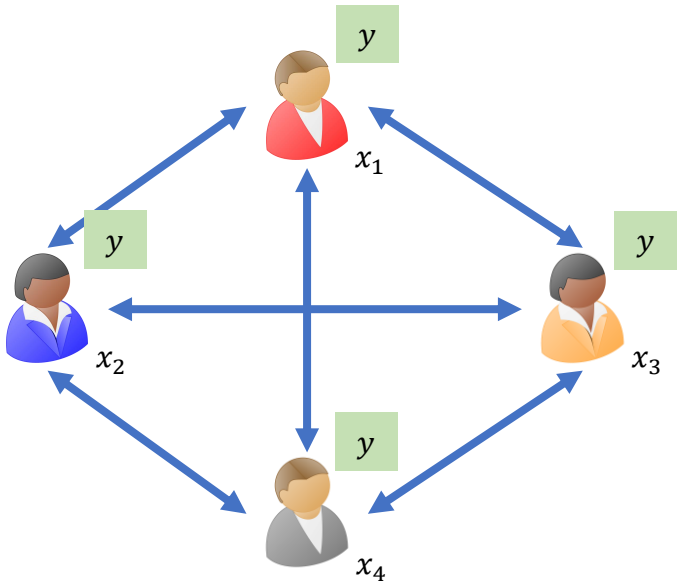


$y = f(x_1, x_2, x_3, x_4)$

ideal world

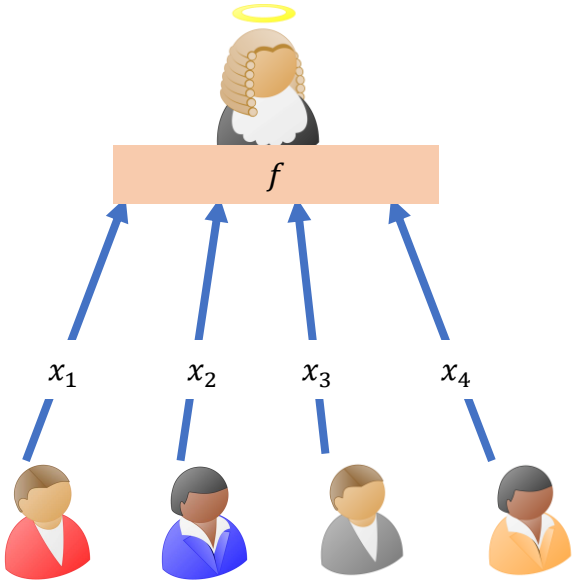
Security

real world



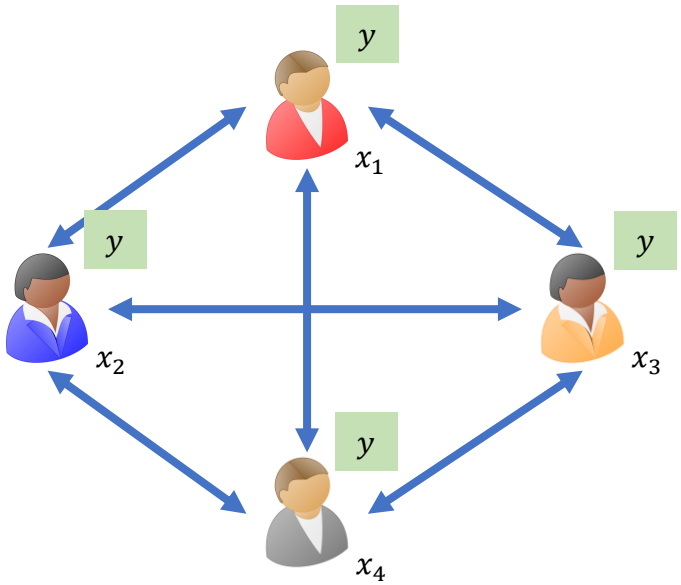
$y = f(x_1, x_2, x_3, x_4)$

ideal world



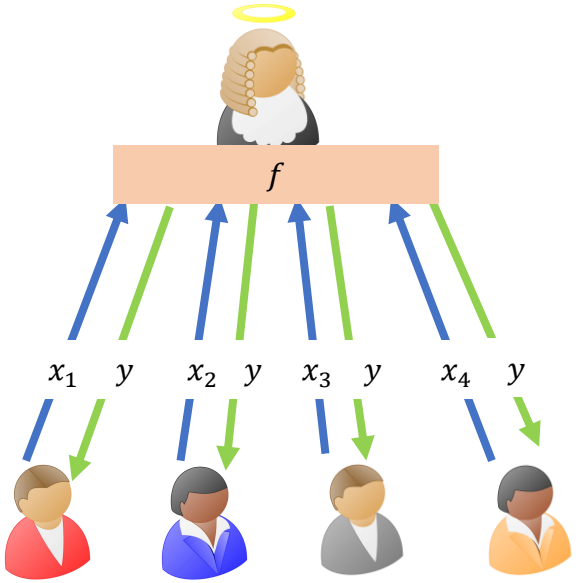
Security

real world



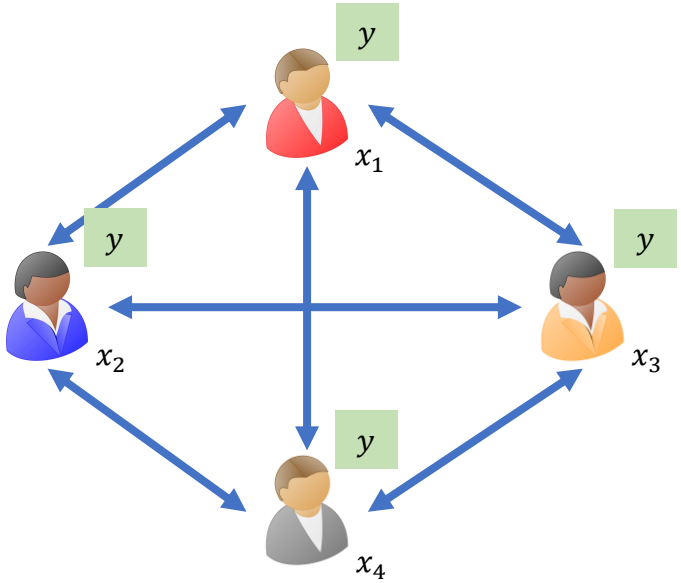
$y = f(x_1, x_2, x_3, x_4)$

ideal world



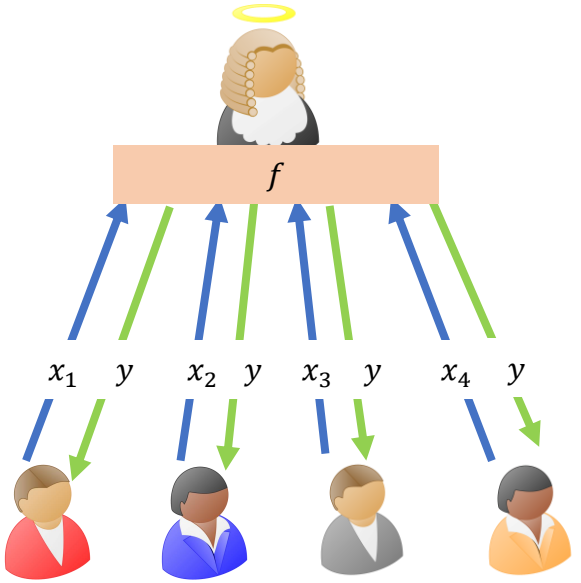
Security

real world



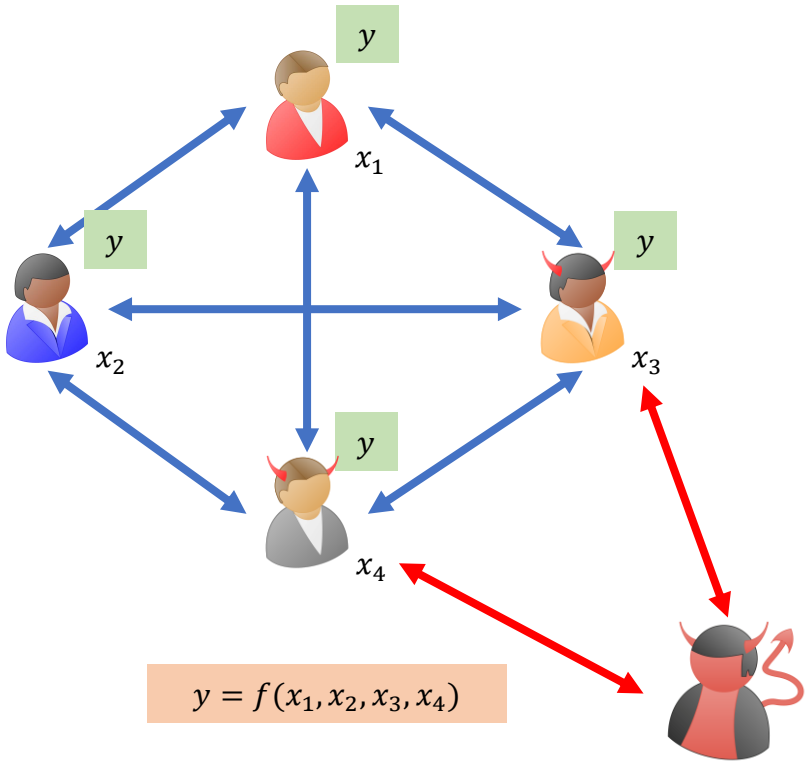
$y = f(x_1, x_2, x_3, x_4)$

ideal world

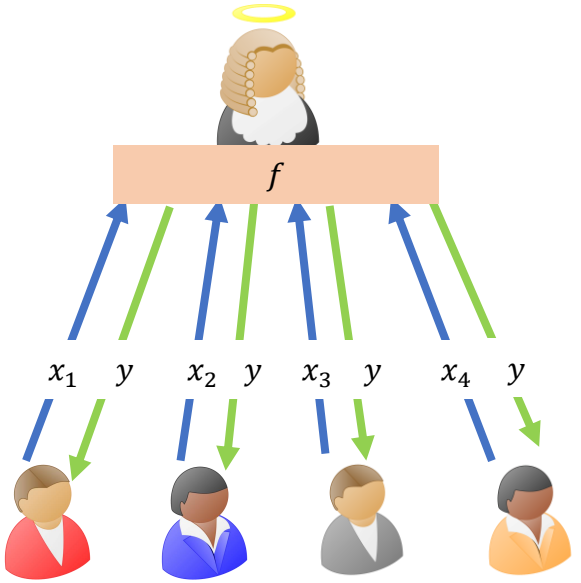


Security

real world

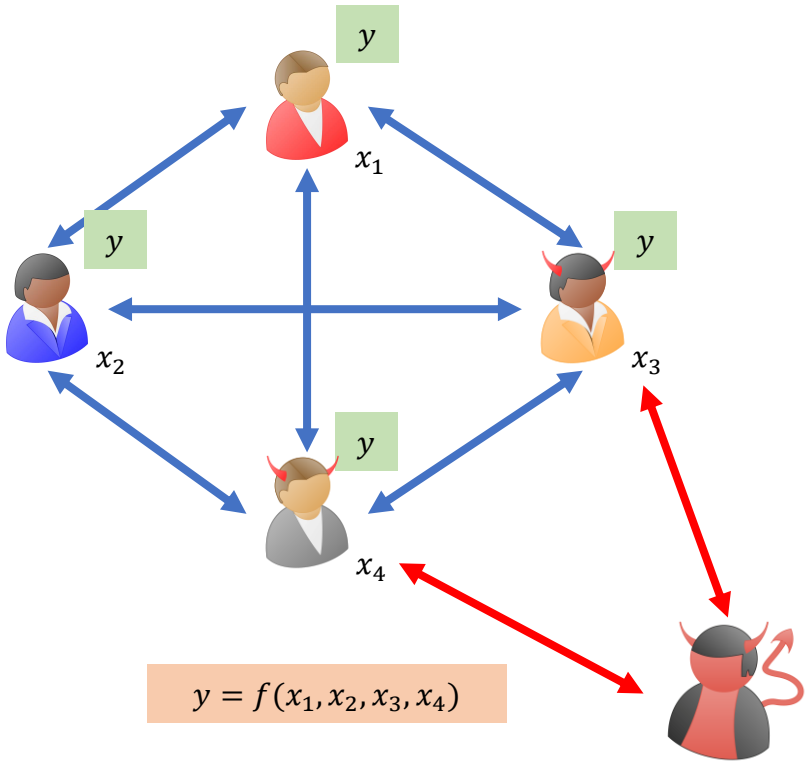


ideal world

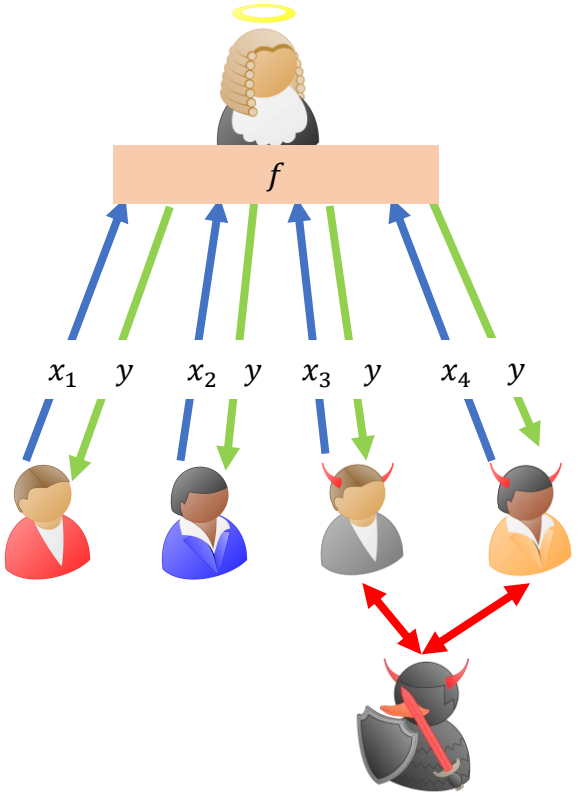


Security

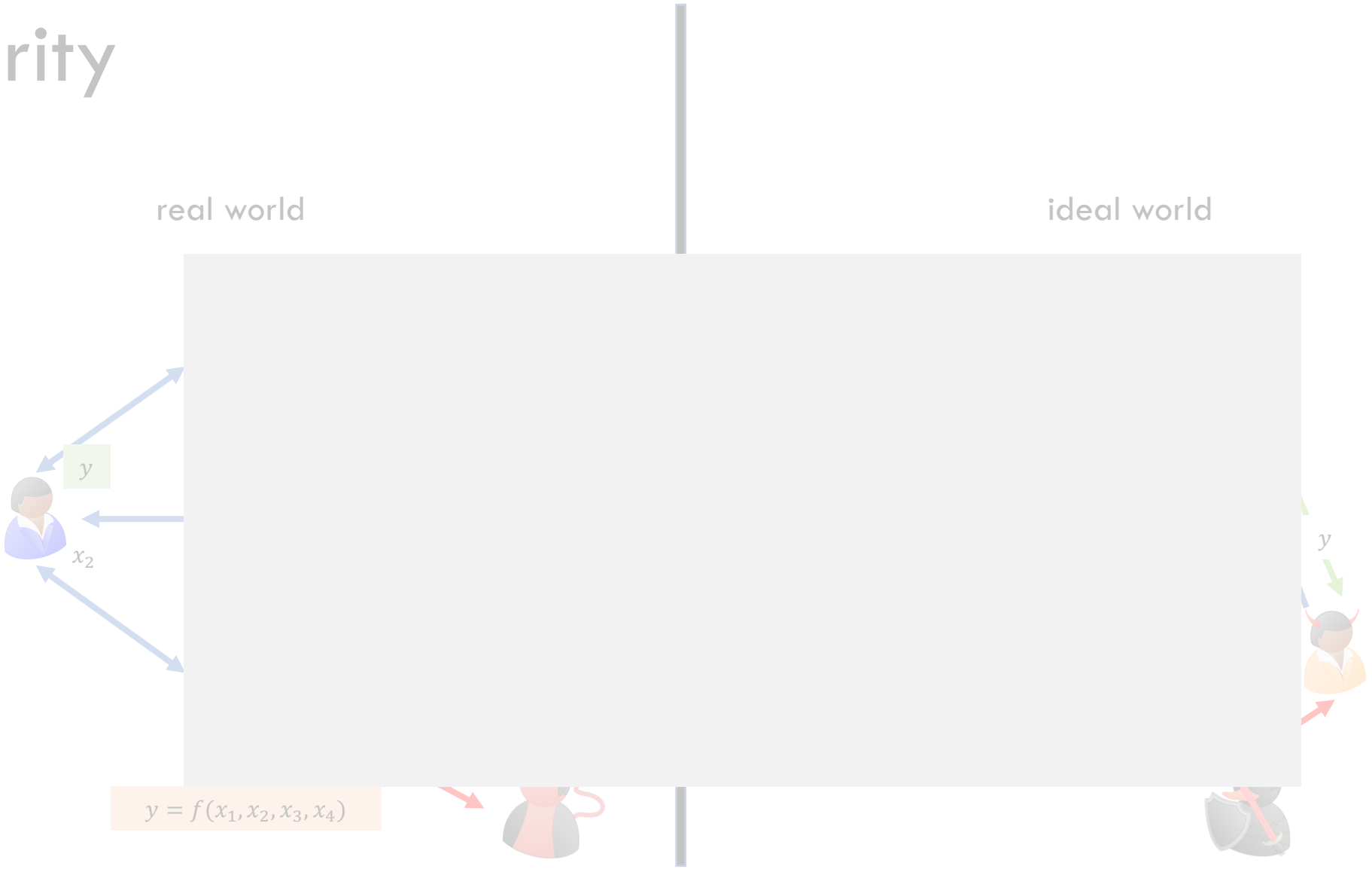
real world



ideal world



Security

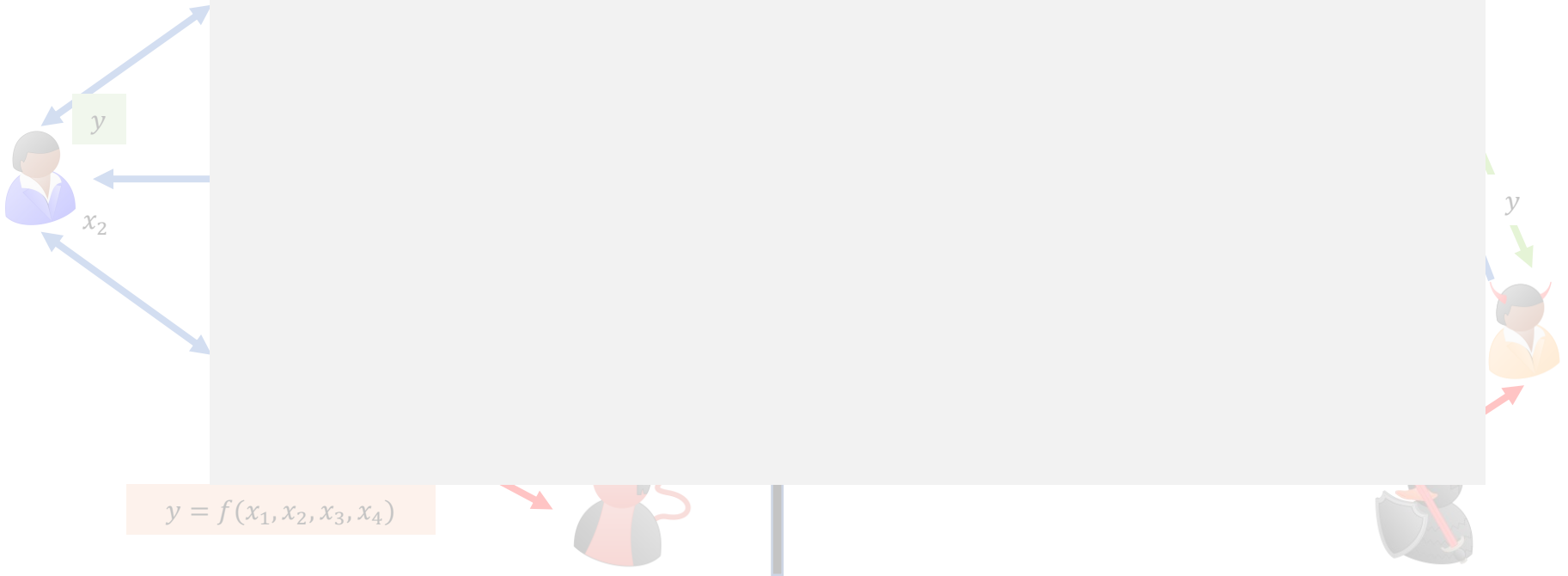


Security

real world

ideal world

Computational security.



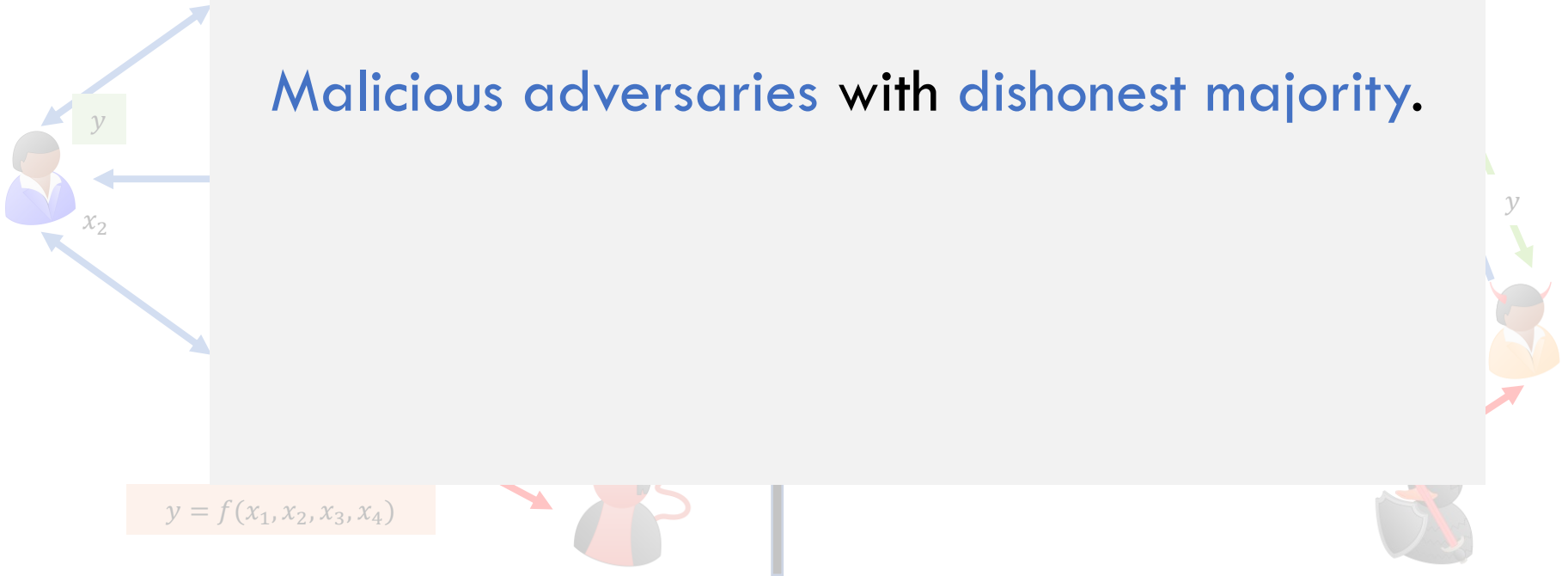
Security

real world

ideal world

Computational security.

Malicious adversaries with dishonest majority.



