

# 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

Abhishek Jain

Johns Hopkins University

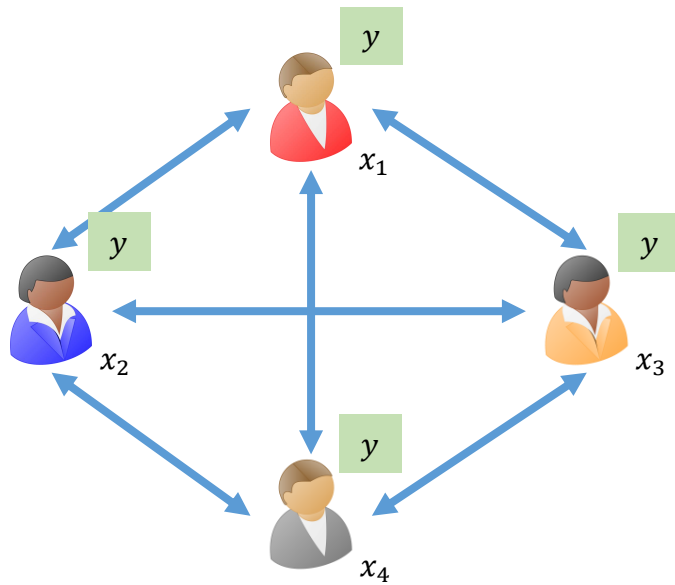
Rafail Ostrovsky

University of California  
Los Angeles

DC Area Crypto Day, Fall 2019

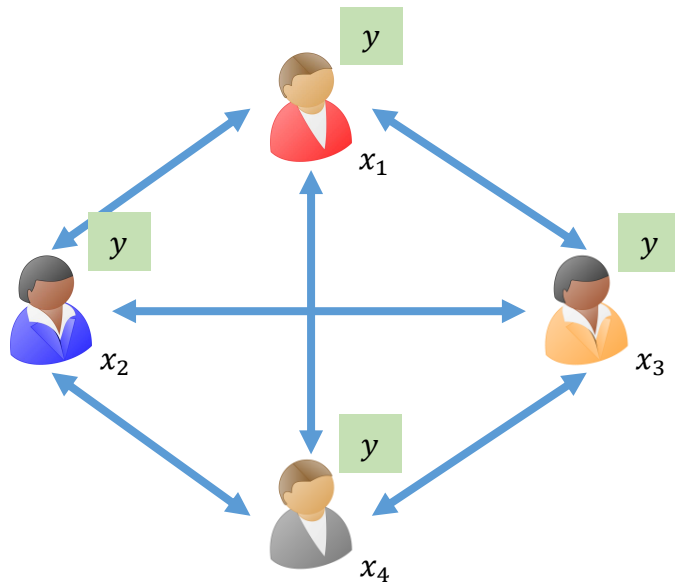
Can we construct **round optimal** multiparty computation from **minimal assumptions**?

# Multiparty Computation (MPC)



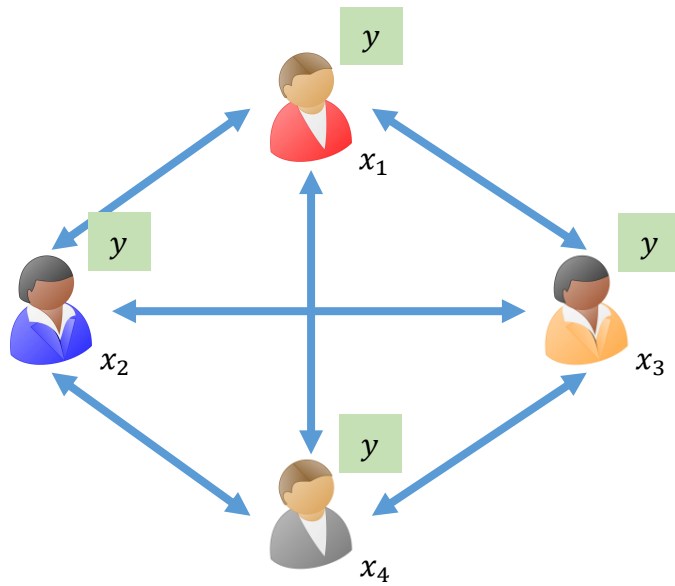
$$y = f(x_1, x_2, x_3, x_4)$$

# Multiparty Computation (MPC)



What is a **round** of computation?