Security

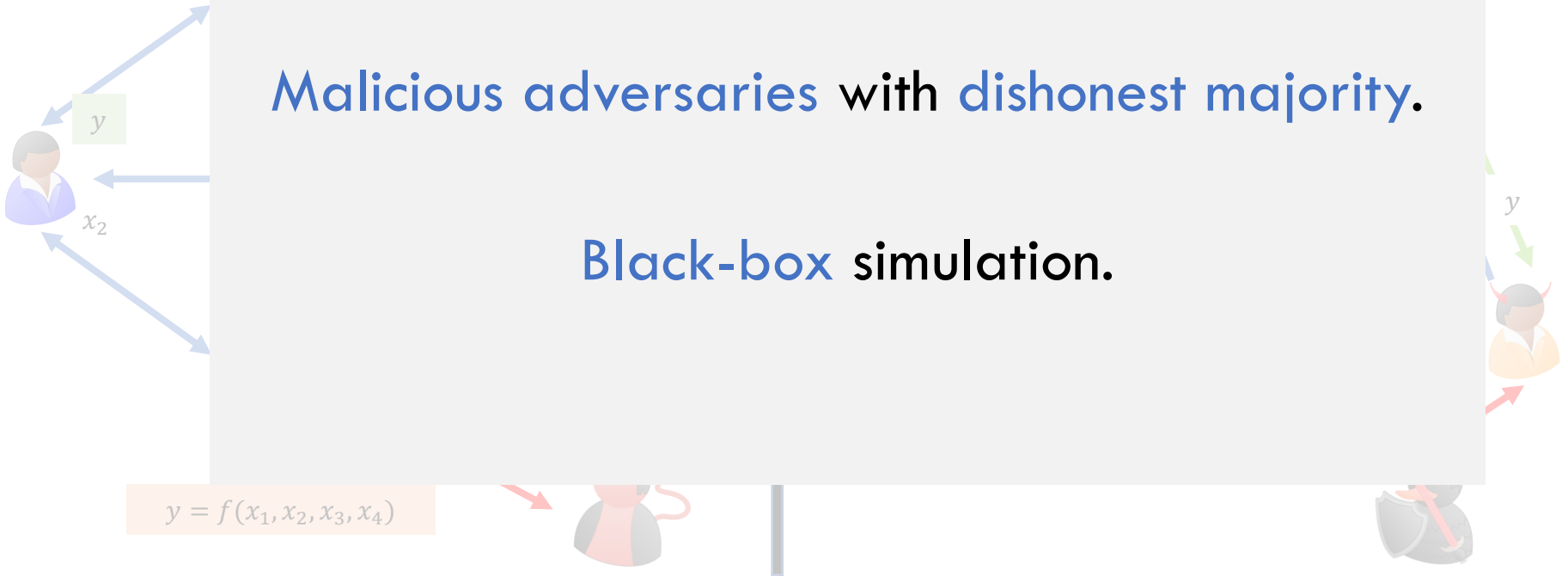
real world

ideal world

Computational security.

Malicious adversaries with dishonest majority.

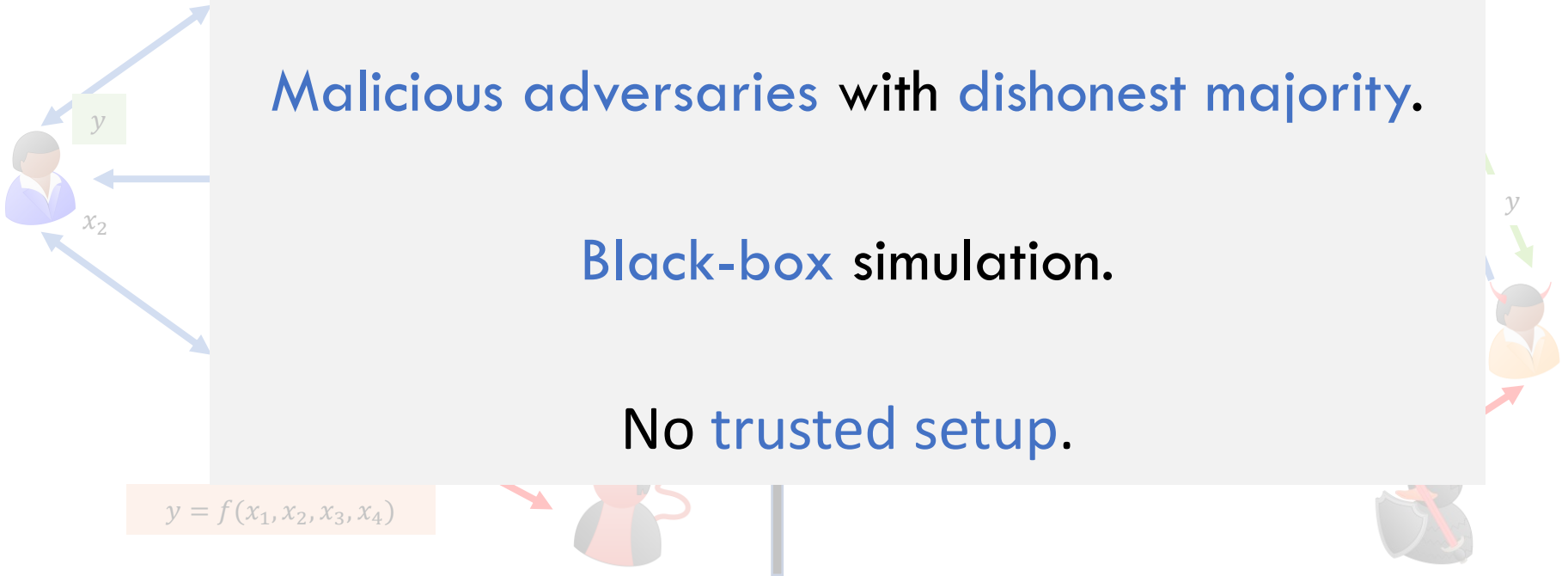
Black-box simulation.



Security

real world

ideal world



Computational security.

Malicious adversaries with dishonest majority.

Black-box simulation.

No trusted setup.

Can we construct round optimal multiparty computation from minimal assumptions?

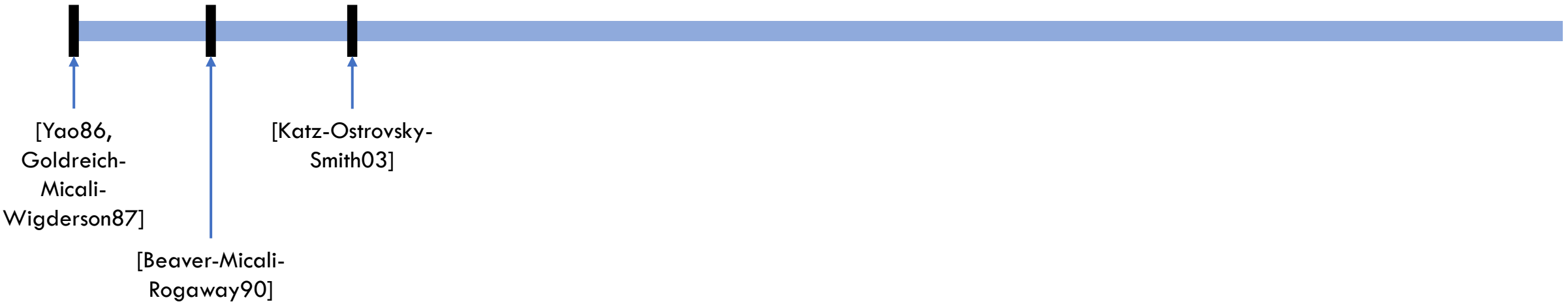
Timeline

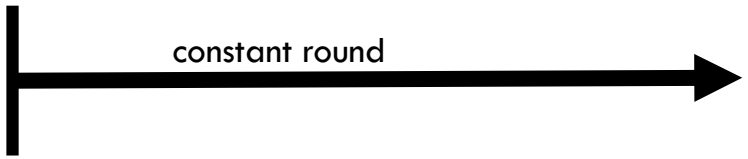
Timeline

Timeline

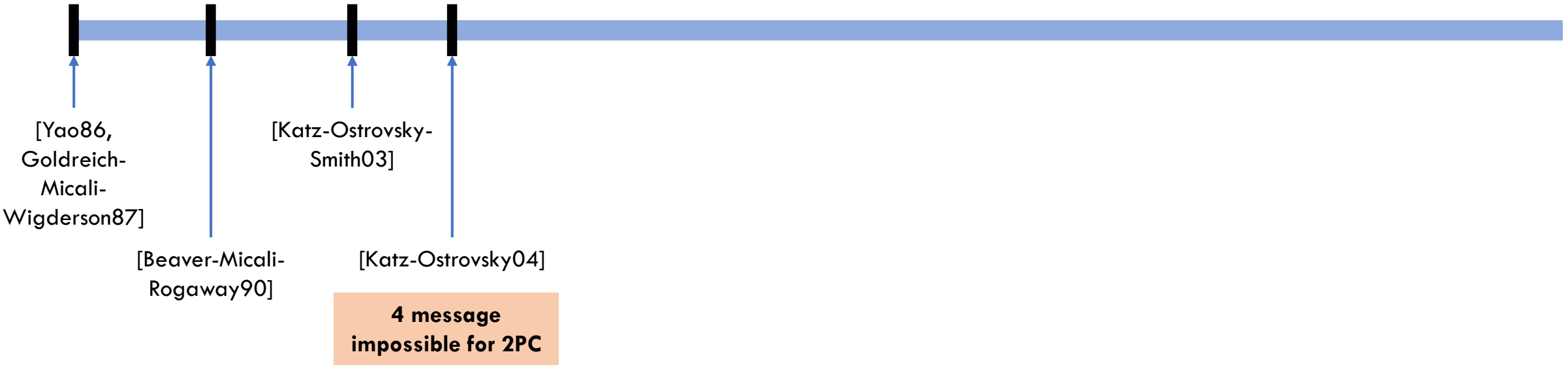

[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
constant round

Timeline

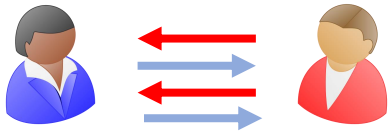

[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]


constant round

Timeline


[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]
[Katz-Ostrovsky04]
4 message impossible for 2PC
constant round

Timeline



[Yao86, Goldreich-Micali-Wigderson87]

[Beaver-Micali-Rogaway90]

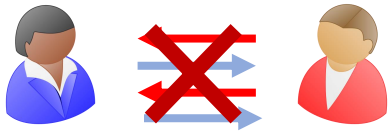
[Katz-Ostrovsky-Smith03]

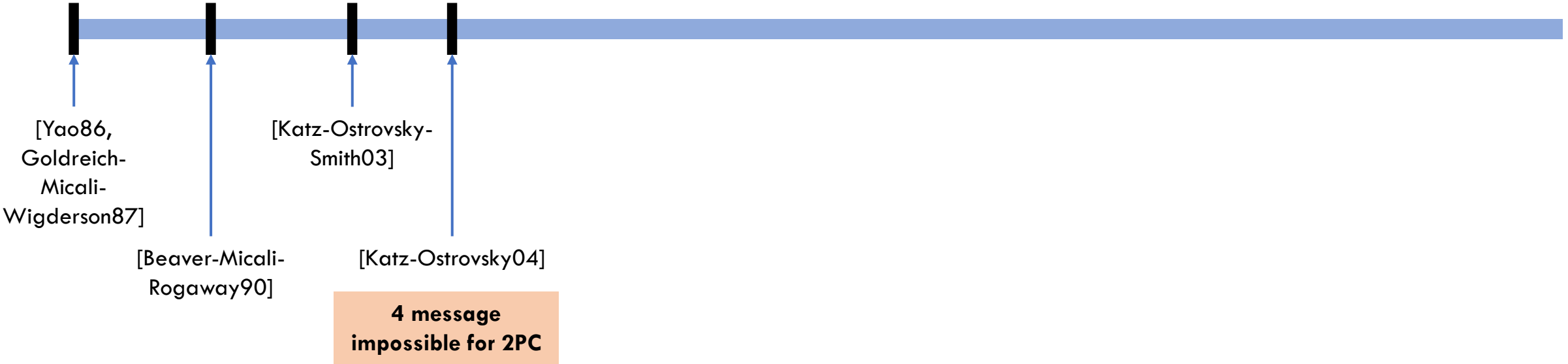
[Katz-Ostrovsky04]

4 message impossible for 2PC

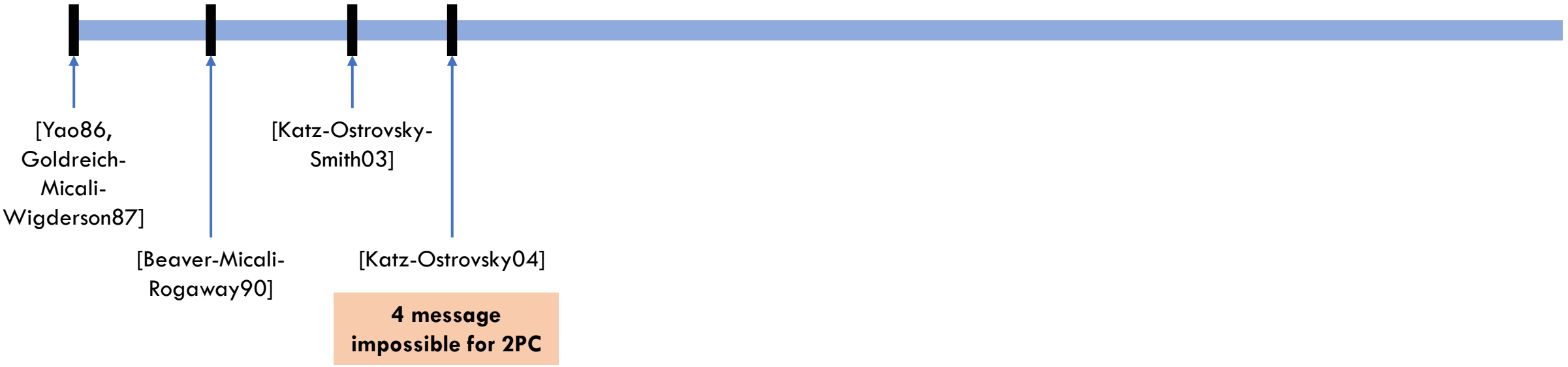
constant round

Timeline

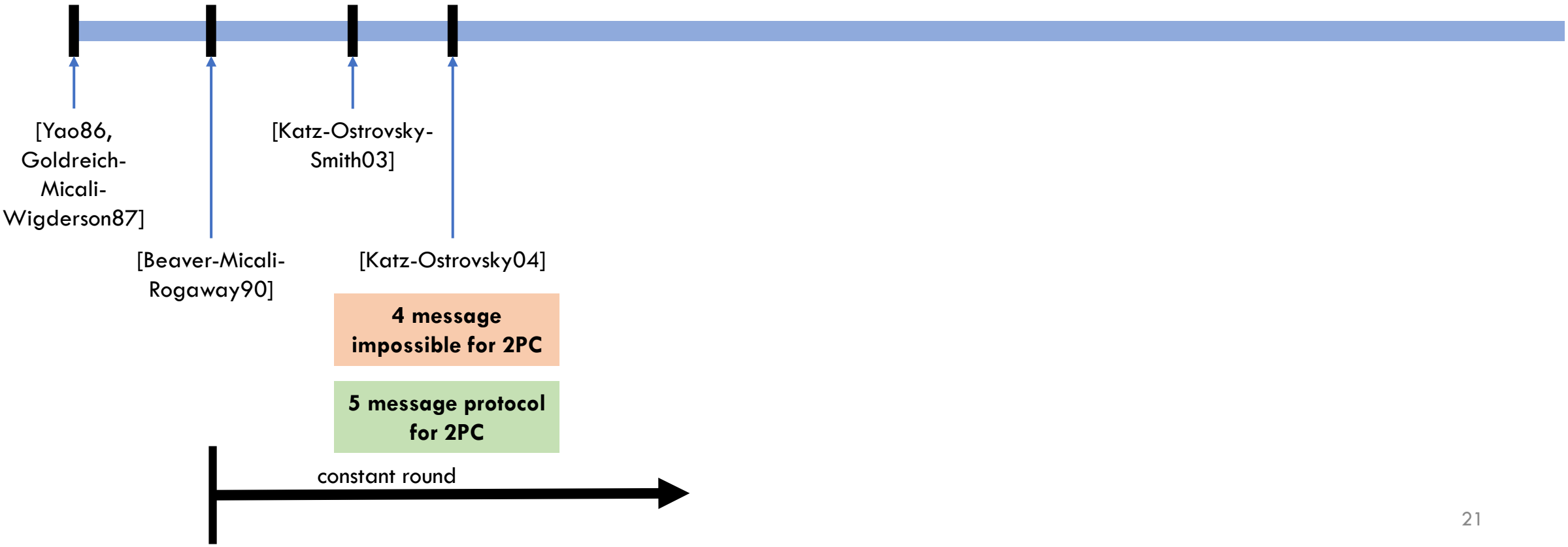



[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]
[Katz-Ostrovsky04]
4 message impossible for 2PC
constant round

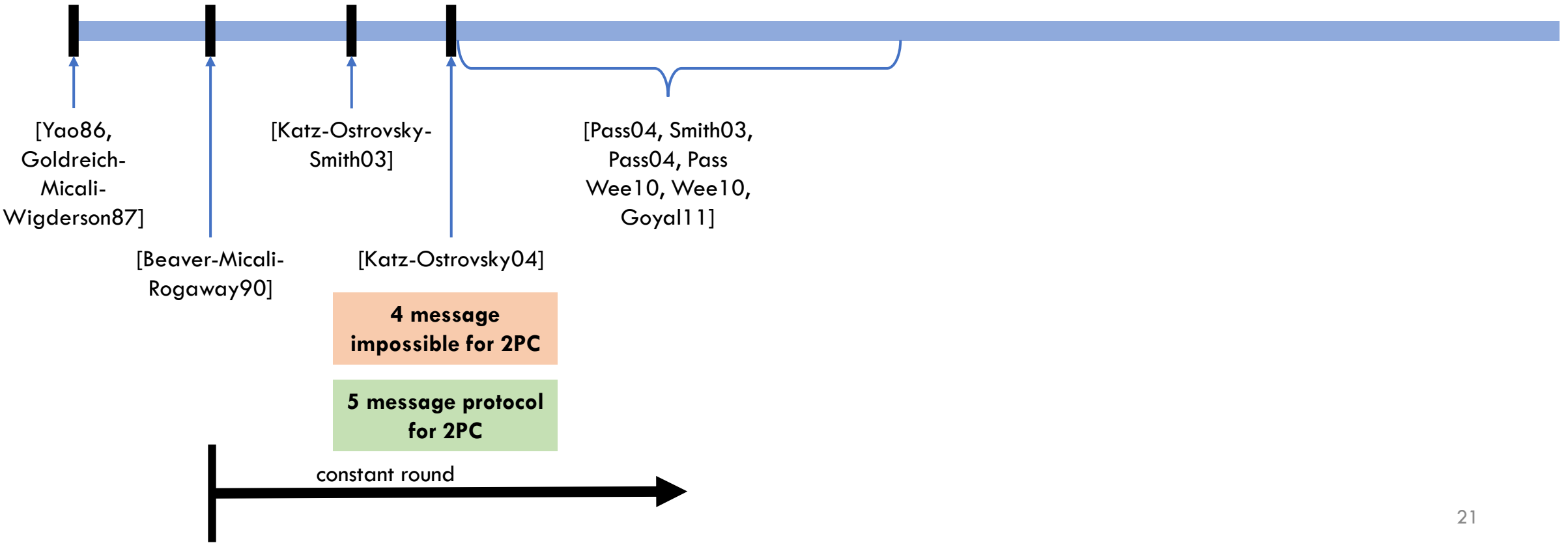
Timeline


[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]
[Katz-Ostrovsky04]
4 message impossible for 2PC
constant round

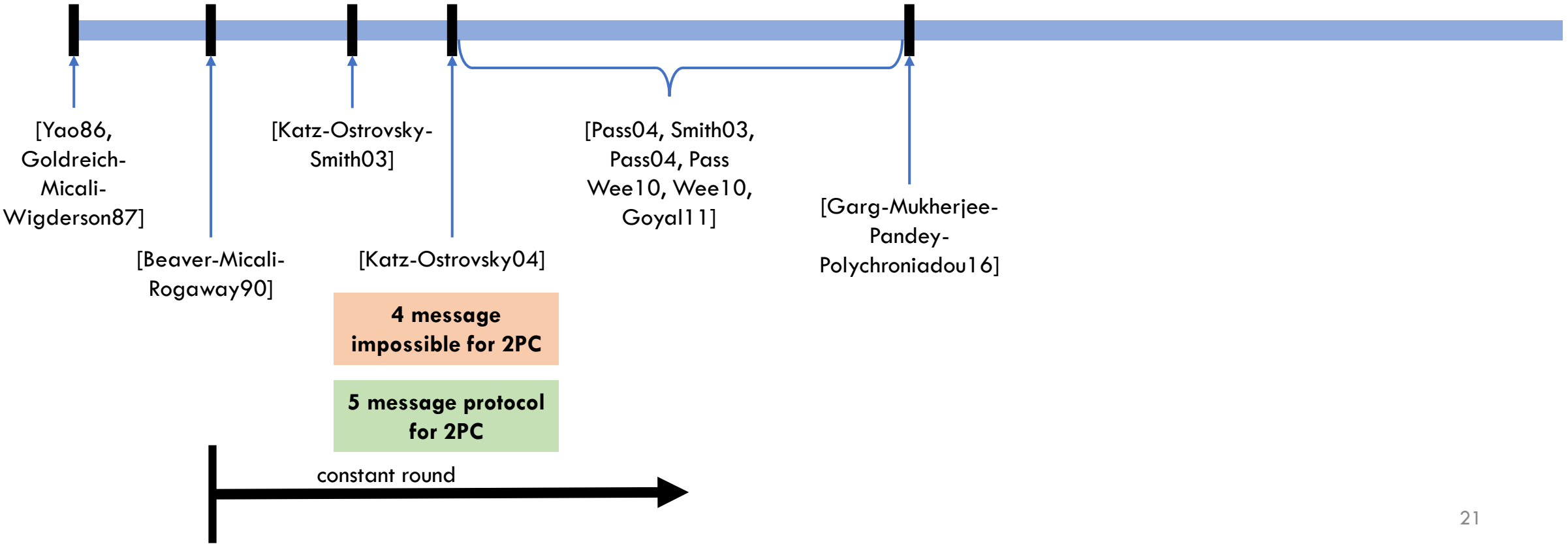
Timeline


[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]
[Katz-Ostrovsky04]
4 message impossible for 2PC
5 message protocol for 2PC
constant round

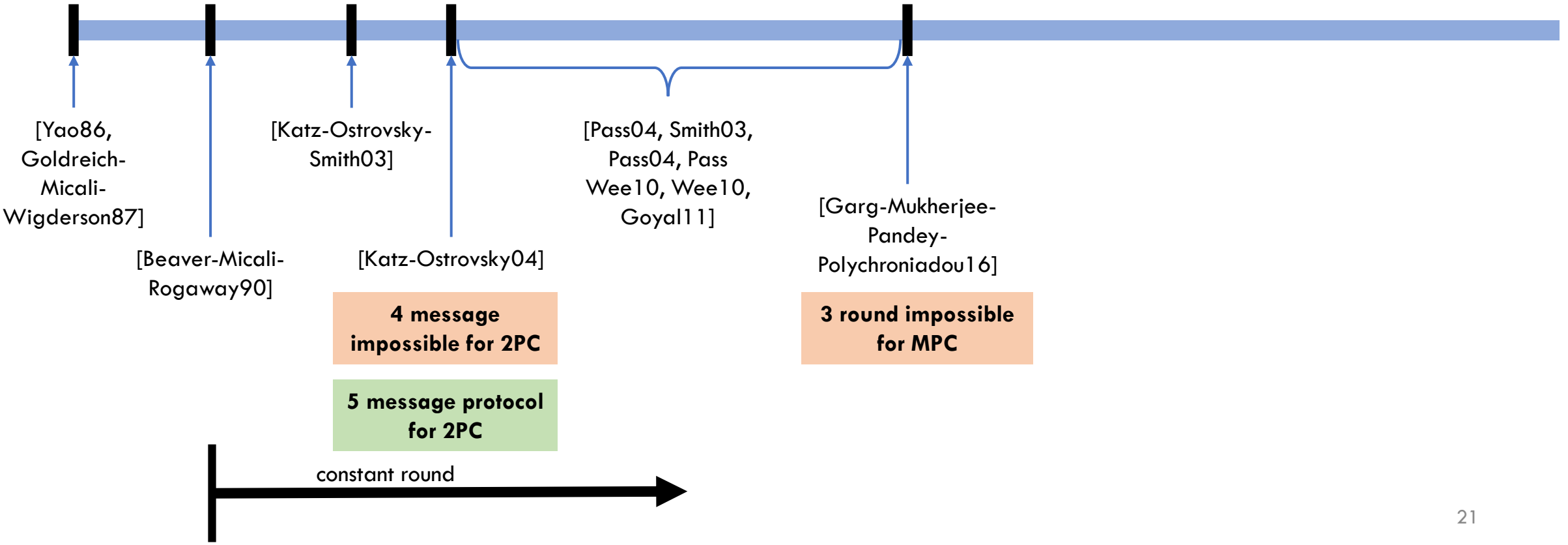
Timeline


[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]
[Katz-Ostrovsky04]
[Pass04, Smith03, Pass04, Pass Wee10, Wee10, Goyal11]
4 message impossible for 2PC
5 message protocol for 2PC
constant round

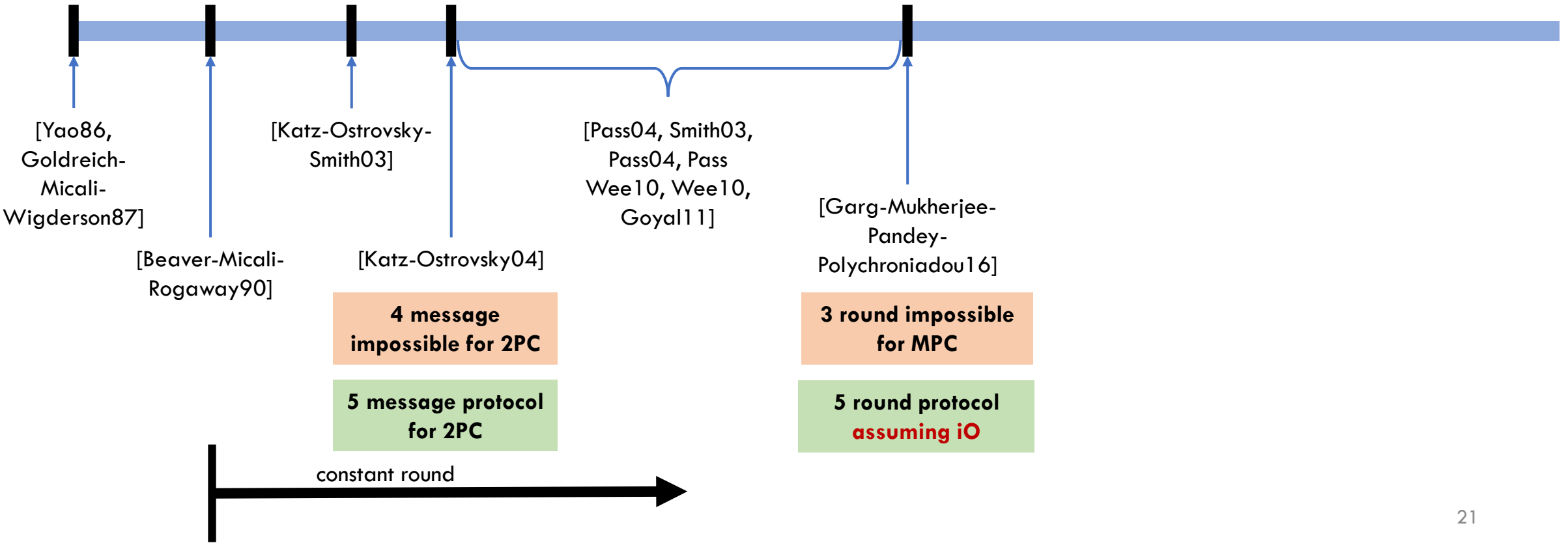
Timeline


[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]
[Katz-Ostrovsky04]
[Pass04, Smith03, Pass04, Pass Wee10, Wee10, Goyal11]
[Garg-Mukherjee-Pandey-Polychroniadou16]
4 message impossible for 2PC
5 message protocol for 2PC
constant round

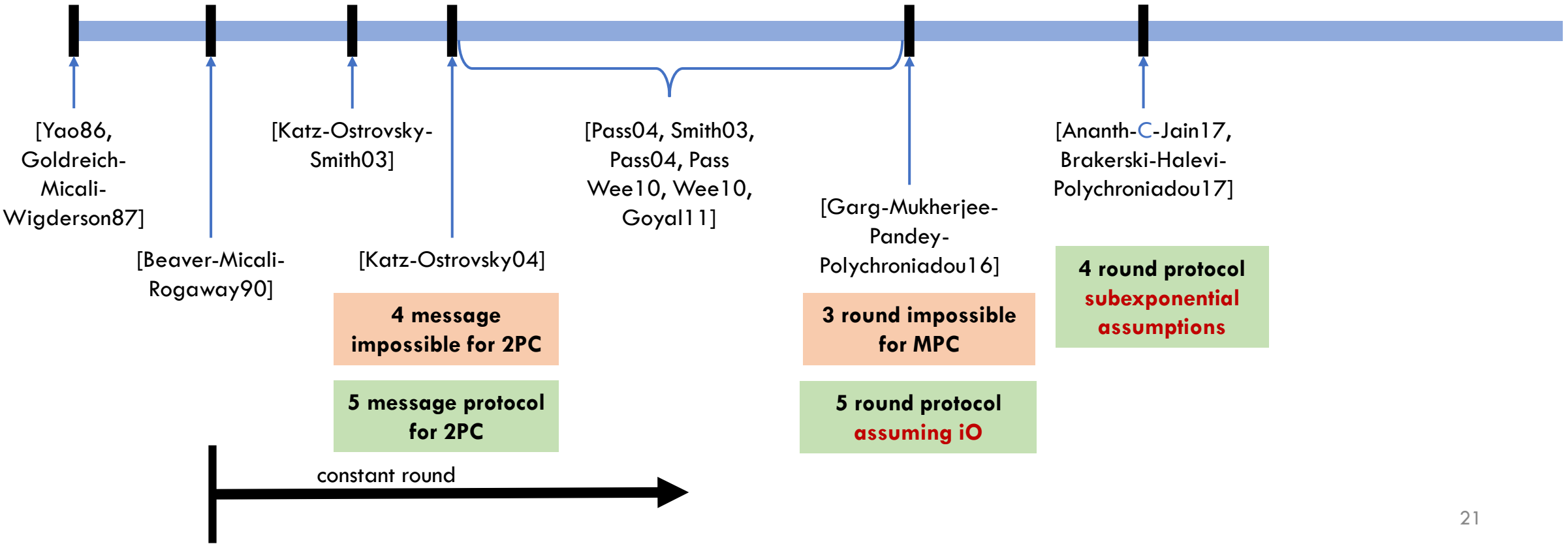
Timeline


[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]
[Katz-Ostrovsky04]
[Pass04, Smith03, Pass04, Pass Wee10, Wee10, Goyal11]
[Garg-Mukherjee-Pandey-Polychroniadou16]
4 message impossible for 2PC
3 round impossible for MPC
5 message protocol for 2PC
constant round

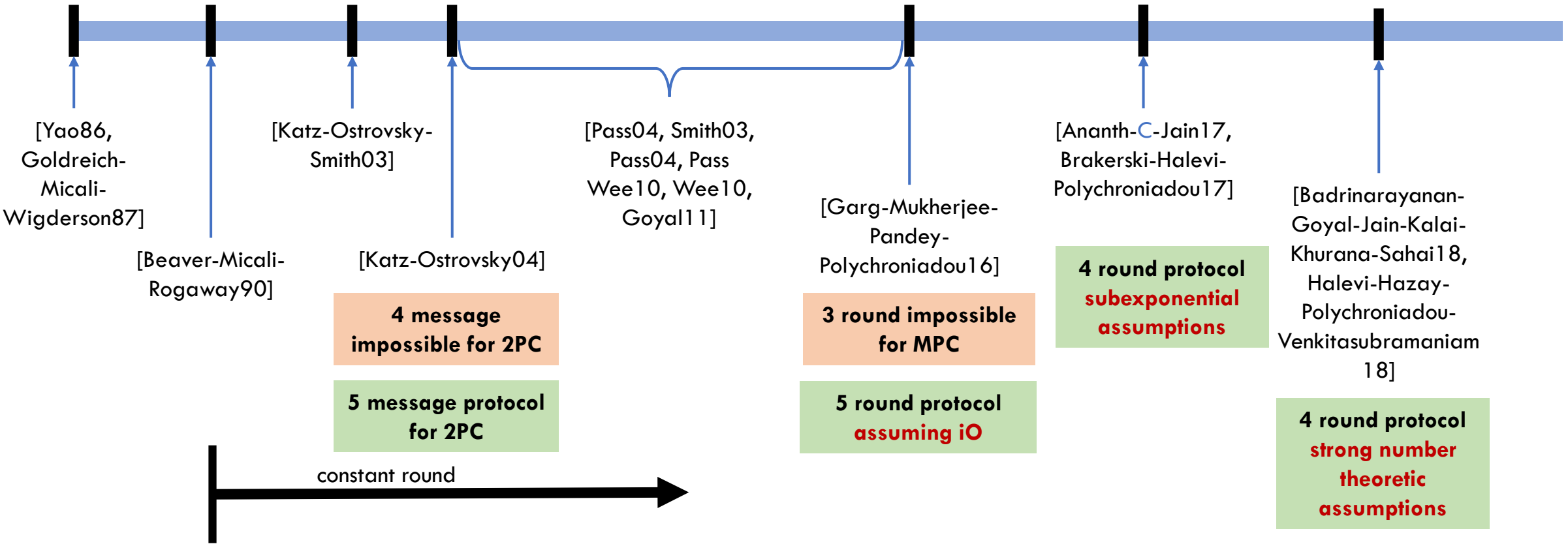
Timeline


[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]
[Katz-Ostrovsky04]
[Pass04, Smith03, Pass04, Pass Wee10, Wee10, Goyal11]
[Garg-Mukherjee-Pandey-Polychroniadou16]
4 message impossible for 2PC
5 message protocol for 2PC
3 round impossible for MPC
5 round protocol assuming iO
constant round

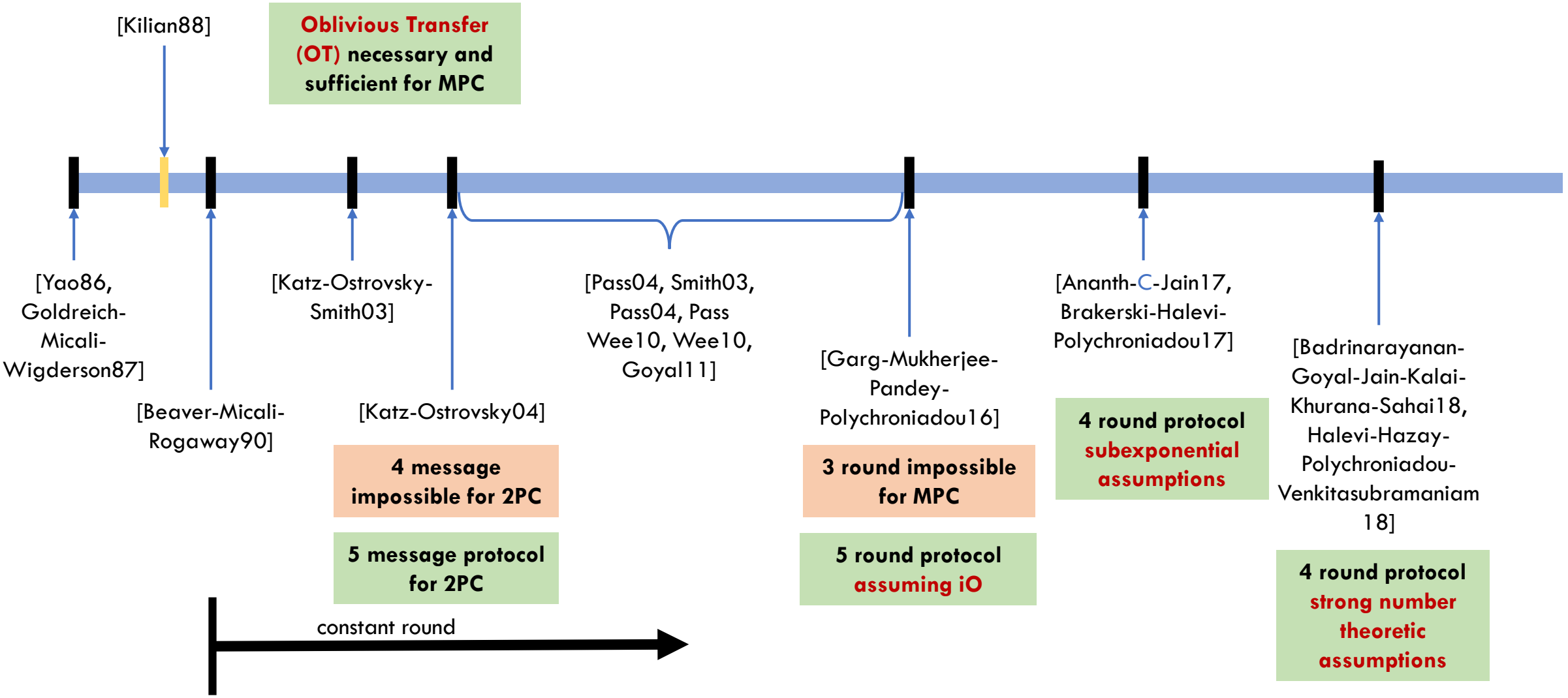
Timeline


[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]
[Katz-Ostrovsky04]
[Pass04, Smith03, Pass04, Pass Wee10, Wee10, Goyal11]
[Garg-Mukherjee-Pandey-Polychroniadou16]
[Ananth-C-Jain17, Brakerski-Halevi-Polychroniadou17]
4 message impossible for 2PC
5 message protocol for 2PC
3 round impossible for MPC
5 round protocol assuming iO
4 round protocol subexponential assumptions
constant round

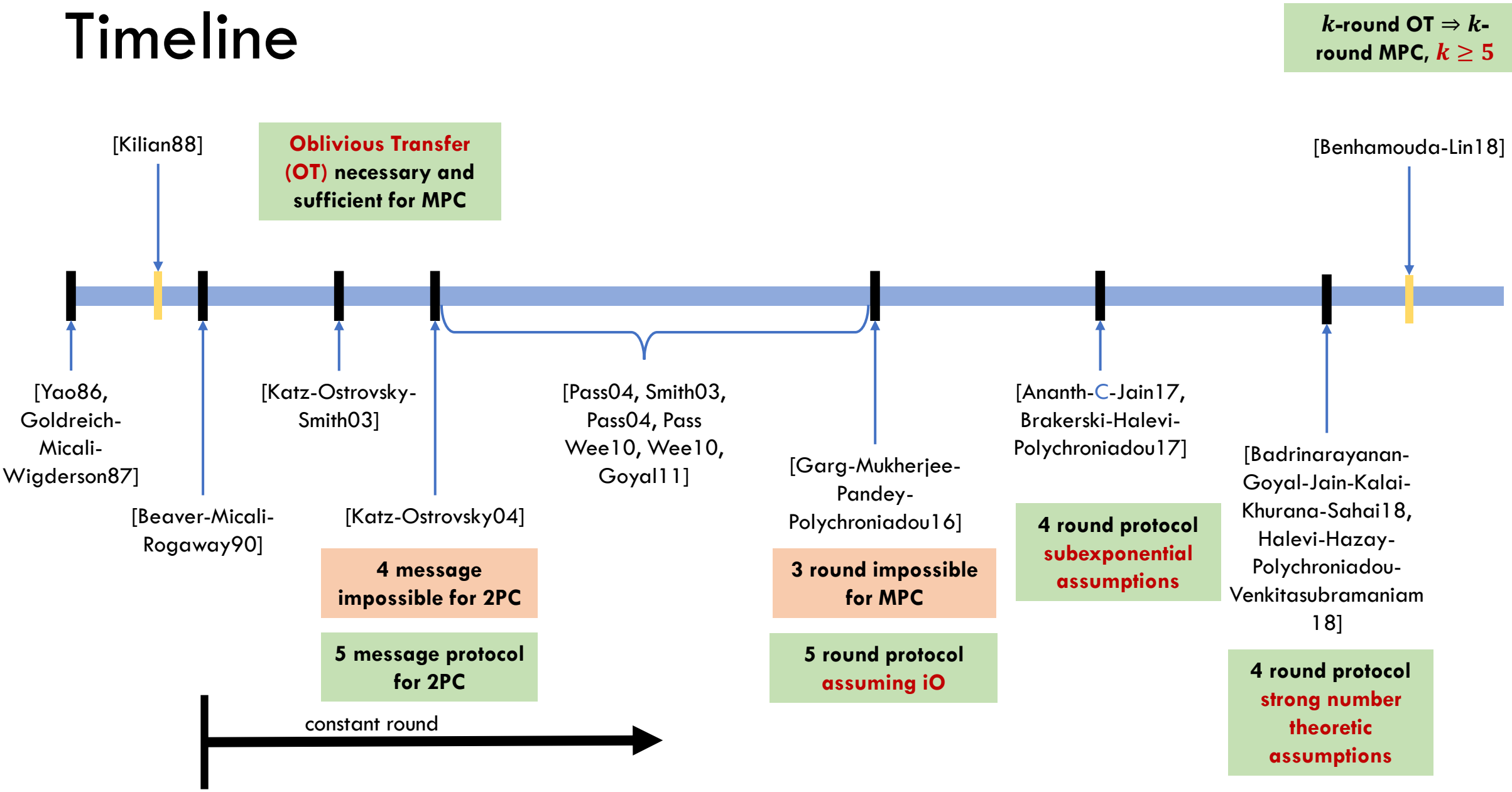
Timeline


[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]
[Katz-Ostrovsky04]
4 message impossible for 2PC
5 message protocol for 2PC
[Pass04, Smith03, Pass04, Pass Wee10, Wee10, Goyal11]
[Garg-Mukherjee-Pandey-Polychroniadou16]
3 round impossible for MPC
5 round protocol assuming iO
[Ananth-C-Jain17, Brakerski-Halevi-Polychroniadou17]
4 round protocol subexponential assumptions
[Badrinarayanan-Goyal-Jain-Kalai-Khurana-Sahai18, Halevi-Hazay-Polychroniadou-Venkitasubramaniam 18]
4 round protocol strong number theoretic assumptions
constant round

Timeline


[Kilian88]
Oblivious Transfer (OT) necessary and sufficient for MPC
[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]
[Katz-Ostrovsky04]
[Pass04, Smith03, Pass04, Pass Wee10, Wee10, Goyal11]
[Garg-Mukherjee-Pandey-Polychroniadou16]
[Ananth-C-Jain17, Brakerski-Halevi-Polychroniadou17]
[Badrinarayanan-Goyal-Jain-Kalai-Khurana-Sahai18, Halevi-Hazay-Polychroniadou-Venkitasubramaniam 18]
4 message impossible for 2PC
5 message protocol for 2PC
3 round impossible for MPC
5 round protocol assuming iO
4 round protocol subexponential assumptions
4 round protocol strong number theoretic assumptions
constant round

Timeline


k-round OT ⇒ k-round MPC, $k \geq 5$
[Kilian88]
Oblivious Transfer (OT) necessary and sufficient for MPC
[Benhamouda-Lin18]
[Yao86, Goldreich-Micali-Wigderson87]
[Beaver-Micali-Rogaway90]
[Katz-Ostrovsky-Smith03]
[Katz-Ostrovsky04]
[Pass04, Smith03, Pass04, Pass Wee10, Wee10, Goyal11]
[Garg-Mukherjee-Pandey-Polychroniadou16]
[Ananth-C-Jain17, Brakerski-Halevi-Polychroniadou17]
[Badrinarayanan-Goyal-Jain-Kalai-Khurana-Sahai18, Halevi-Hazay-Polychroniadou-Venkitasubramaniam 18]
4 message impossible for 2PC
5 message protocol for 2PC
3 round impossible for MPC
5 round protocol assuming iO
4 round protocol subexponential assumptions
4 round protocol strong number theoretic assumptions
constant round

Our results

Assuming 4 round oblivious transfer (OT), there exists a 4 round MPC protocol.

Our results

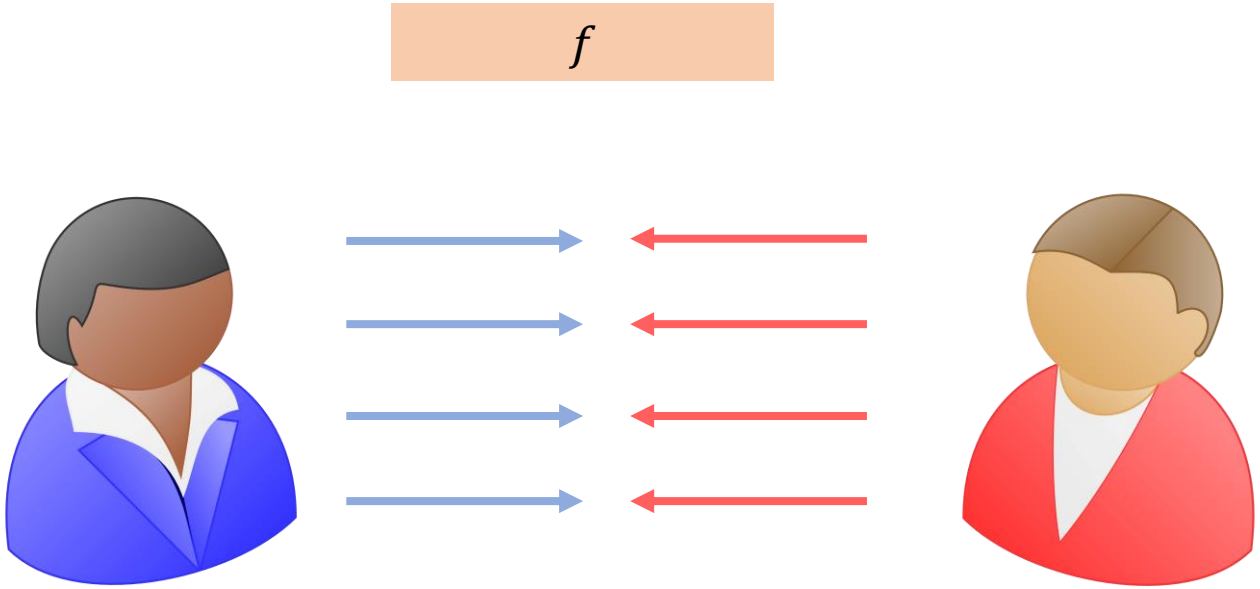
Assuming 4 round oblivious transfer (OT), there exists a 4 round MPC protocol.

OT: Indistinguishability security against malicious sender, and extraction of receiver bit.

OT protocols satisfying such properties are indeed known.

Protecting the 4^{th} round message

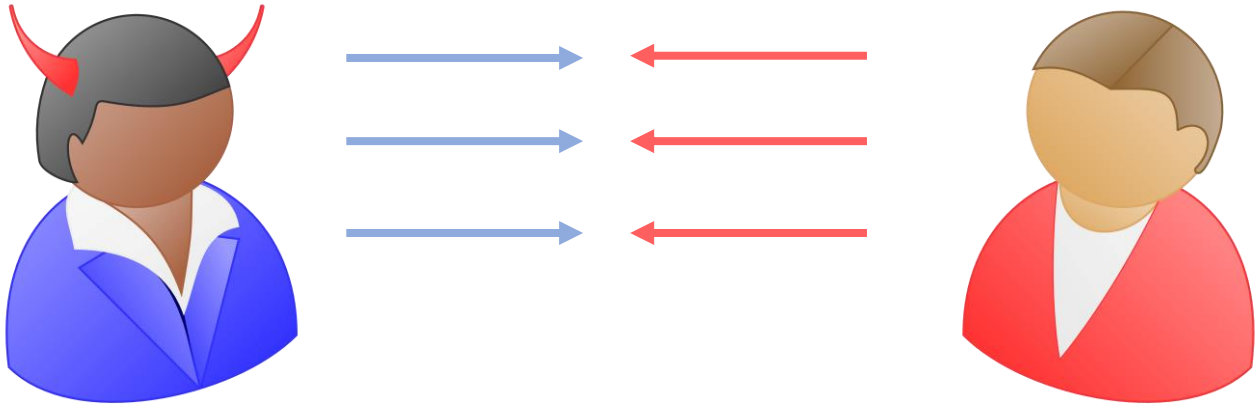
Challenge: Enforcing Honest Behavior



Any 4 round protocol computing a function f.