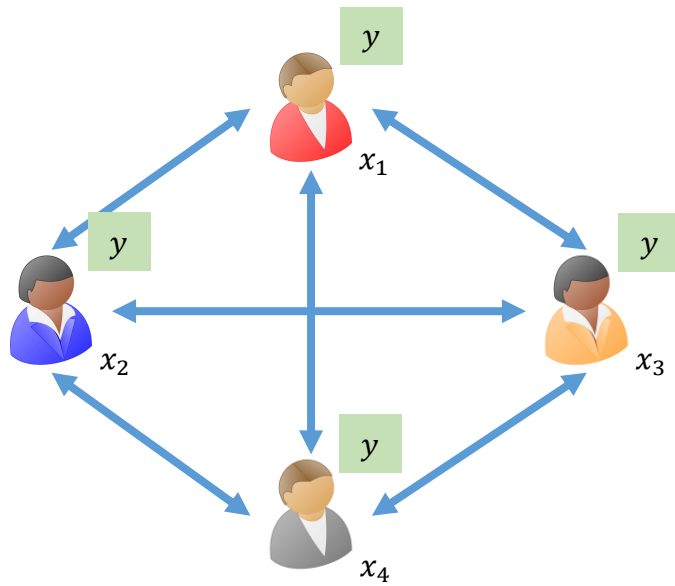
# Security



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

# Security

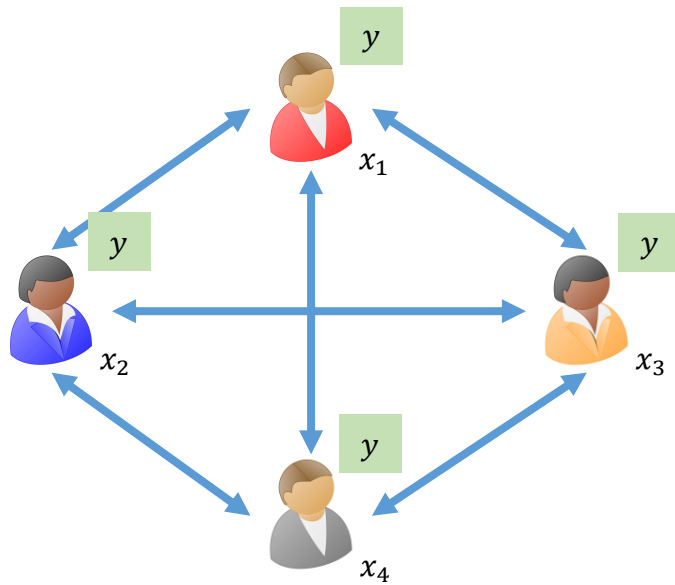
real world



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

# Security

real world

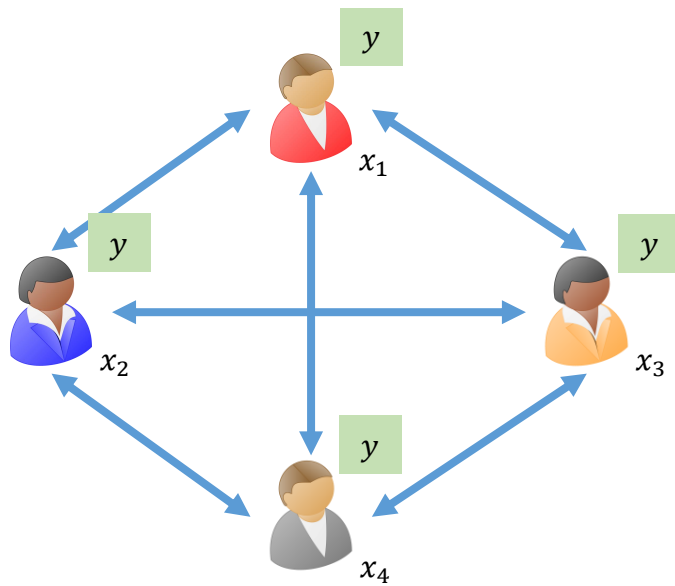


$$y = f(x_1, x_2, x_3, x_4)$$

ideal world

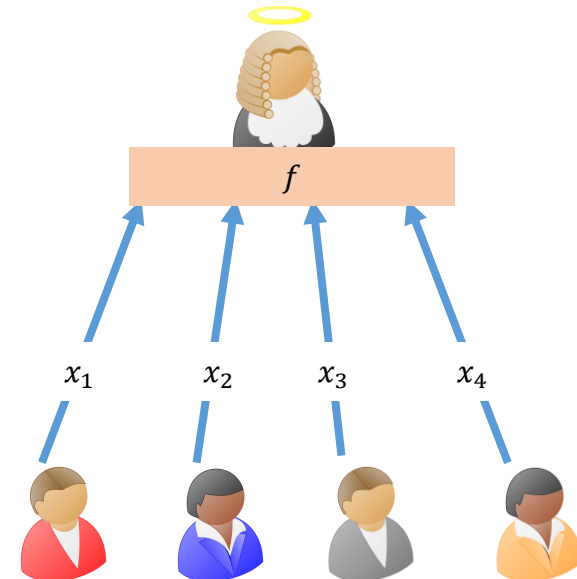