Challenge: Enforcing Honest Behavior

f



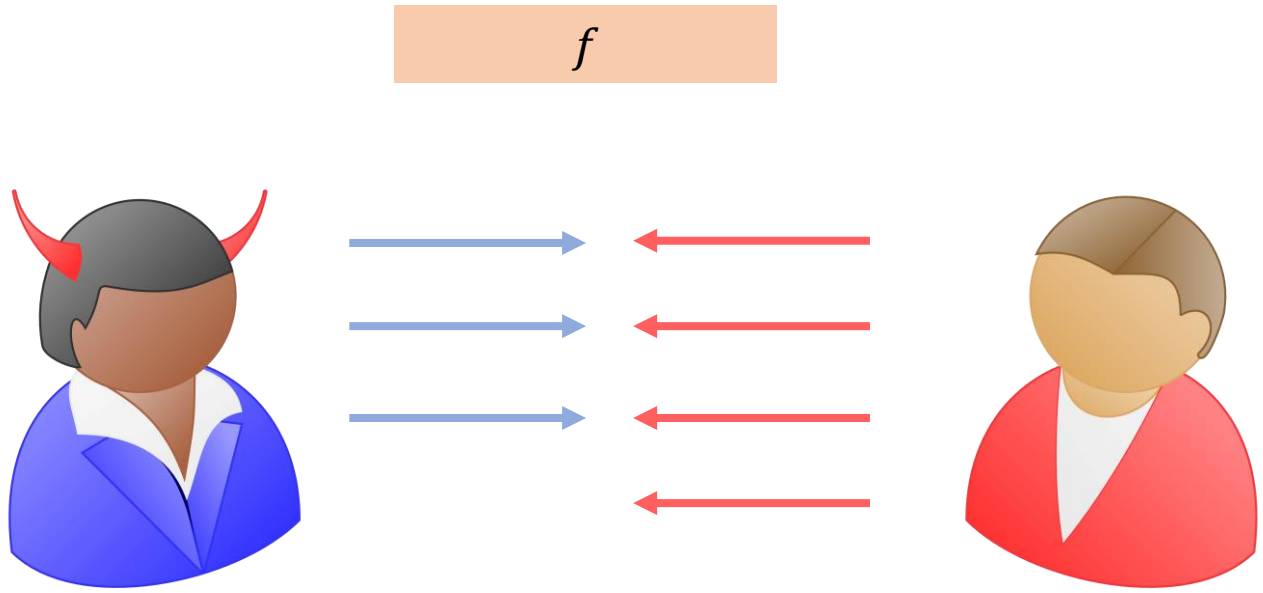
Rushing adversary

May decide not to send its message after it sees Bob's message.

Challenge: Enforcing Honest Behavior

Rushing adversary

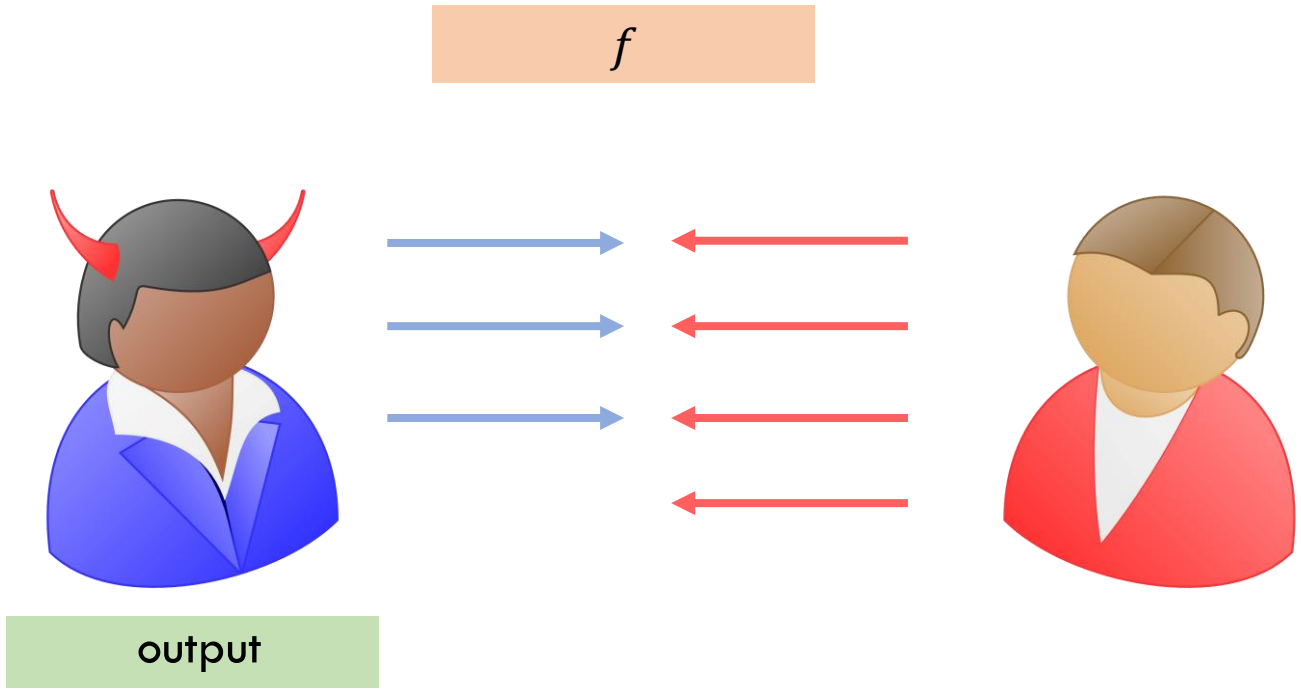
May decide not to send its message after it sees Bob's message.



Challenge: Enforcing Honest Behavior

Rushing adversary

May decide not to send its message after it sees Bob's message.



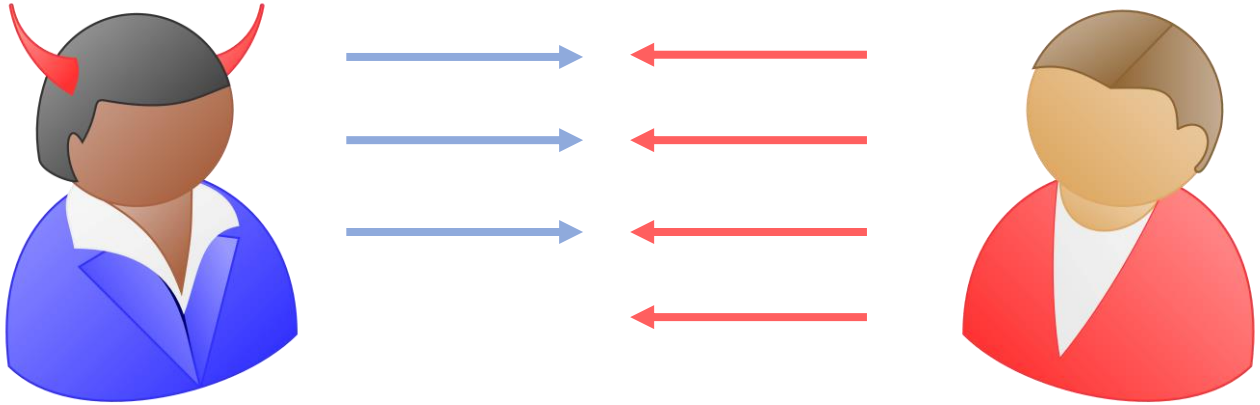
Only Alice learns the output.

Challenge: Enforcing Honest Behavior

identity

Rushing adversary

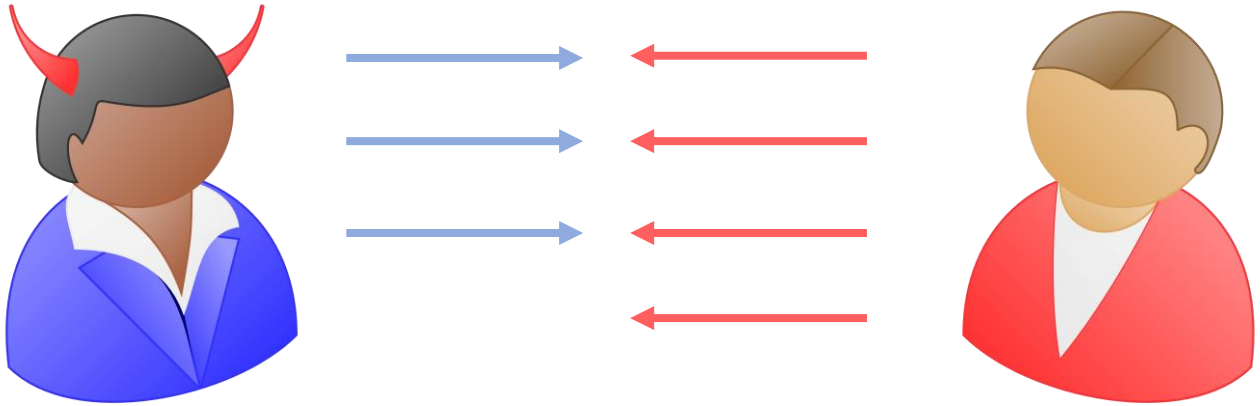
May decide not to send its message after it sees Bob's message.



output

Challenge: Enforcing Honest Behavior

identity



Bob's input

Rushing adversary

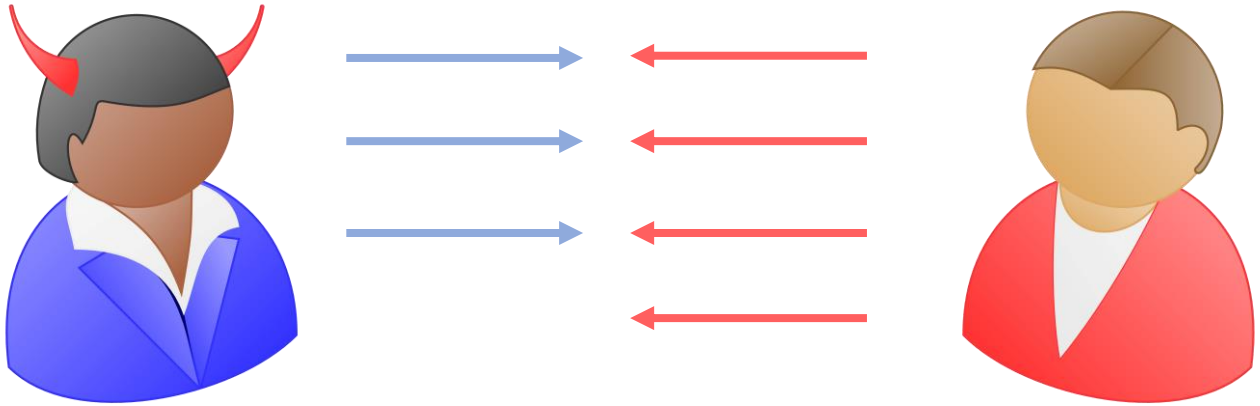
May decide not to send its message after it sees Bob's message.

Challenge: Enforcing Honest Behavior

identity

Rushing adversary

May decide not to send its message after it sees Bob's message.

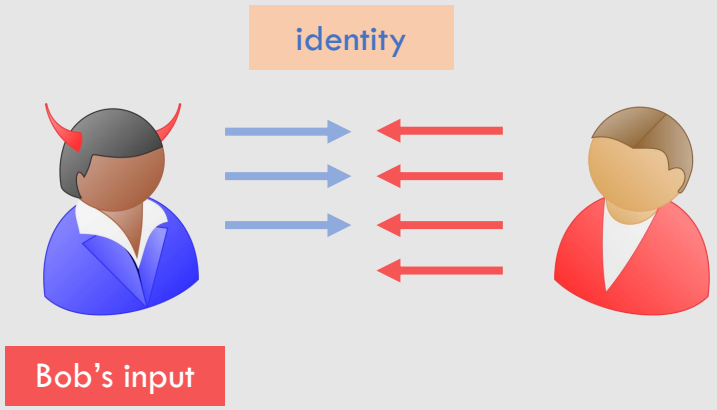


Bob's input

Don't send fourth round message unless Alice proves honest behavior.

Challenge: Enforcing Honest Behavior

Don't send fourth round message unless Alice proves honest behavior.

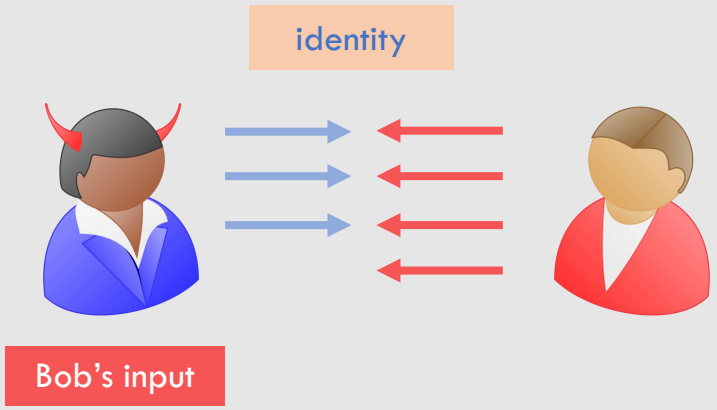


Typical approach:

Alice convinces Bob of honest behavior via zero-knowledge proof before Bob sends his fourth round message.

Challenge: Enforcing Honest Behavior

Don't send fourth round message unless Alice proves honest behavior.



Typical approach:

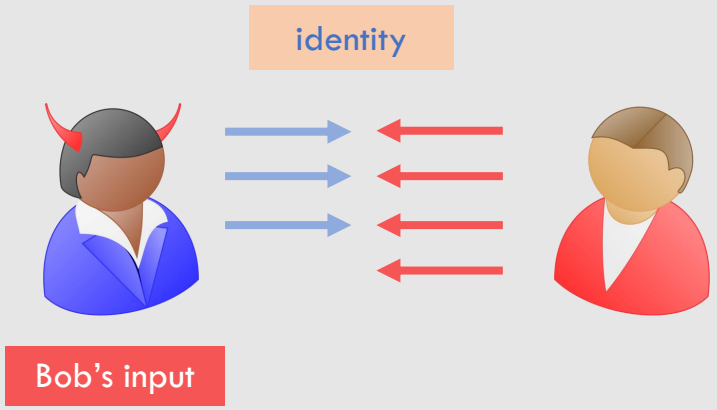
Alice convinces Bob of honest behavior via zero-knowledge proof before Bob sends his fourth round message.

Requires 3 round zero-knowledge proofs

[Goldreich-Krawczyk'96]: Impossible with Black-box simulation.

Challenge: Enforcing Honest Behavior

Don't send fourth round message unless Alice proves honest behavior.



Typical approach:

Alice convinces Bob of honest behavior via zero-knowledge proof before Bob sends his fourth round message.

Requires 3 round zero-knowledge proofs

[Goldreich-Krawczyk'96]: Impossible with Black-box simulation.

Many other challenges, but for this talk, we focus on solving this challenge.

Interactive Multiparty Conditional Disclosure of Secret (MCDS)

Conditional Disclosure of Secrets (CDS)

Conditional Disclosure of Secrets (CDS)

message

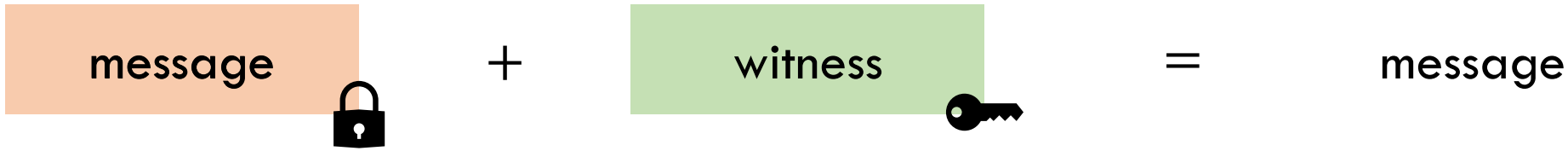
Conditional Disclosure of Secrets (CDS)

Conditional Disclosure of Secrets (CDS)

Conditional Disclosure of Secrets (CDS)

If witness satisfies specified condition.

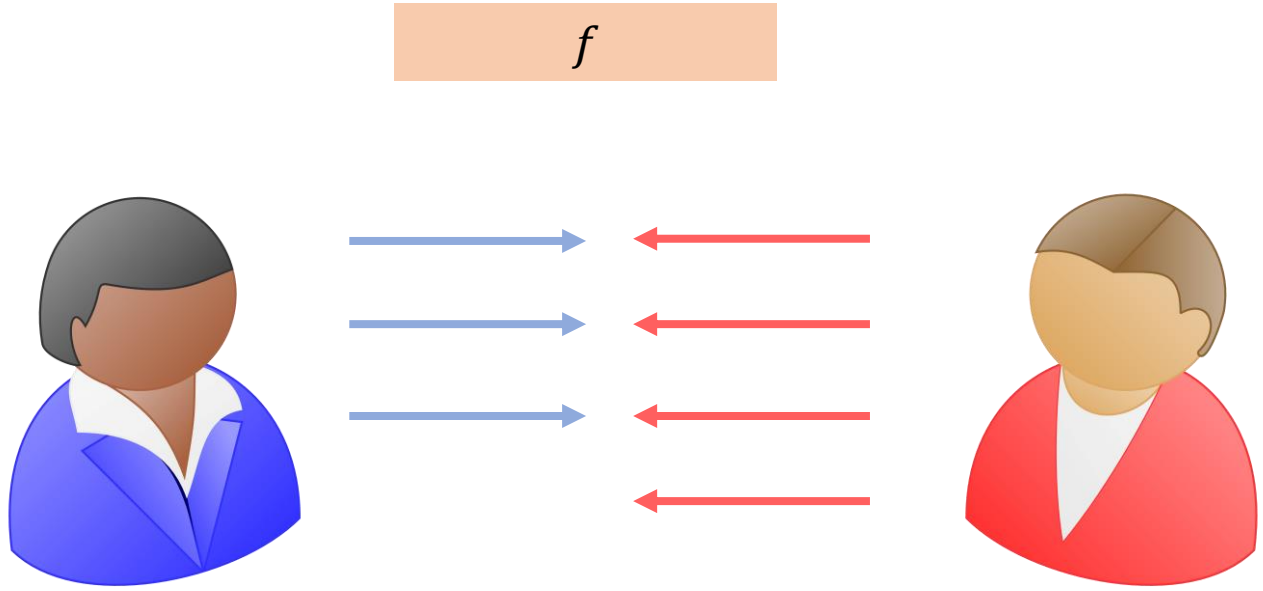
Conditional Disclosure of Secrets (CDS)



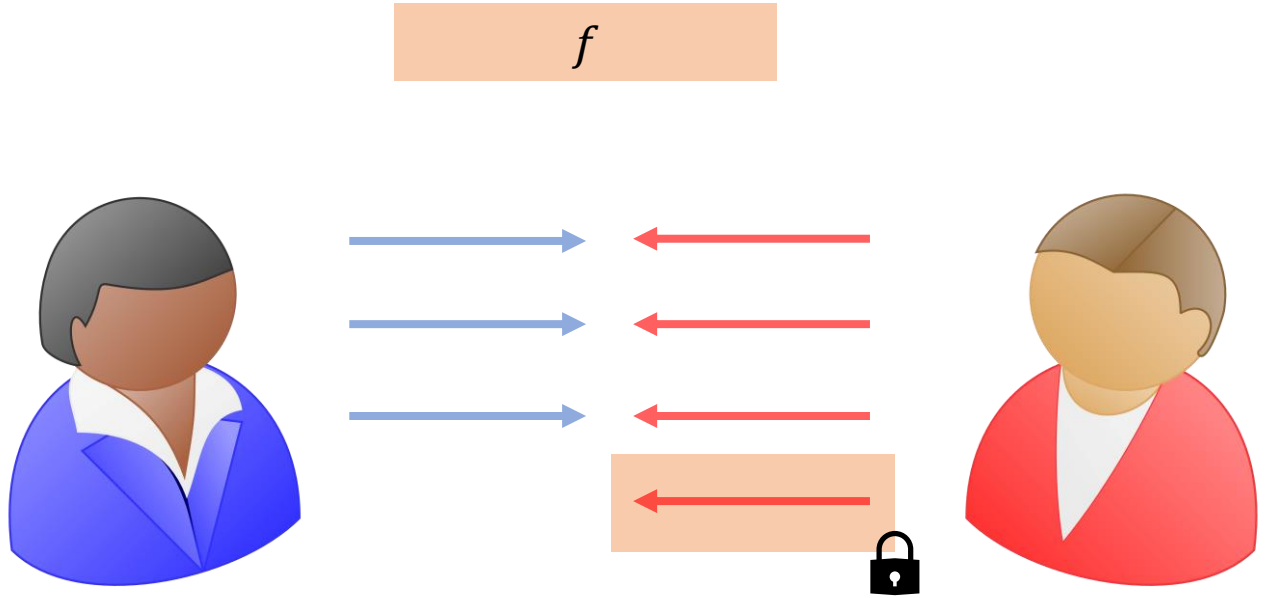
If witness satisfies specified condition.

[Gertner-Ishai-Kushilevitz-Malkin98, Aiello-Ishai-Reingold01]

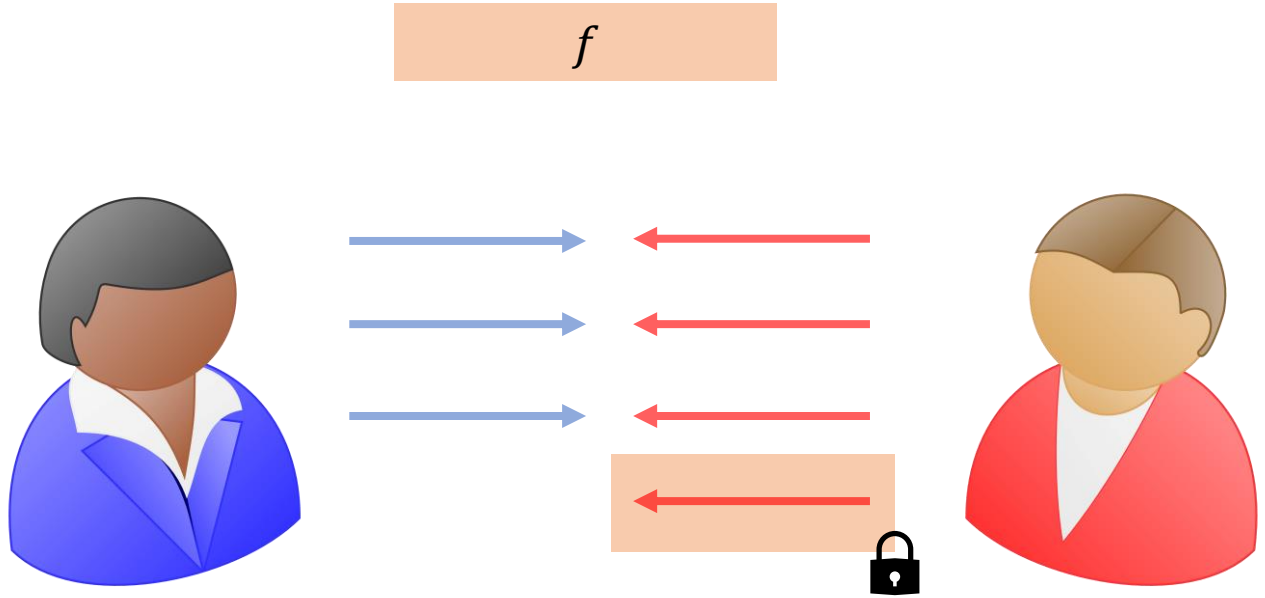
CDS as safety net



CDS as safety net

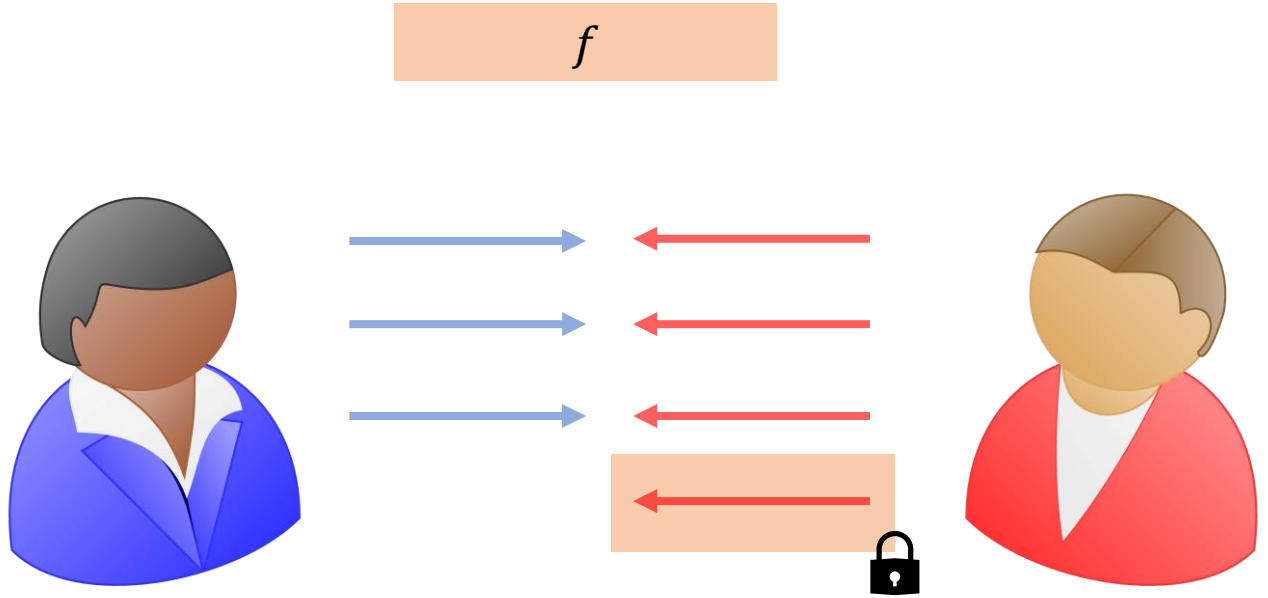


CDS as safety net



"I behaved honestly"

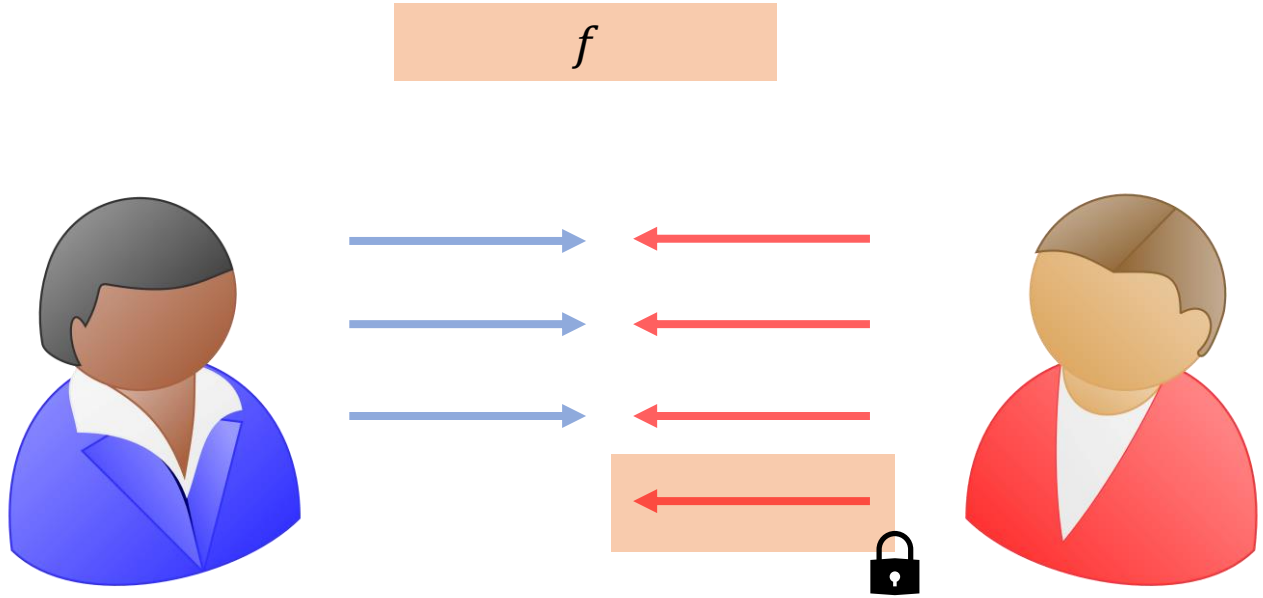
CDS as safety net



"I behaved honestly"

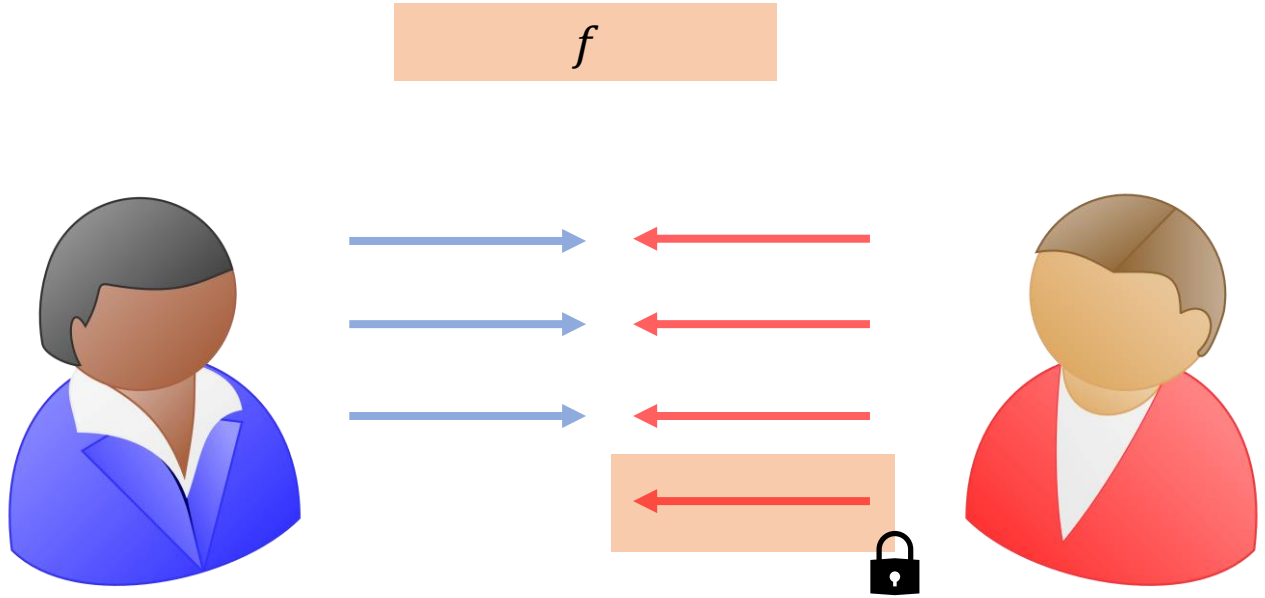
How do we prove honest behavior?

CDS as safety net



input and randomness

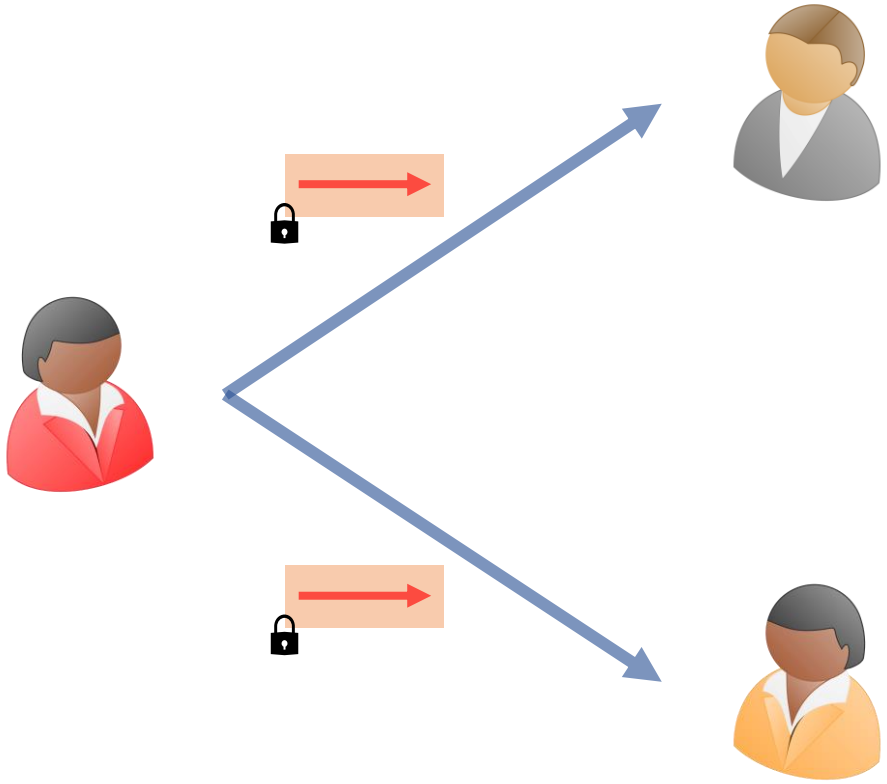
CDS as safety net



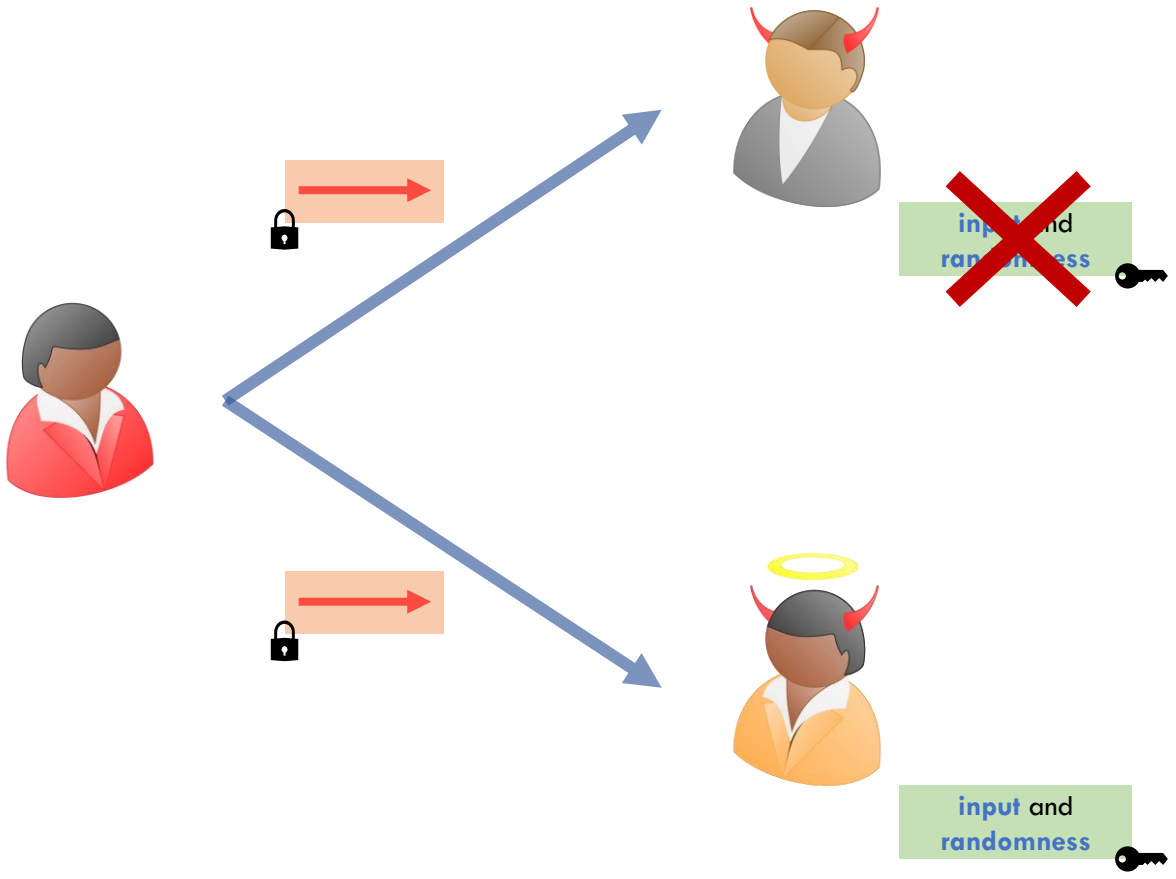
input and randomness

Does this work with more than 2 parties?

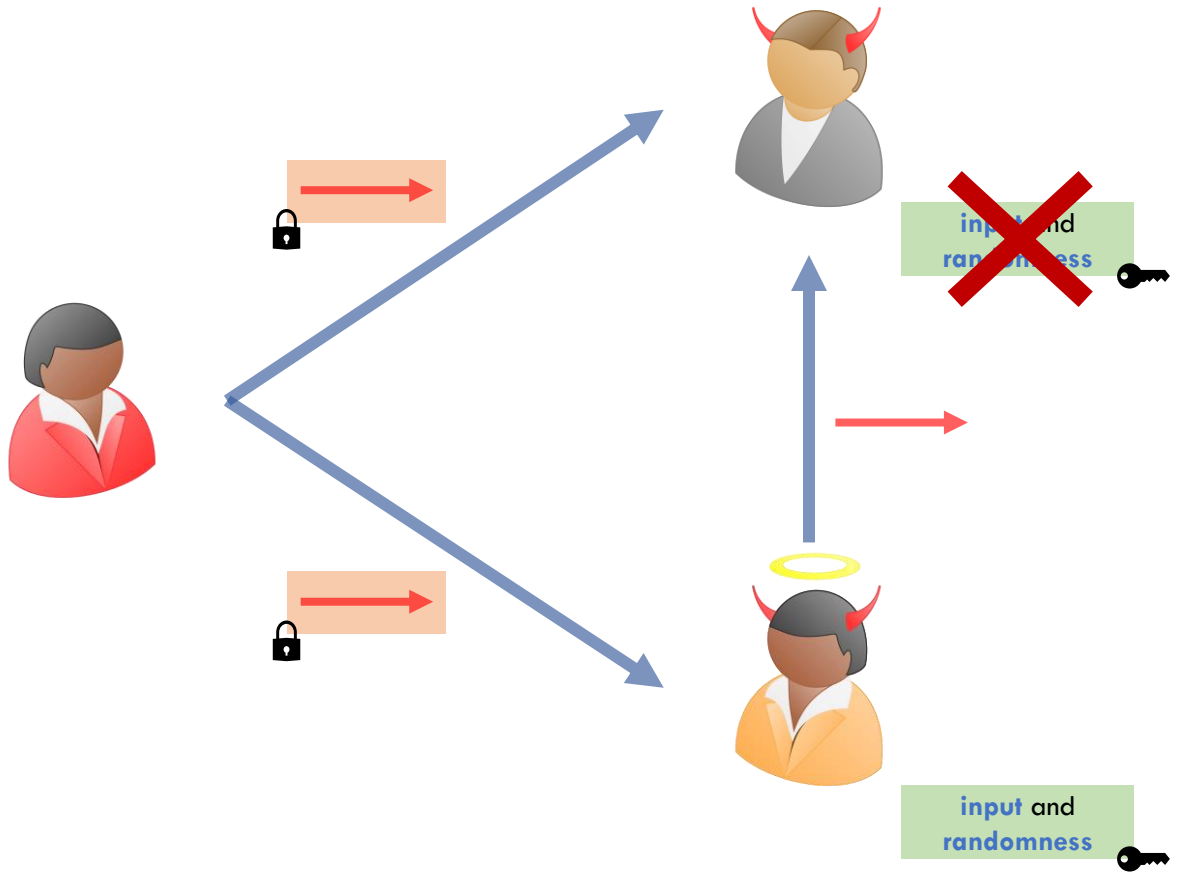
CDS as safety net



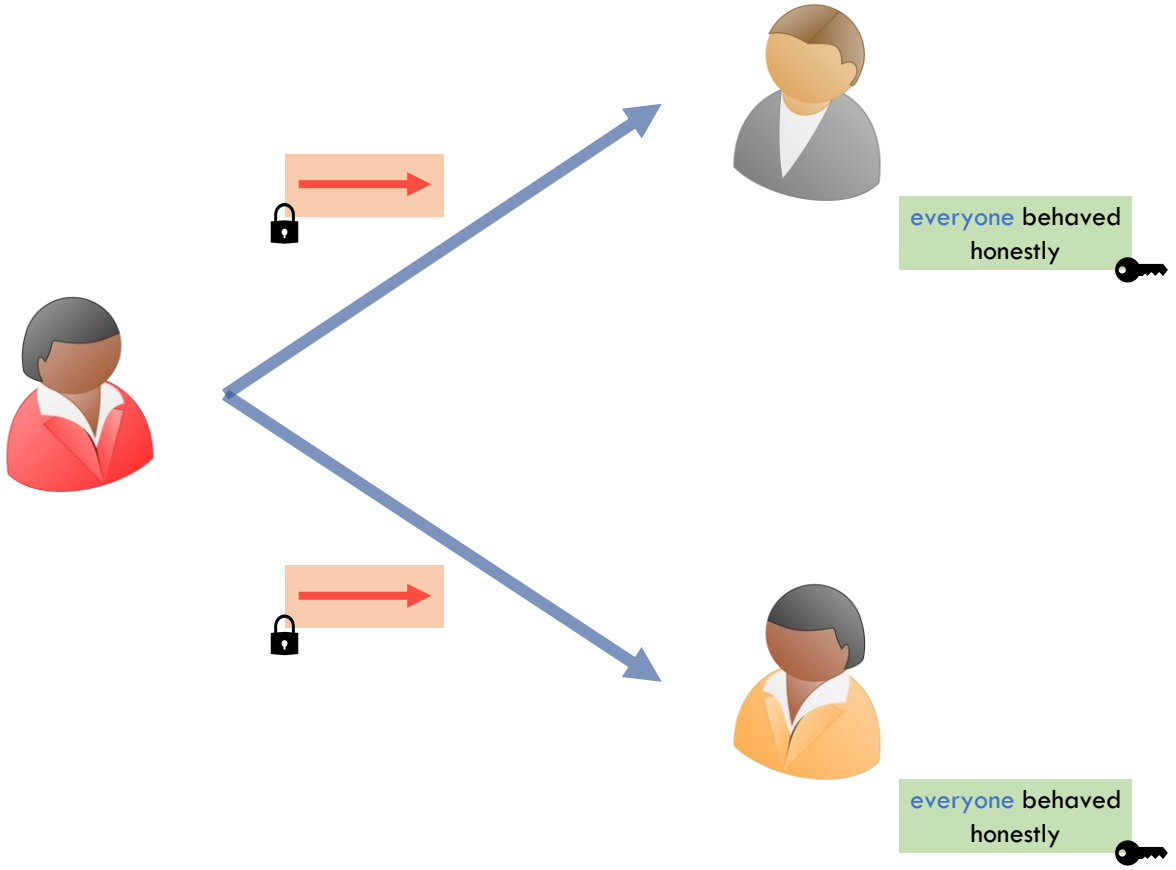
CDS as safety net



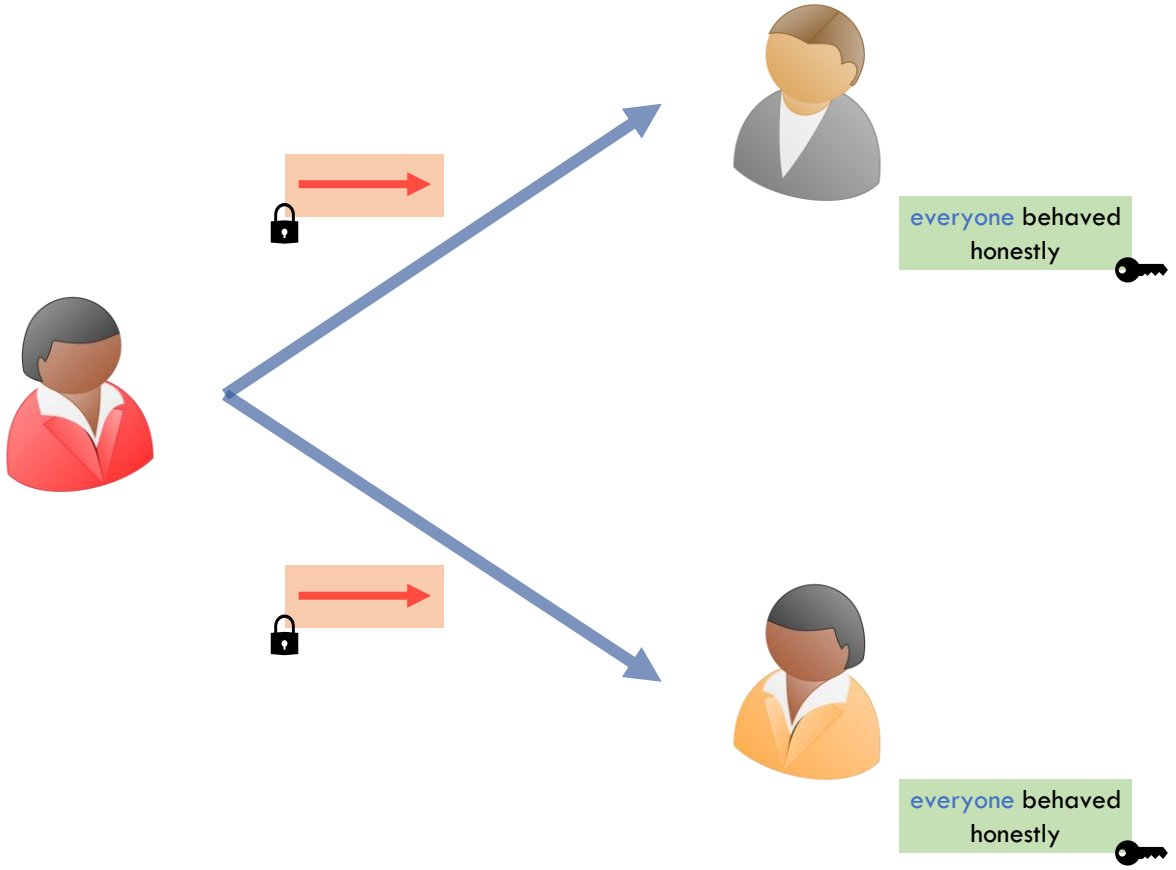
CDS as safety net



CDS as safety net



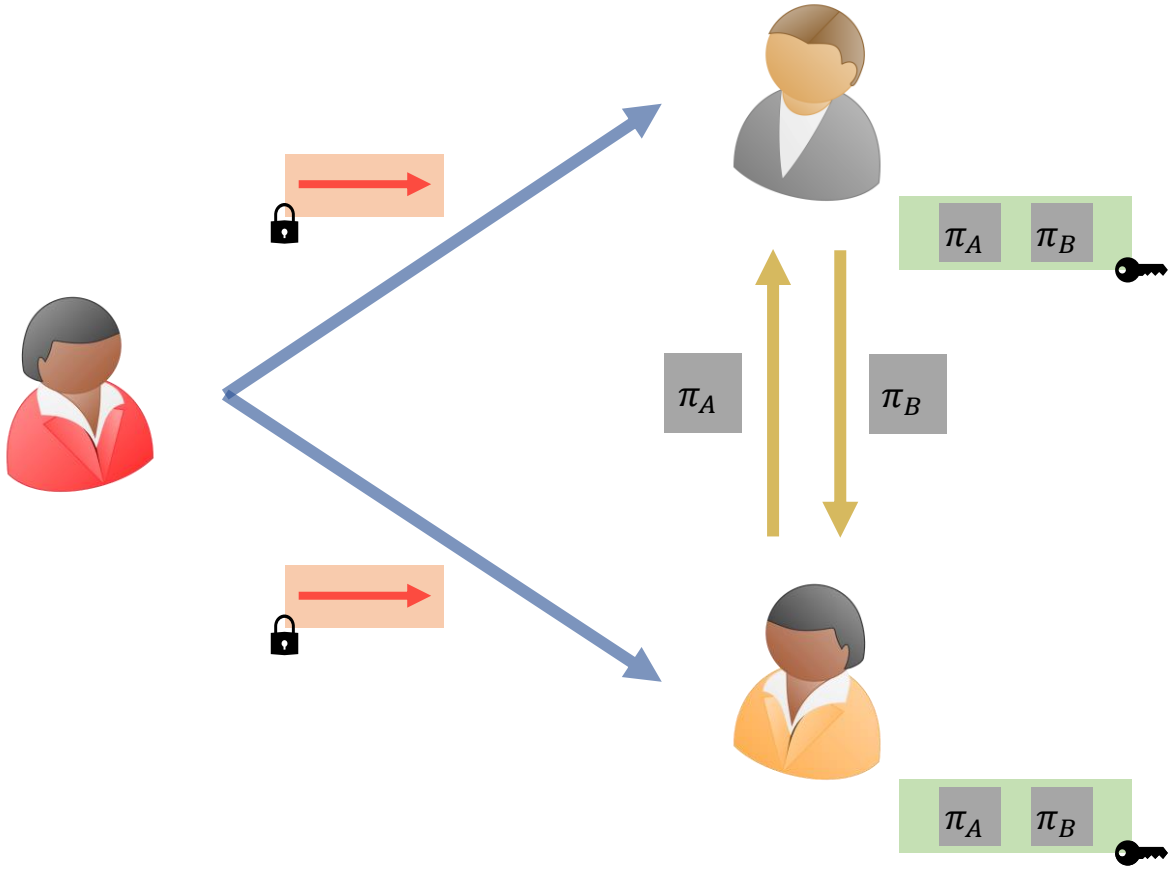
CDS as safety net



Want a public witness at the end of the fourth round.

Use 4 round zero-knowledge proofs.