# Security

real world



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

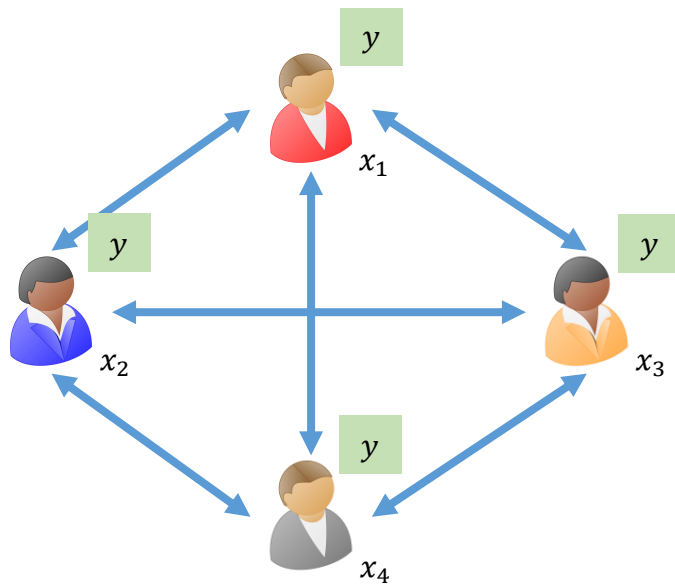
ideal world





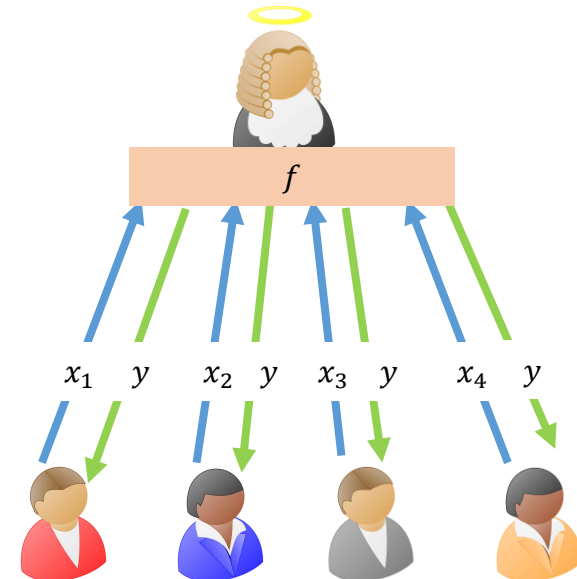
# Security

real world



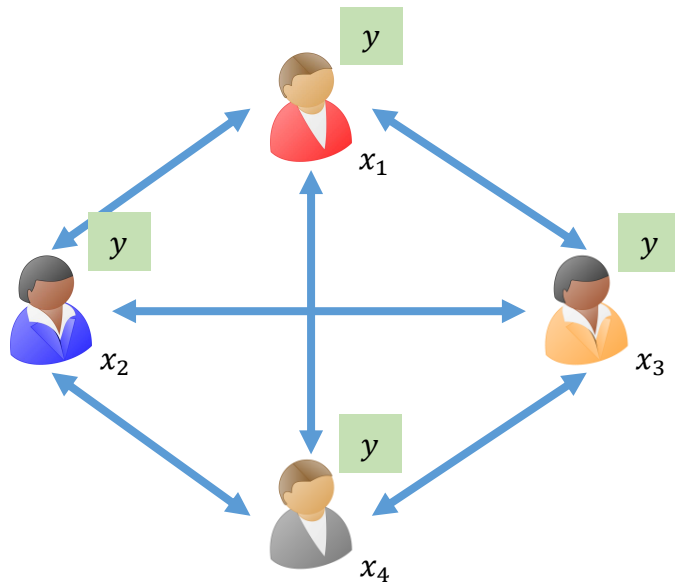
$$y = f(x_1, x_2, x_3, x_4)$$

ideal world



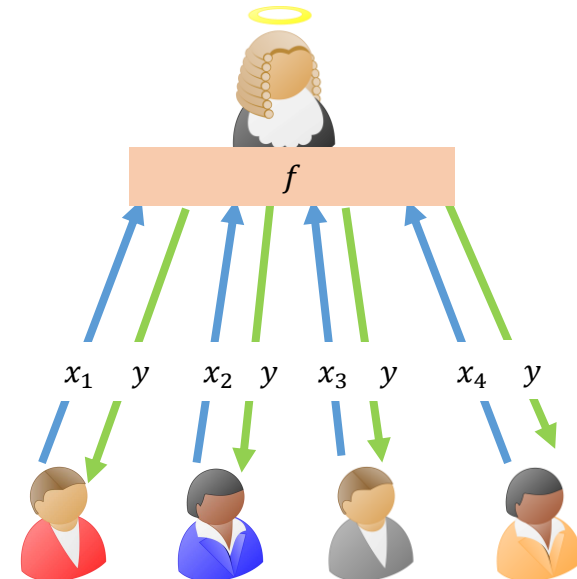
# Security

real world