CDS as safety net



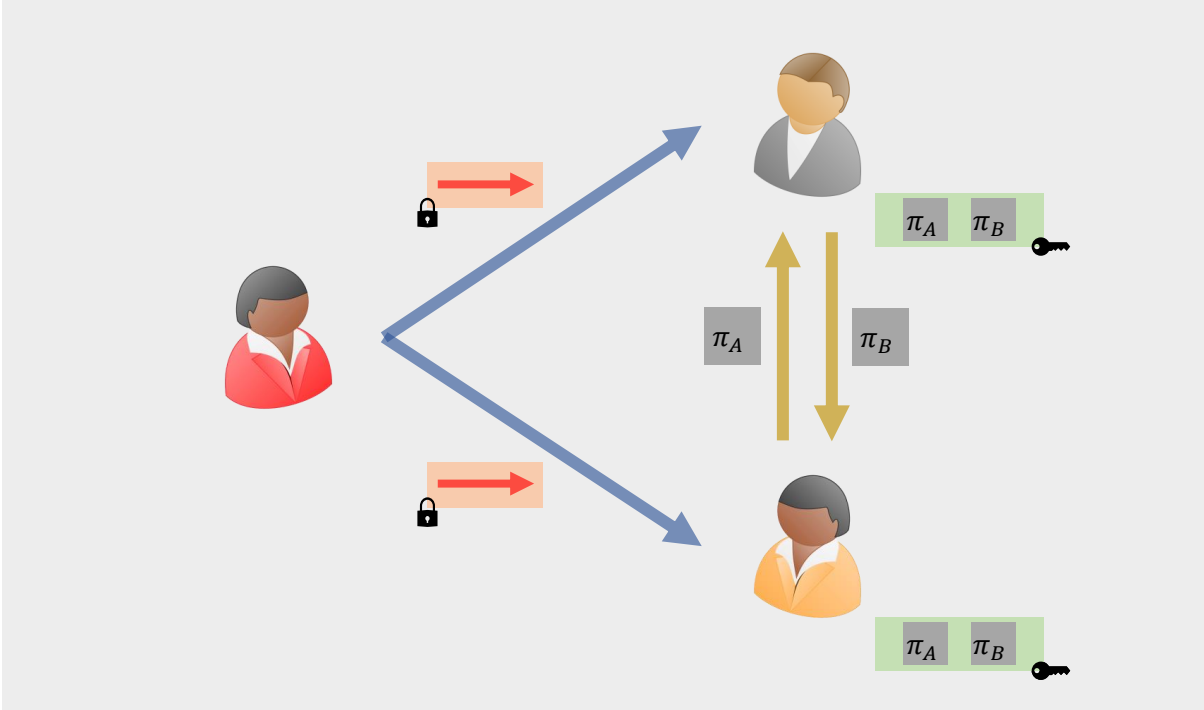
Want a public witness at the end of the fourth round.

Use 4 round zero-knowledge proofs.

Implementing CDS?

We want to build a CDS based on OT.

Only known non-interactive realization is Witness Encryption, which is known assuming Indistinguishability Obfuscation (iO).



Interactive Multiparty CDS (MCDS)

Interactive Multiparty CDS (MCDS)

Oblivious Transfer (OT)

Interactive Multiparty CDS (MCDS)

Oblivious Transfer (OT)

Garbled Circuit

Interactive Multiparty CDS (MCDS)

Oblivious Transfer (OT)

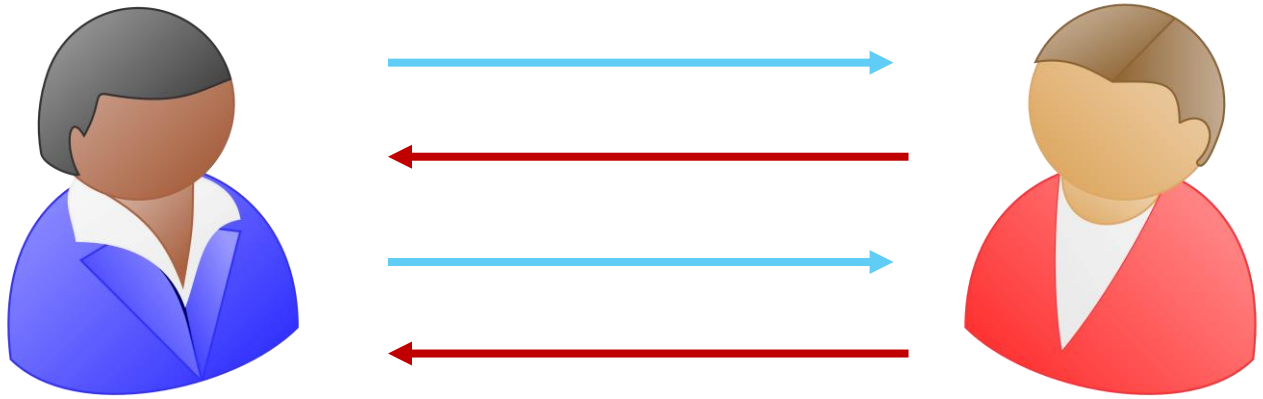
Garbled Circuit

Interactive Multiparty CDS (MCDS)

Oblivious Transfer (OT)

Garbled Circuit

1-out-of-2 OT [Even-Goldreich-Lempel'82]

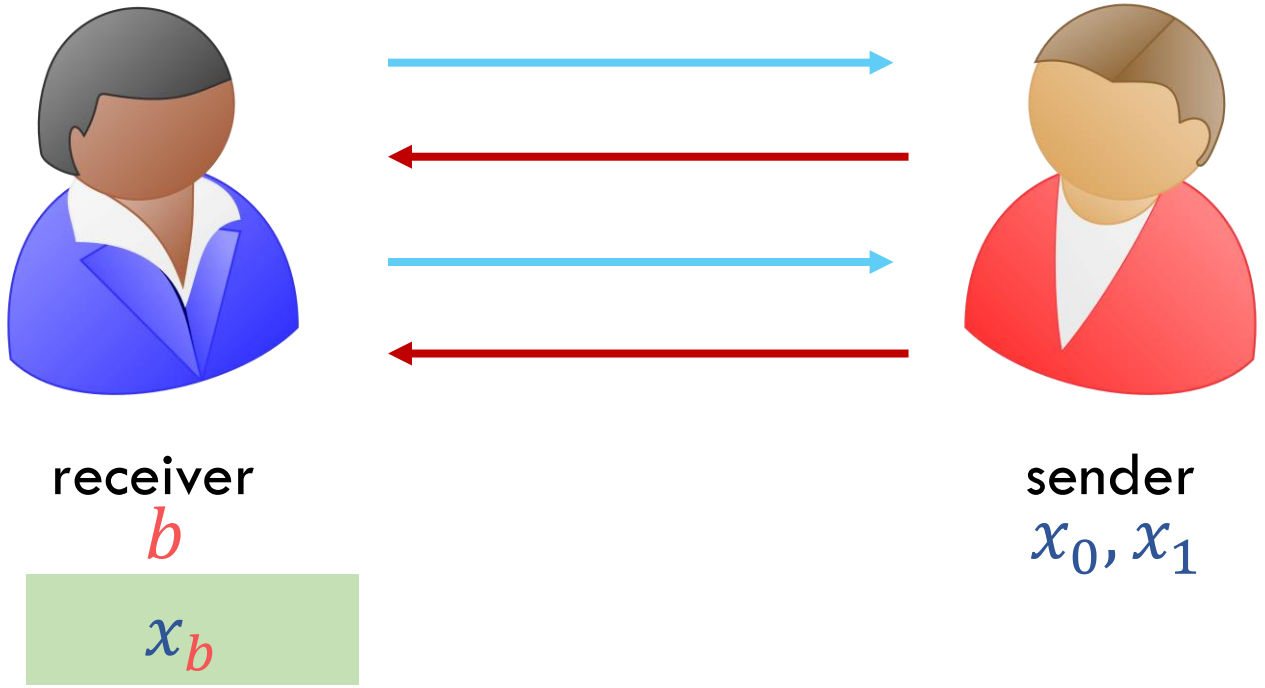


Interactive Multiparty CDS (MCDS)

Oblivious Transfer (OT)

Garbled Circuit

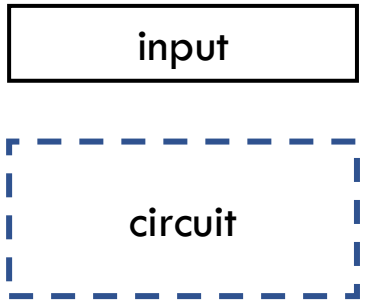
1-out-of-2 OT [Even-Goldreich-Lempel'82]



Interactive Multiparty CDS (MCDS)

Oblivious Transfer (OT)

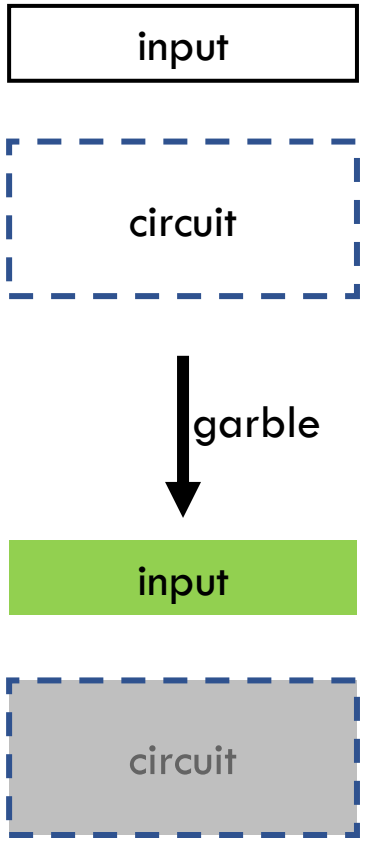
Garbled Circuit



Interactive Multiparty CDS (MCDS)

Oblivious Transfer (OT)

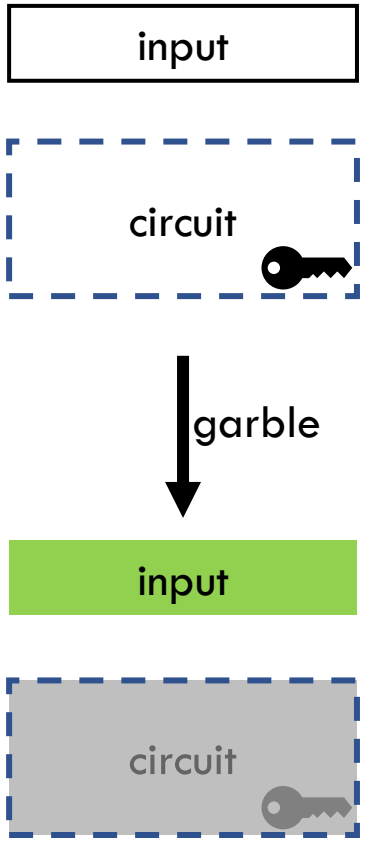
Garbled Circuit



Interactive Multiparty CDS (MCDS)

Oblivious Transfer (OT)

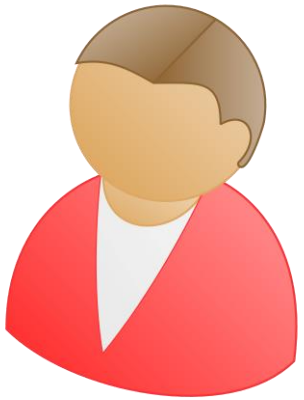
Garbled Circuit



Interactive MCDS

witness

receiver



sender

message

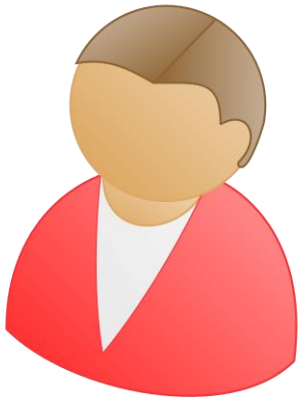
Input: witness

if witness satisfies condition,
output message

Interactive MCDS

witness

receiver



sender

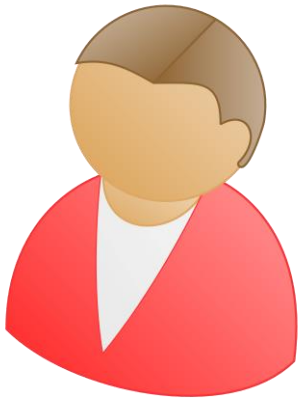
message

Input: witness

if witness satisfies condition,
output message

Interactive MCDS

witness



message

Input: witness

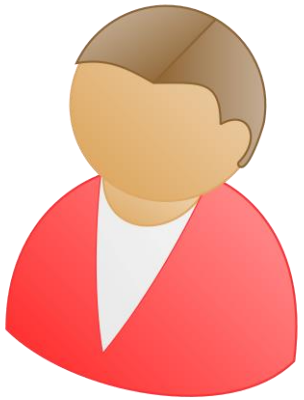
if witness satisfies condition,
output message

receiver

sender

Interactive MCDS

witness



message

Input: witness

if witness satisfies condition,
output message

receiver

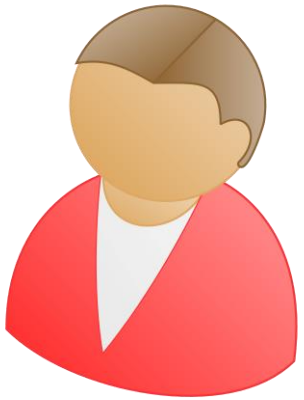
sender

Interactive MCDS

witness

Input: witness

if witness satisfies condition,
output message



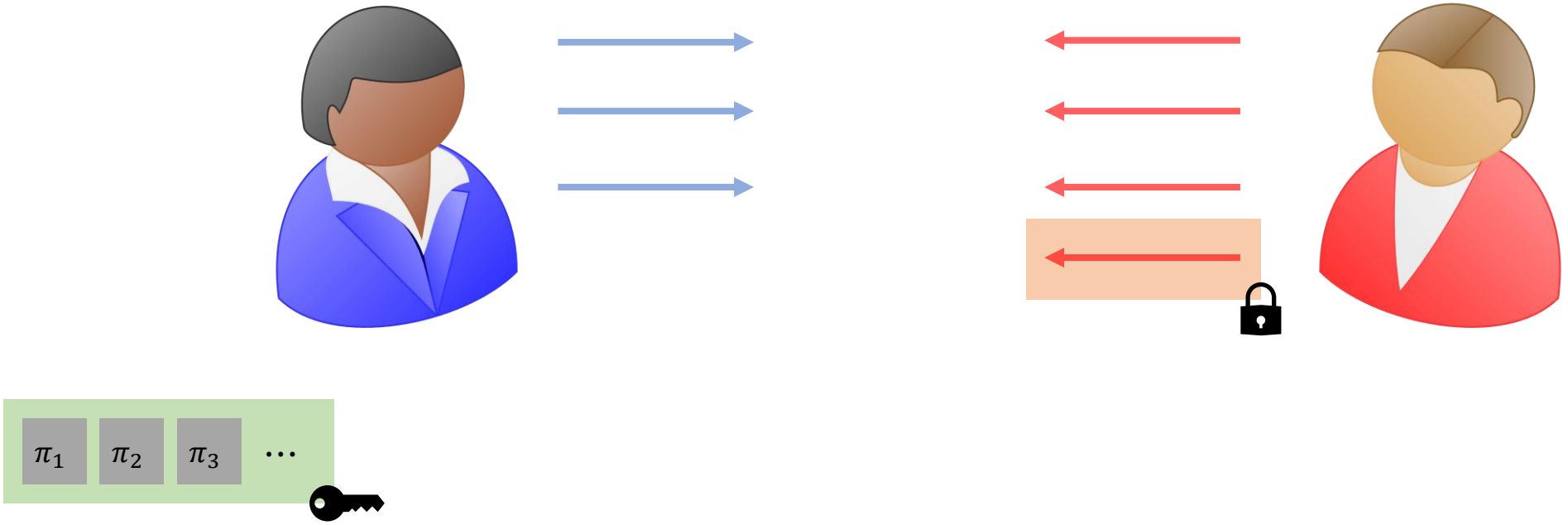
message

receiver

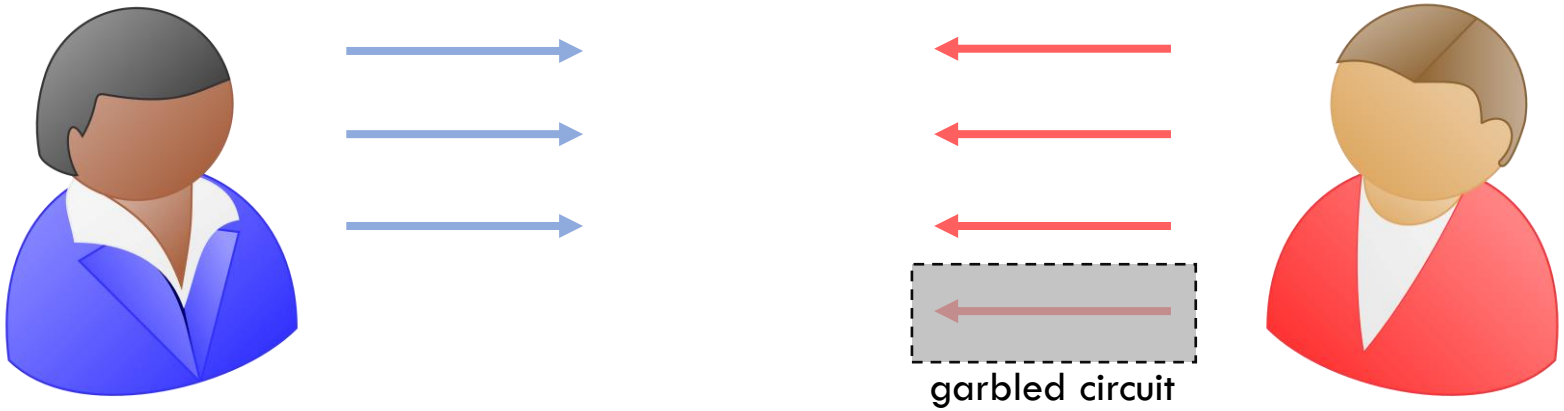
sender

Interactive MCDS to protect 4^{th} round

Interactive MCDS to protect 4^{th} round

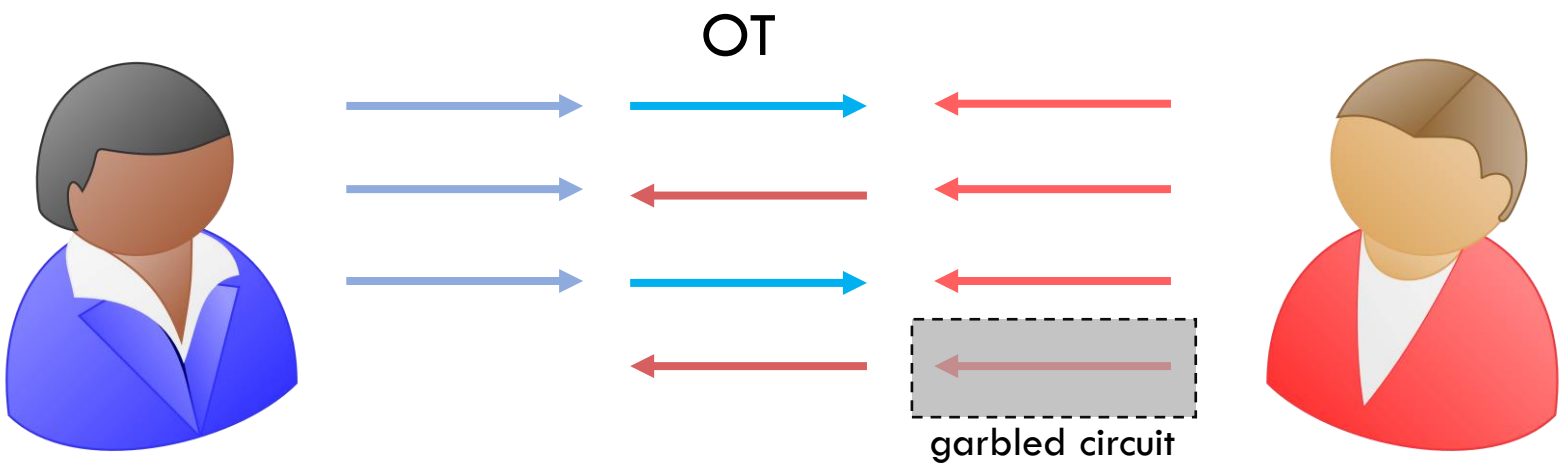


Interactive MCDS to protect 4^{th} round



π_1 π_2 π_3 $\cdots$

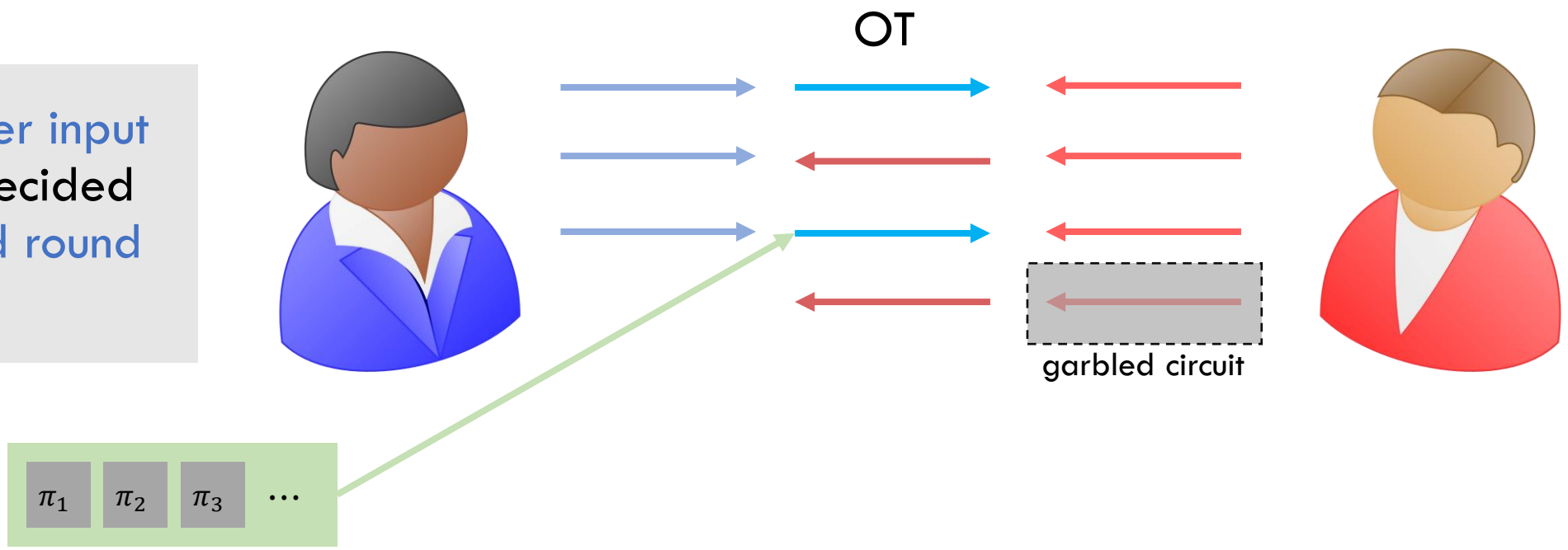
Interactive MCDS to protect 4^{th} round



π_1 π_2 π_3 $\cdots$

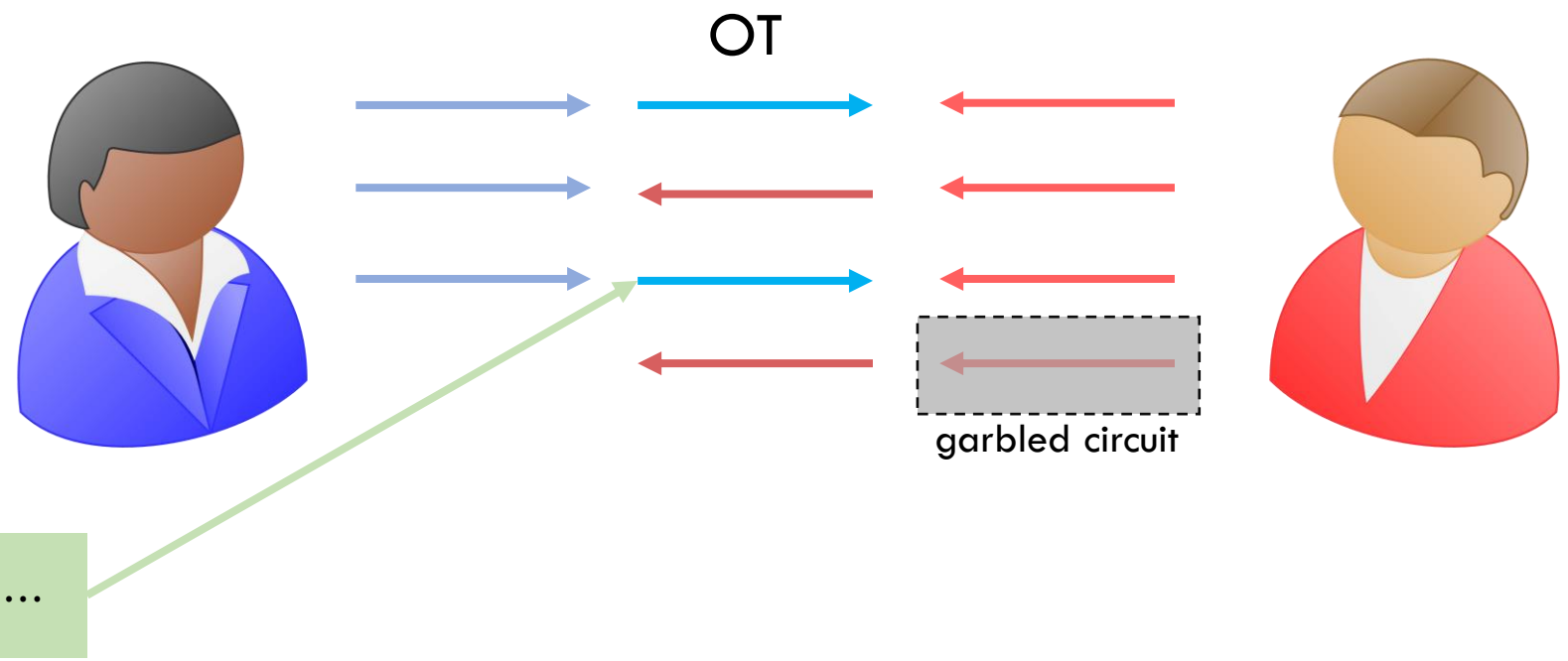
Interactive MCDS to protect 4^{th} round

OT receiver input must be decided by the 3rd round of the OT.



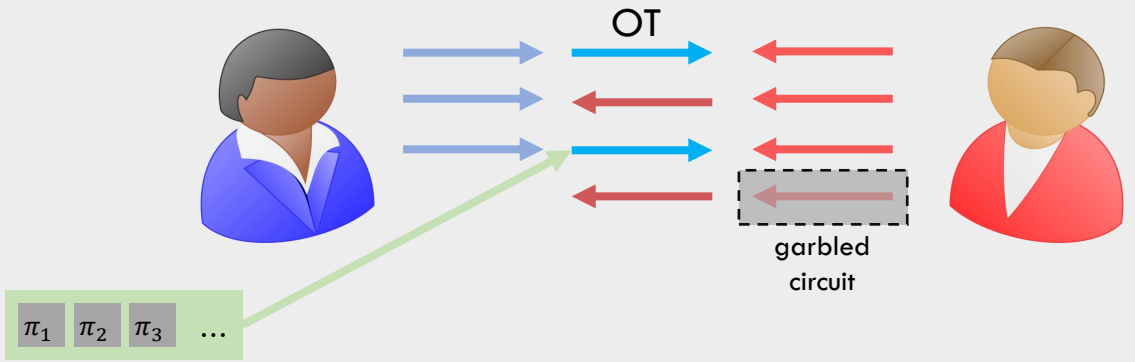
Interactive MCDS to protect 4^{th} round

OT receiver input must be decided by the 3rd round of the OT.



Requires 3 round zero-knowledge proofs!

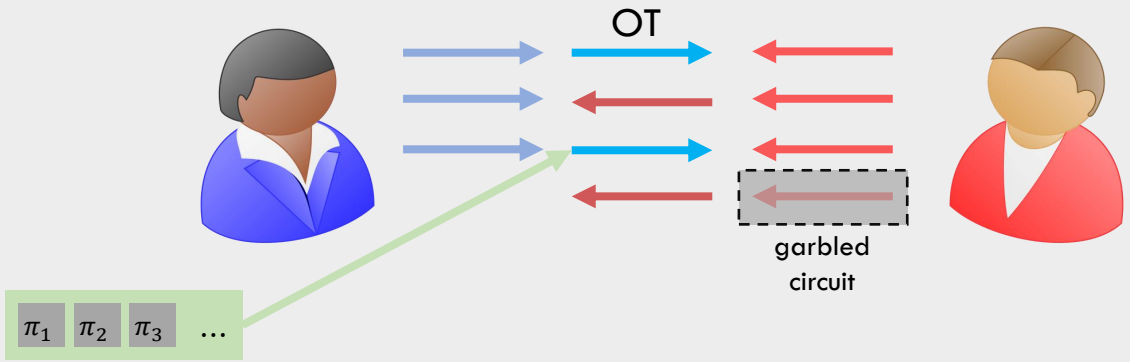
Weakened Requirement from ZK proof?



Requires 3 round zero-knowledge proofs!

Weakened Requirement from ZK proof?

1. ZK in the simultaneous message model.

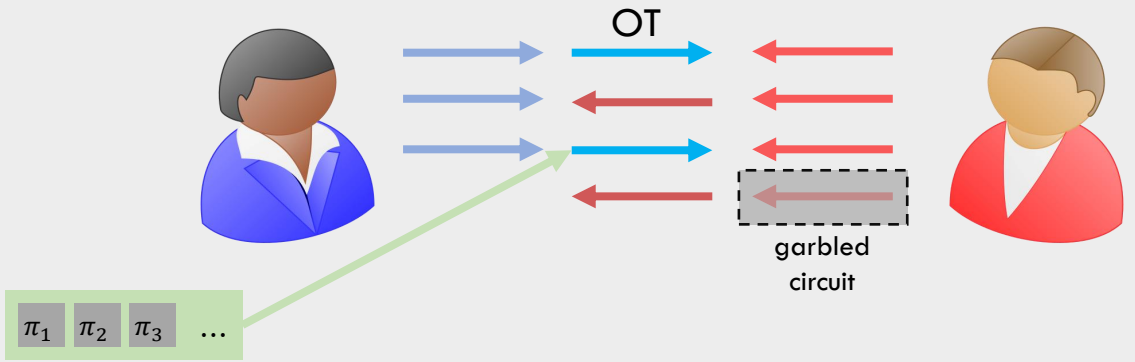


Requires 3 round zero-knowledge proofs!

Weakened Requirement from ZK proof?

1. ZK in the simultaneous message model.
2. The third round of the ZK proof hidden until the fourth round of MPC.

   Remains hidden if Bob aborts in the third round. Essentially repurposing a three round protocol to work in four rounds.

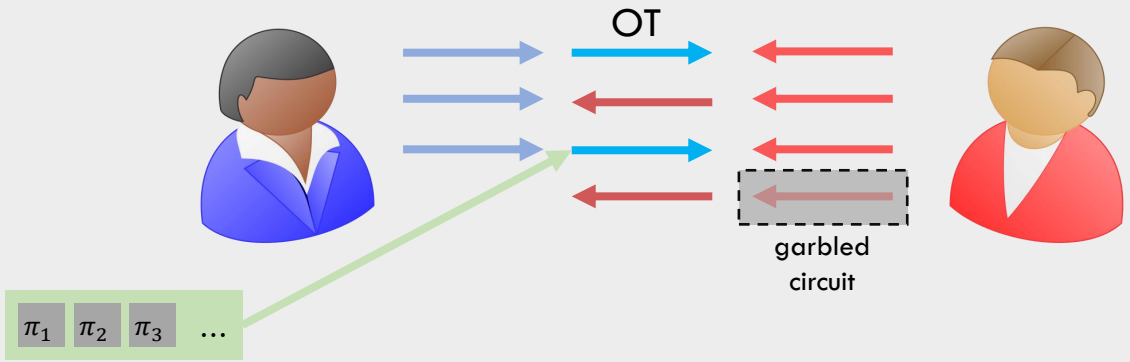


Requires 3 round zero-knowledge proofs!

Weakened Requirement from ZK proof?

1. ZK in the simultaneous message model.
2. The third round of the ZK proof hidden until the fourth round of MPC.

   Remains hidden if Bob aborts in the third round. Essentially repurposing a three round protocol to work in four rounds.



Requires 3 round zero-knowledge proofs!

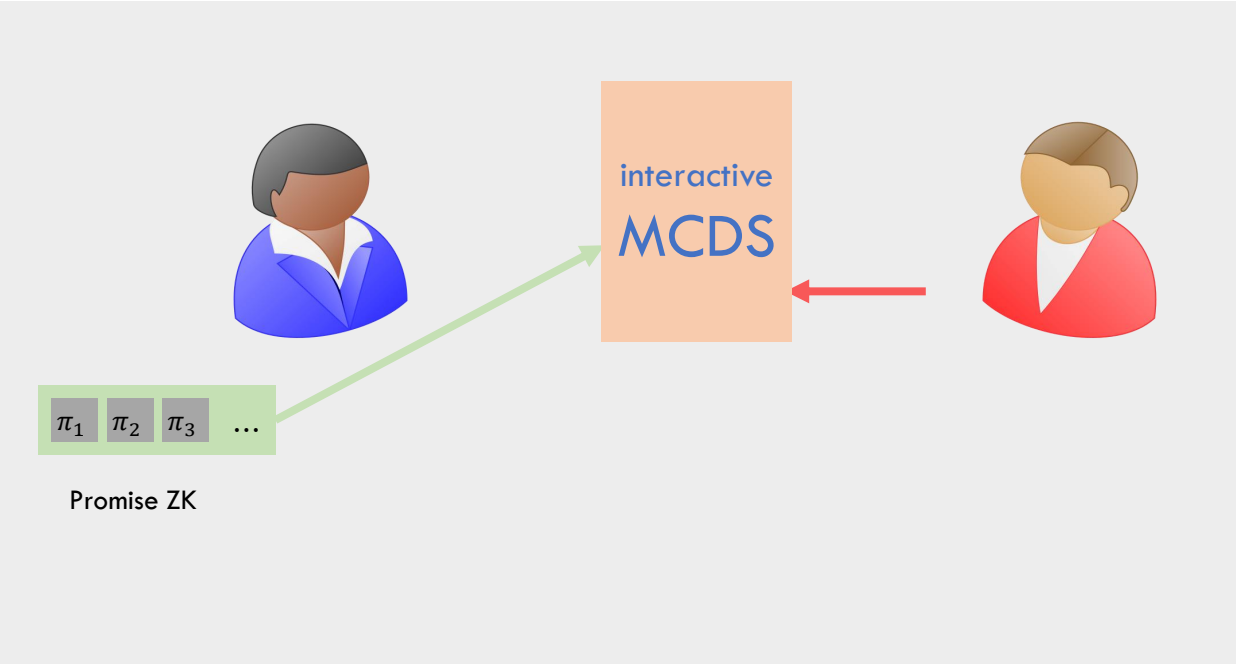
Promise Zero-Knowledge [Badrinarayanan-Goyal-Jain-Kalai-Khurana-Sahai18]

Assuming OT, there exists a 3 round zero-knowledge protocol in the simultaneous message model secure against verifiers who do not abort.

Weakened Requirement from ZK proof?

1. ZK in the simultaneous message model.
2. The third round of the ZK proof hidden until the fourth round of MPC.

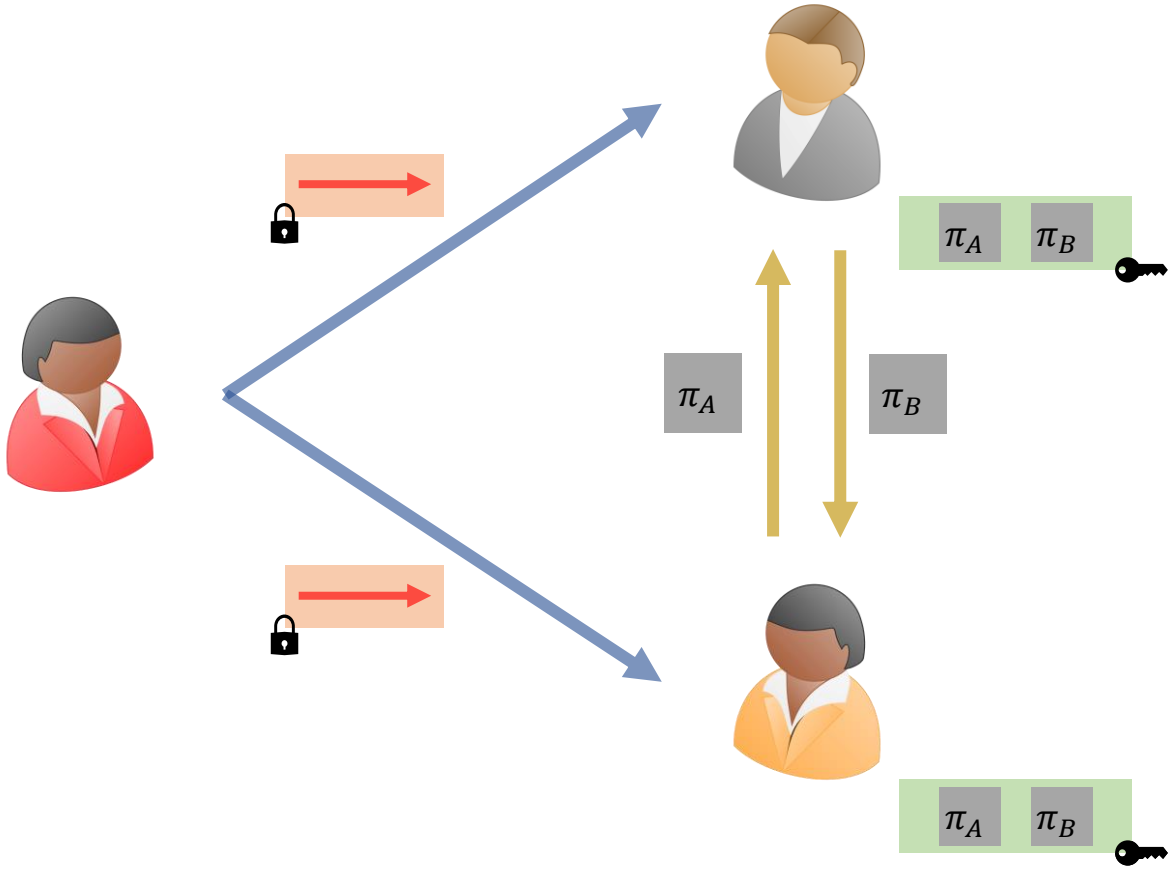
   Remains hidden if Bob aborts in the third round. Essentially repurposing a three round protocol to work in four rounds.



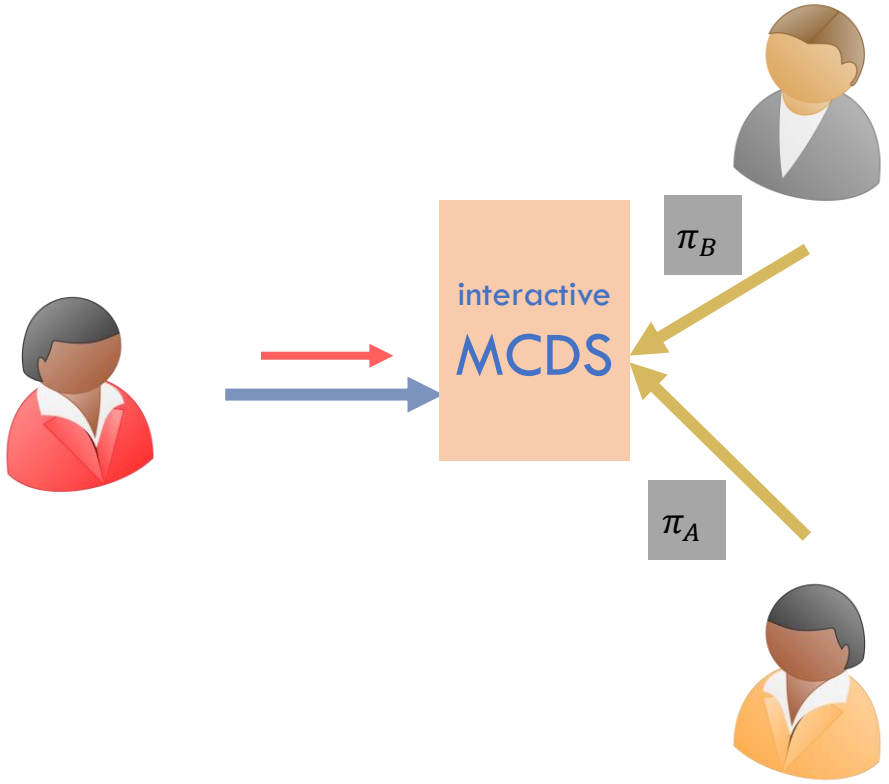
Promise Zero-Knowledge [Badrinarayanan-Goyal-Jain-Kalai-Khurana-Sahai18]

Assuming OT, there exists a 3 round zero-knowledge protocol in the simultaneous message model secure against verifiers who do not abort.

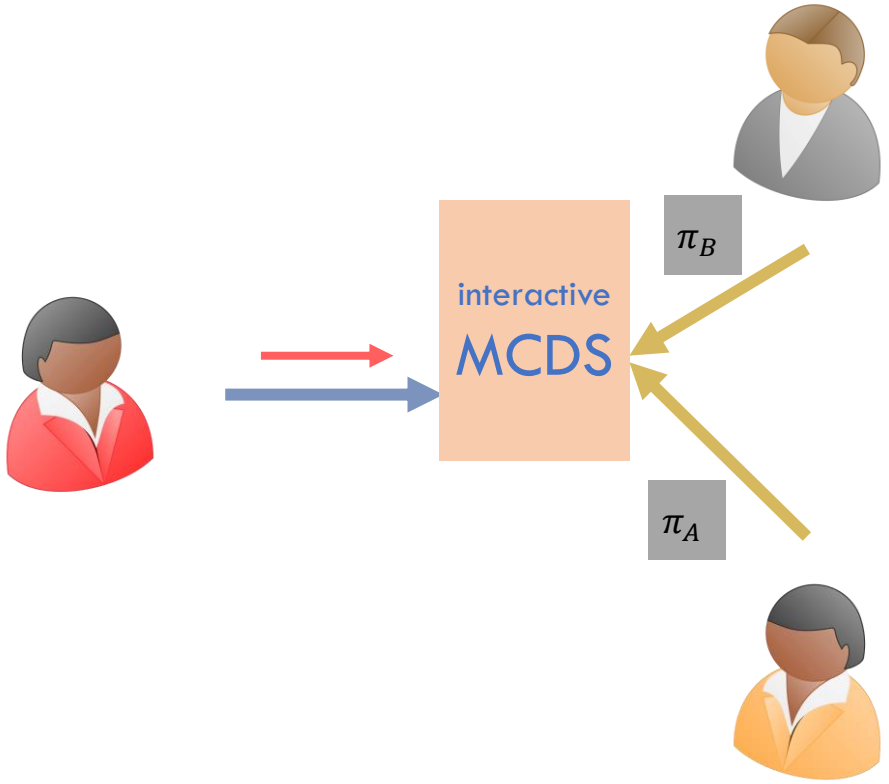
Putting it together in the multiparty setting



Putting it together in the multiparty setting



Putting it together in the multiparty setting



Receive Carol's fourth round message if Promise ZK proofs of Alice and Bob verify.

Nobody receives Carol's message if even one party cheats.

Towards a Full Protocol

Many moving components in the final protocol.

Towards a Full Protocol

Many moving components in the final protocol.

Non-malleability challenges in limited rounds.

Towards a Full Protocol

Many moving components in the final protocol.

Non-malleability challenges in limited rounds.

Black-box simulation requires rewinding the adversary.

- Eg: used to extract adversary's input.
- Primitives need to be secure in the presence of rewinds.

Towards a Full Protocol

Many moving components in the final protocol.

Non-malleability challenges in limited rounds.

Black-box simulation requires rewinding the adversary.

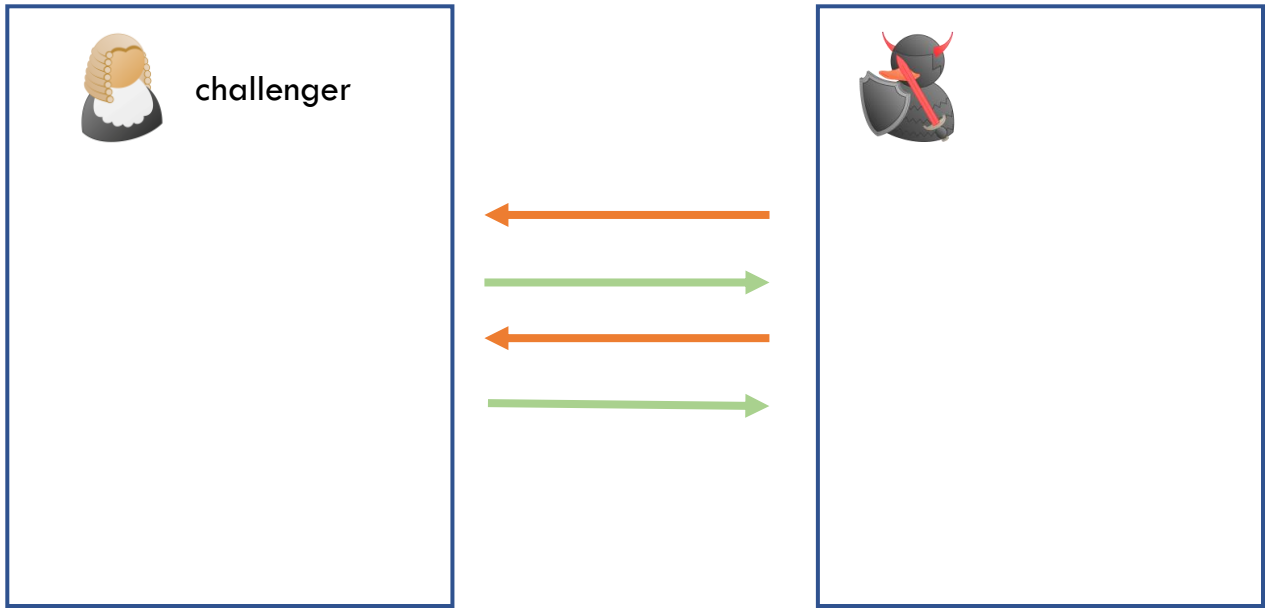
- Eg: used to extract adversary's input.
- Primitives need to be secure in the presence of rewinds.

[New!] Assuming regular OT, we construct an OT protocol that retains security guarantees in the presence of a bounded number of rewinds.