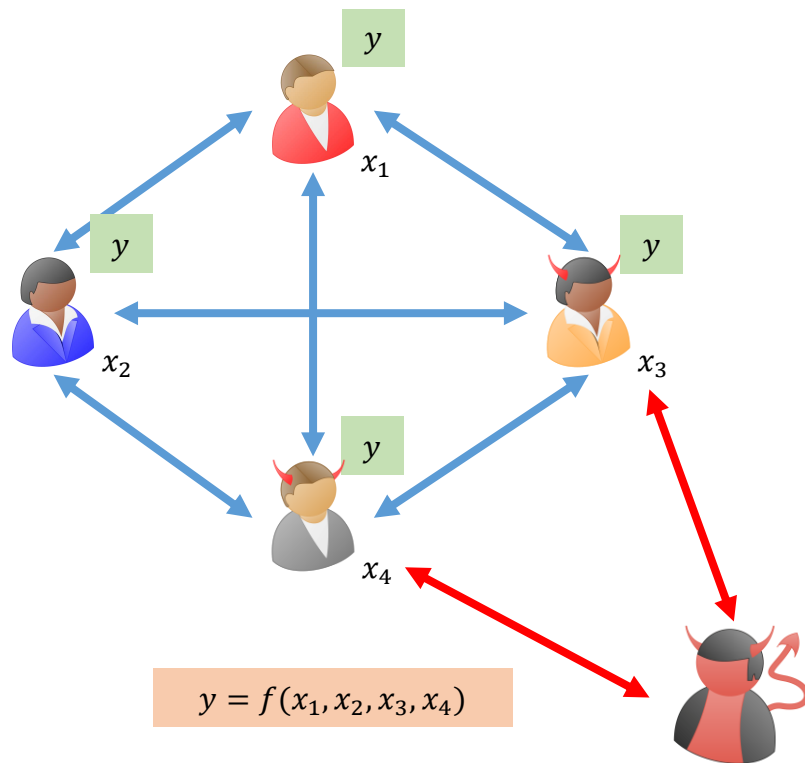
$$y = f(x_1, x_2, x_3, x_4)$$

ideal world

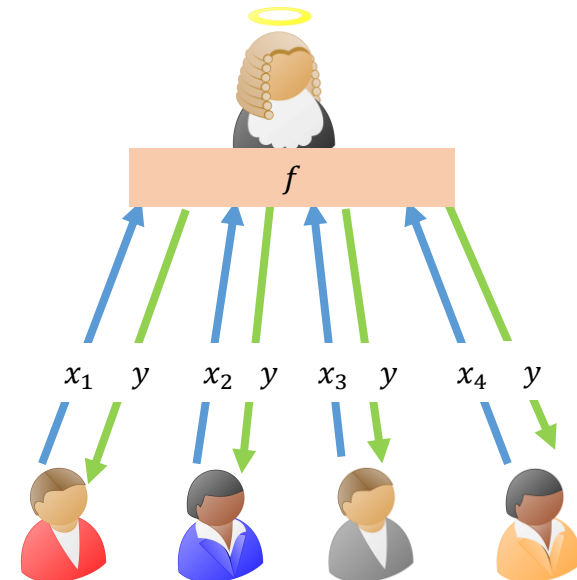


# Security

real world

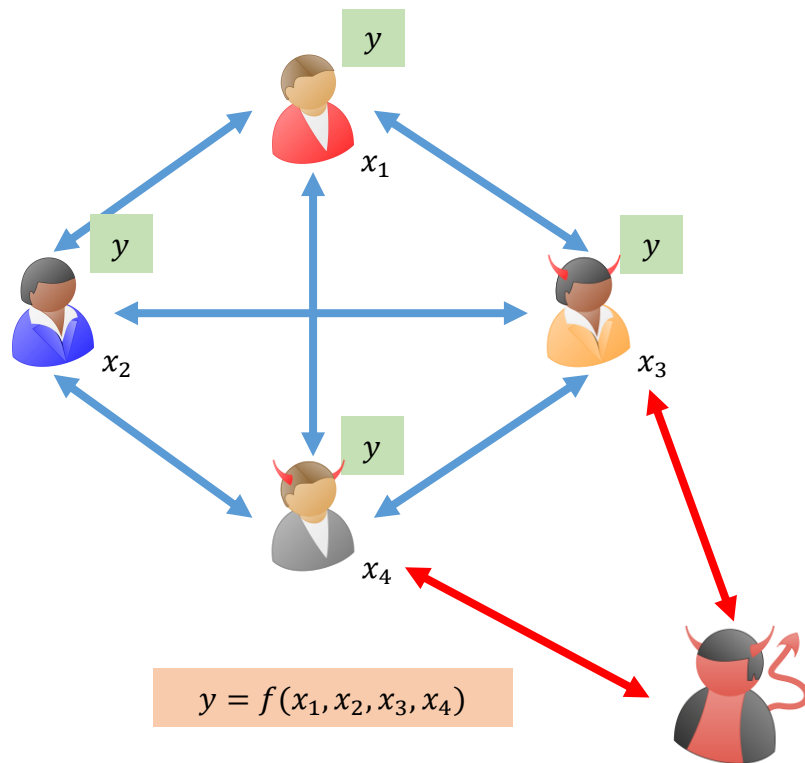


ideal world

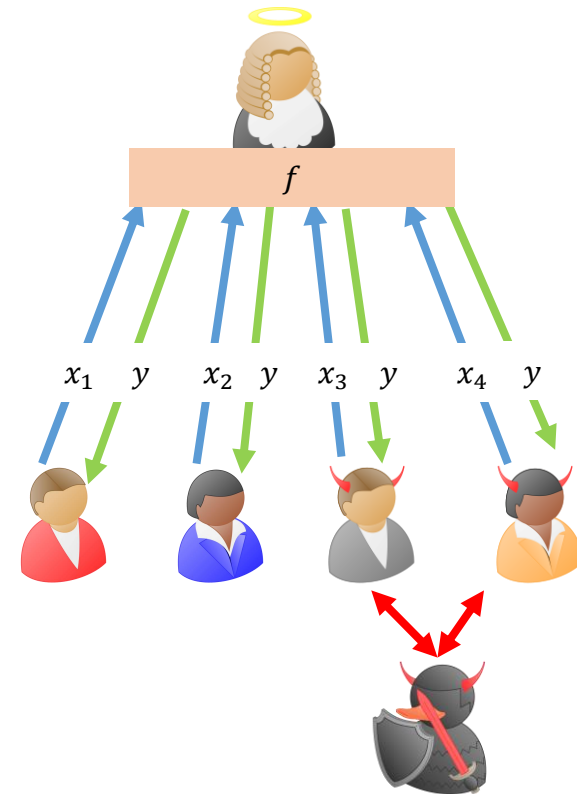


# Security

real world



ideal world



Can we construct **round optimal** multiparty computation from  