Bounded Rewind Secure OT

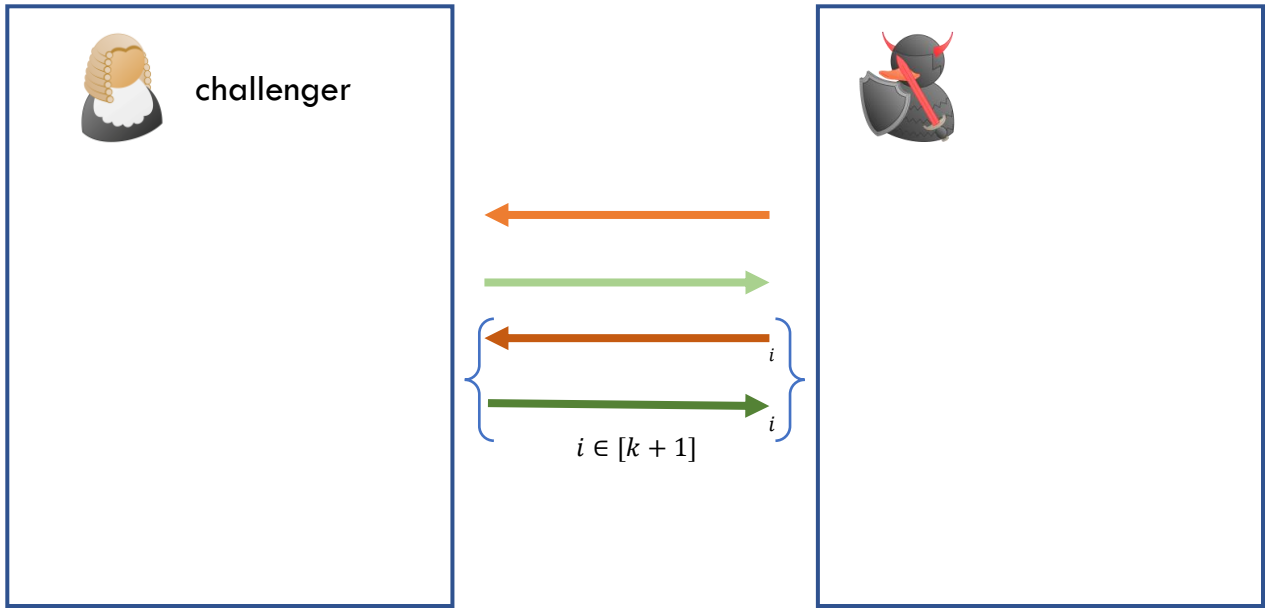
High level idea

k-Bounded Rewind Security



Regular challenger-adversary game

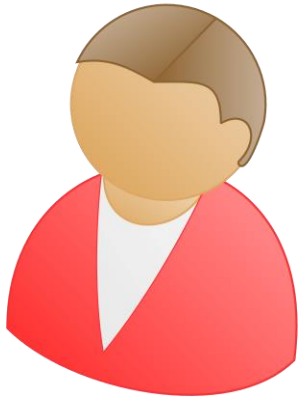
k-Bounded Rewind Security



Bounded rewind challenger-adversary game

4 round 1-Rewind Secure OT

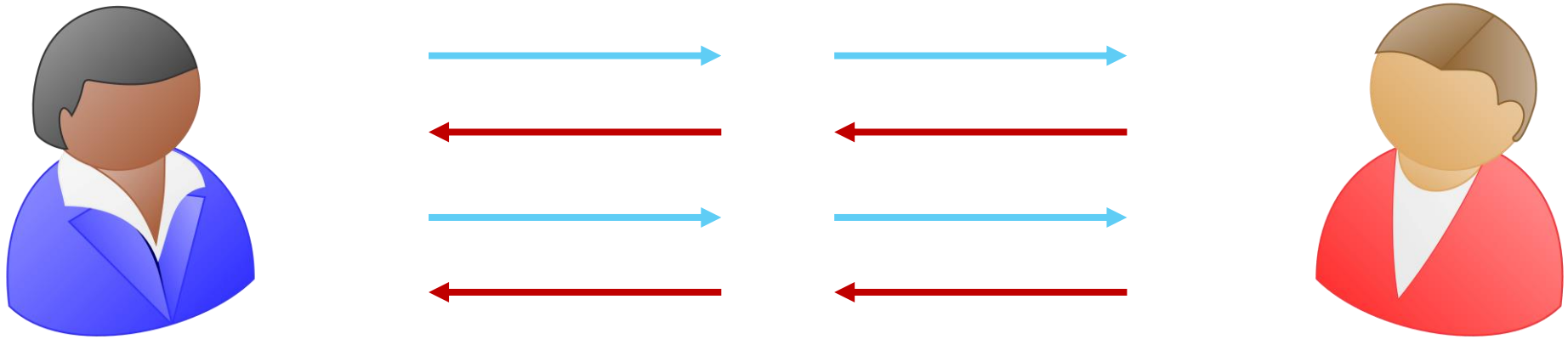
receiver
b



sender
x_0, x_1

Receiver input should be hidden from an adversarial sender that can rewind the receiver once.

4 round 1-Rewind Secure OT

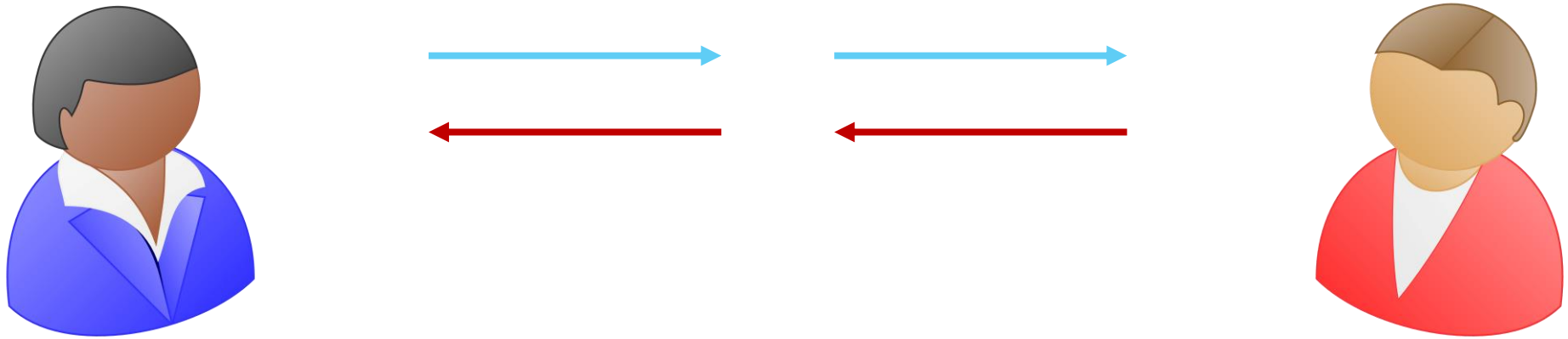


receiver
b

sender
x_0, x_1

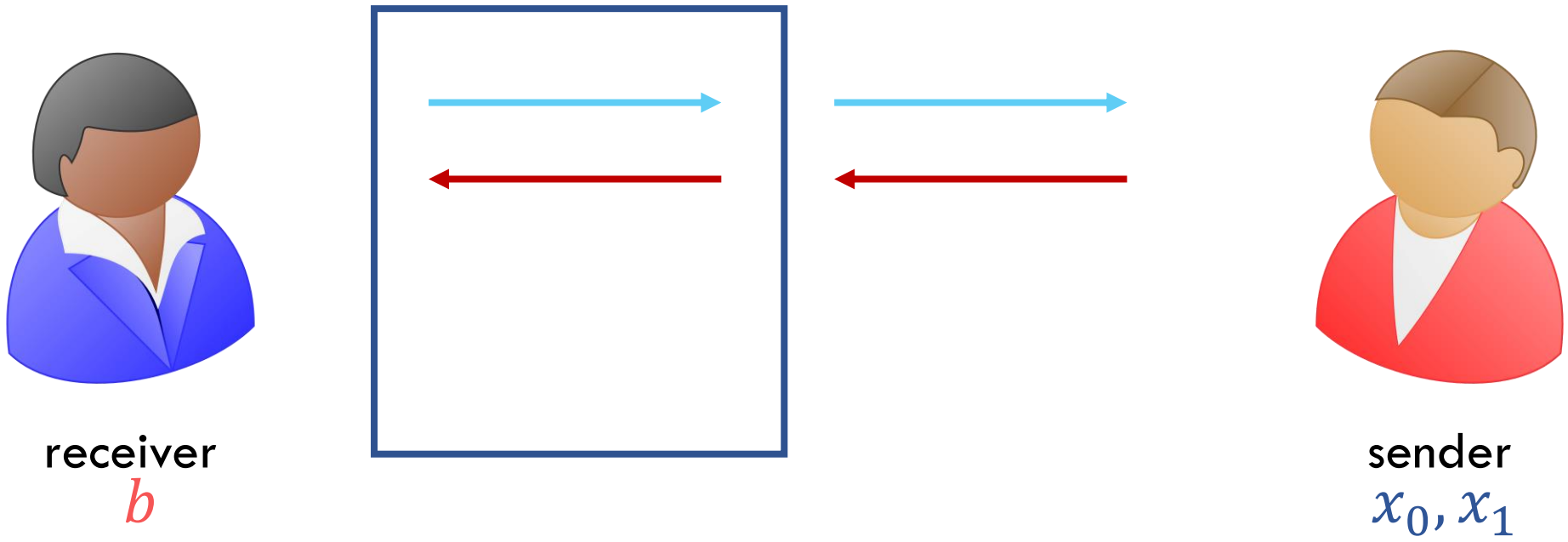
Run two parallel copies of the OT. The receiver picks a random OT in the third round to proceed.

4 round 1-Rewind Secure OT



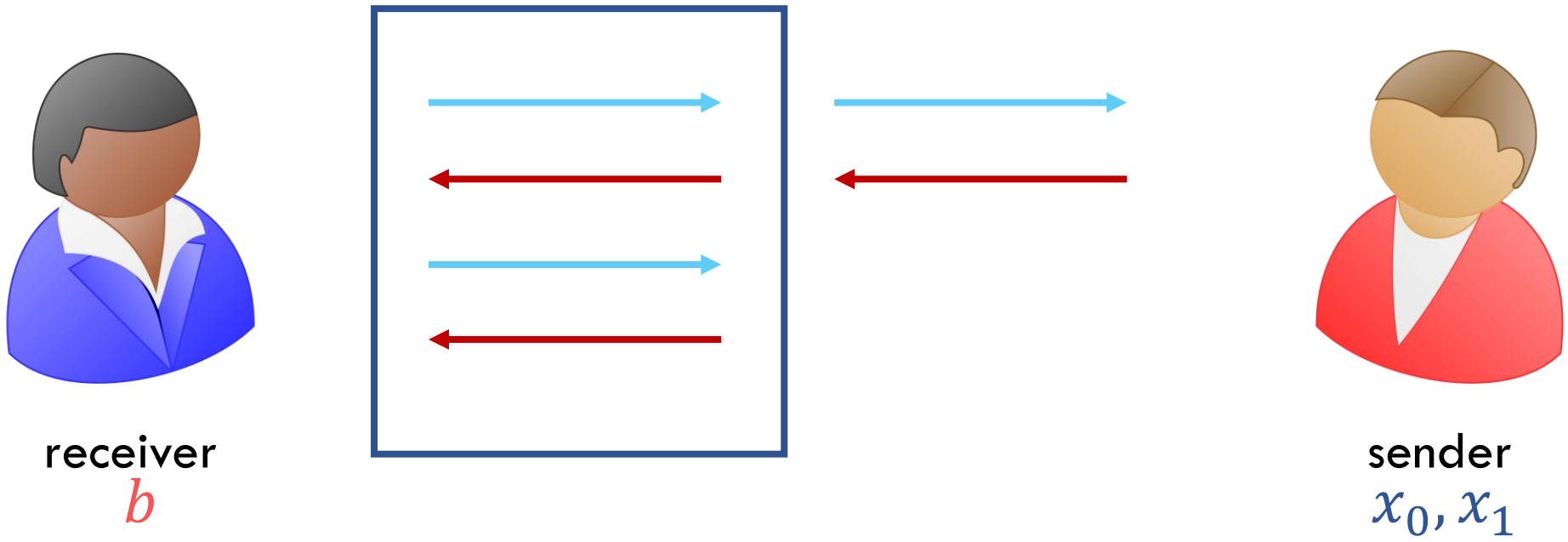
Run two parallel copies of the OT. The receiver picks a random OT in the third round to proceed.

4 round 1-Rewind Secure OT



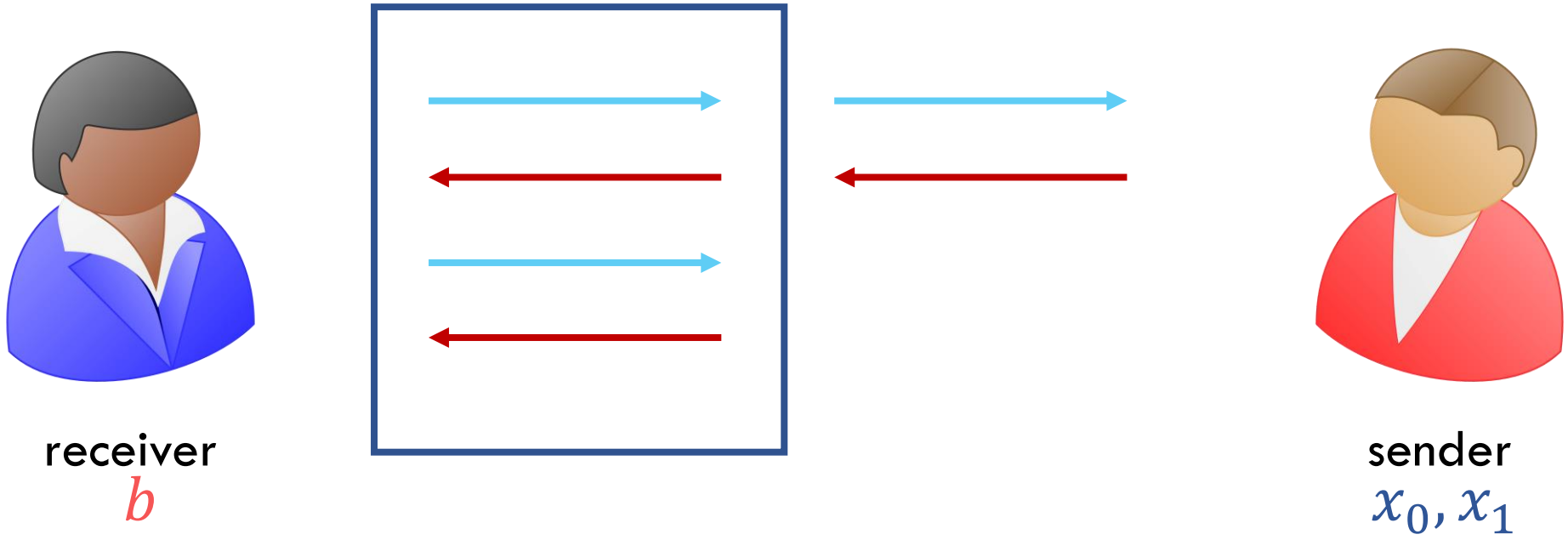
Run two parallel copies of the OT. The receiver picks a random OT in the third round to proceed.

4 round 1-Rewind Secure OT



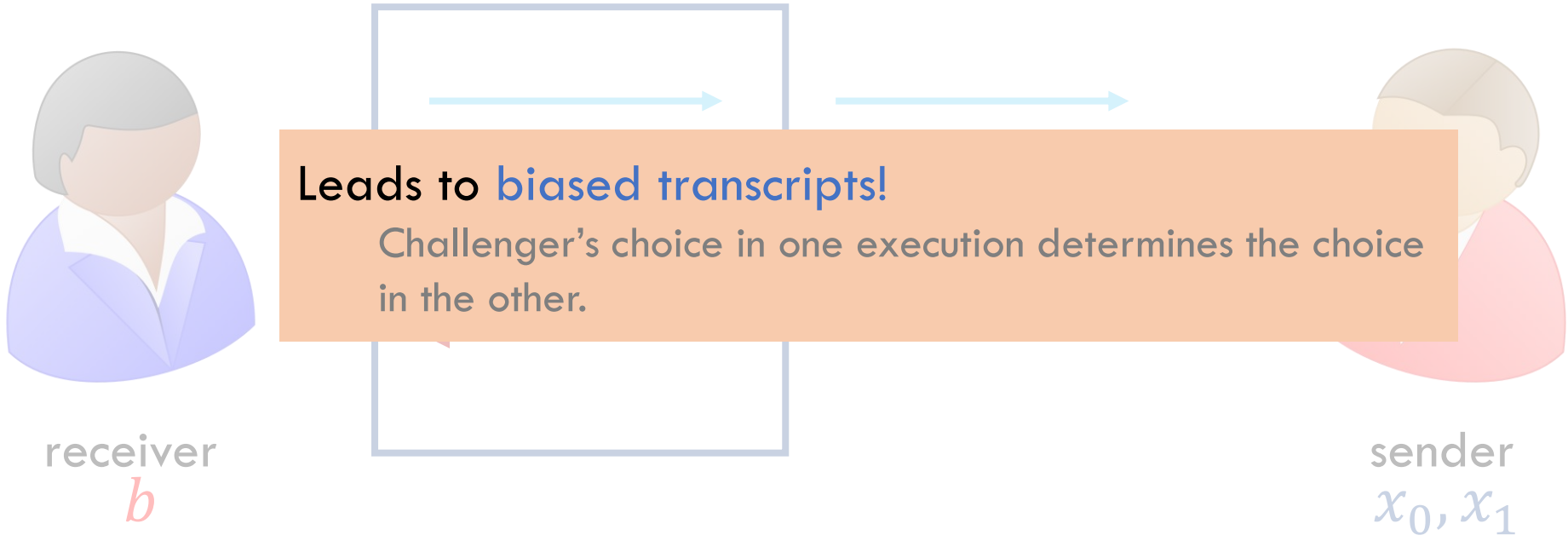
Run two parallel copies of the OT. The receiver picks a random OT in the third round to proceed.

4 round 1-Rewind Secure OT



Challenger can use a different instance in the two executions (one rewind).

4 round 1-Rewind Secure OT



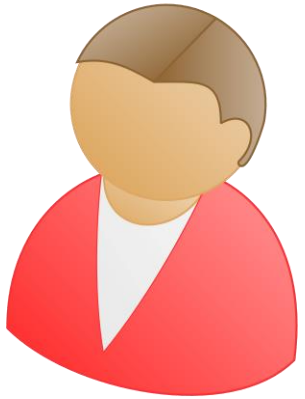
Challenger can use a different instance in the two executions (one rewind).

4 round 1-Rewind Secure OT

High level idea: secret share receiver input

receiver

$b = b_1 \oplus b_2$

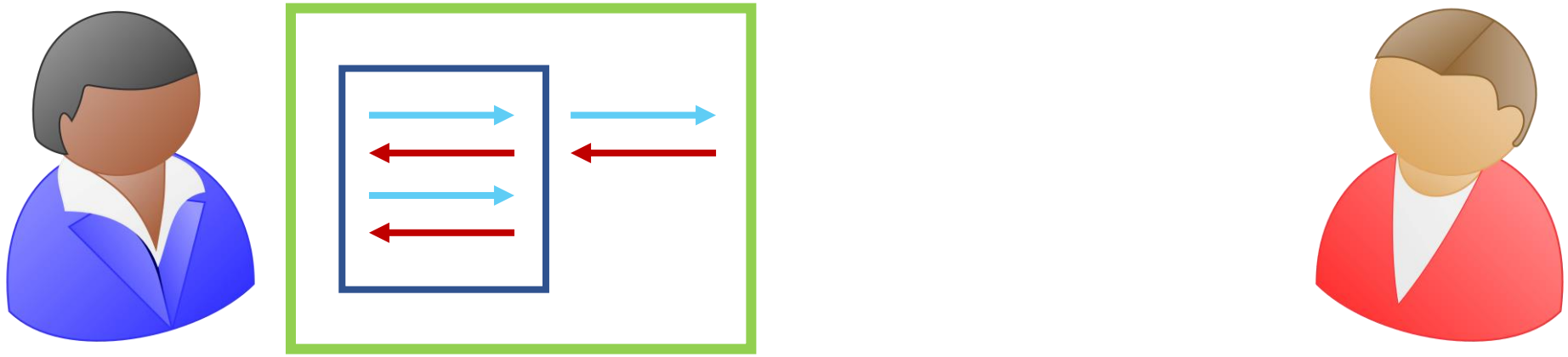


sender

x_0, x_1

4 round 1-Rewind Secure OT

High level idea: secret share receiver input



receiver

$b = b_1 \oplus b_2$

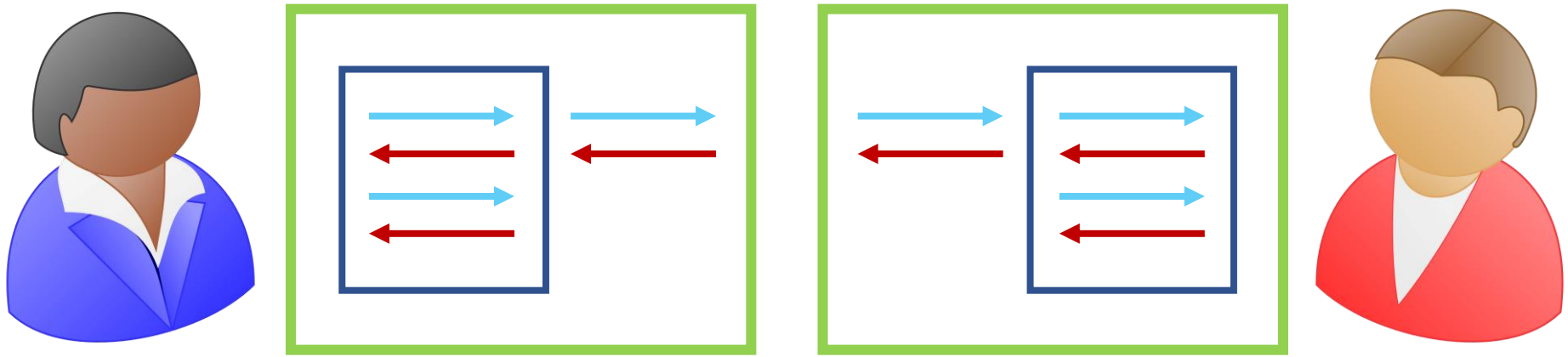
b_1

sender

x_0, x_1

4 round 1-Rewind Secure OT

High level idea: secret share receiver input



receiver

$b = b_1 \oplus b_2$

b_1

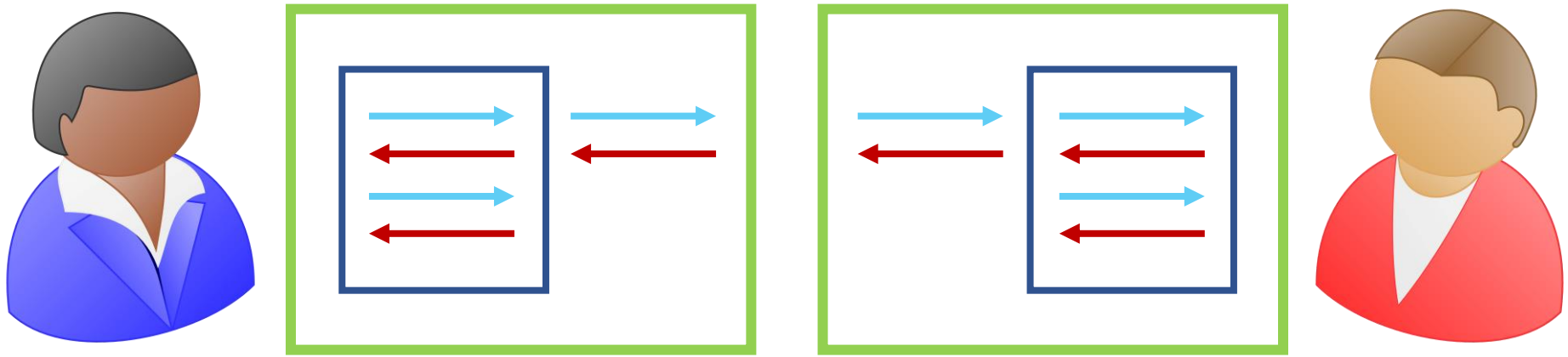
b_2

sender

x_0, x_1

4 round 1-Rewind Secure OT

High level idea: secret share receiver input



receiver

$b = b_1 \oplus b_2$

sender

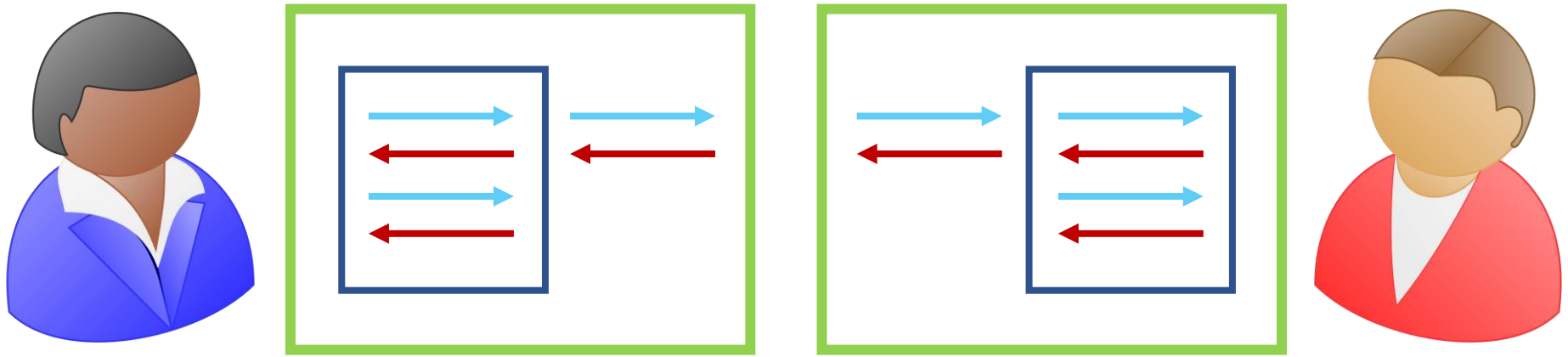
x_0, x_1

In each execution, the challenger independently samples which instance to use for every index.

Secure if at least one index results in two different executions. Can be amplified.

4 round 1-Rewind Secure OT

High level idea: secret share receiver input



receiver

$b = b_1 \oplus b_2$

sender

x_0, x_1

High level idea: details missing.

In each execution, the challenger independently samples which instance to use for every index.

Secure if at least one index results in two different executions. Can be amplified.

Assuming 4 round oblivious transfer (OT), there exists a 4 round MPC protocol.

Assuming 4 round oblivious transfer (OT), there exists a 4 round MPC protocol.

Thank you. Questions?

Arka Rai Choudhuri

achoud@cs.jhu.edu

ia.cr/2019/216