**minimal assumptions**?

Can we construct **round optimal** multiparty computation from  
**minimal assumptions**?

**Computational** security.

Can we construct **round optimal** multiparty computation from **minimal assumptions**?

**Computational** security.

**Malicious adversaries** with **dishonest majority**.

Can we construct **round optimal** multiparty computation from **minimal assumptions**?

**Computational** security.

**Malicious adversaries** with **dishonest majority**.

**Black-box** simulation.



Can we construct **round optimal** multiparty computation from **minimal assumptions**?

**Computational** security.

**Malicious adversaries** with **dishonest majority**.

**Black-box** simulation.

No **trusted setup**.

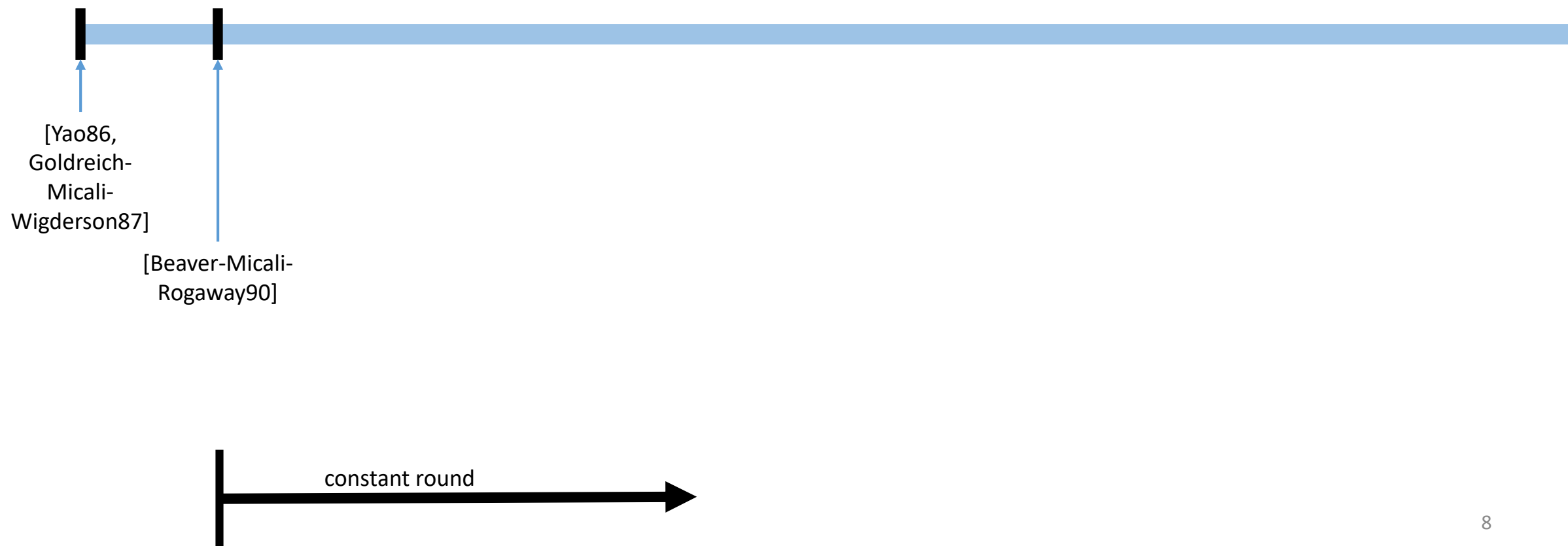
# Timeline



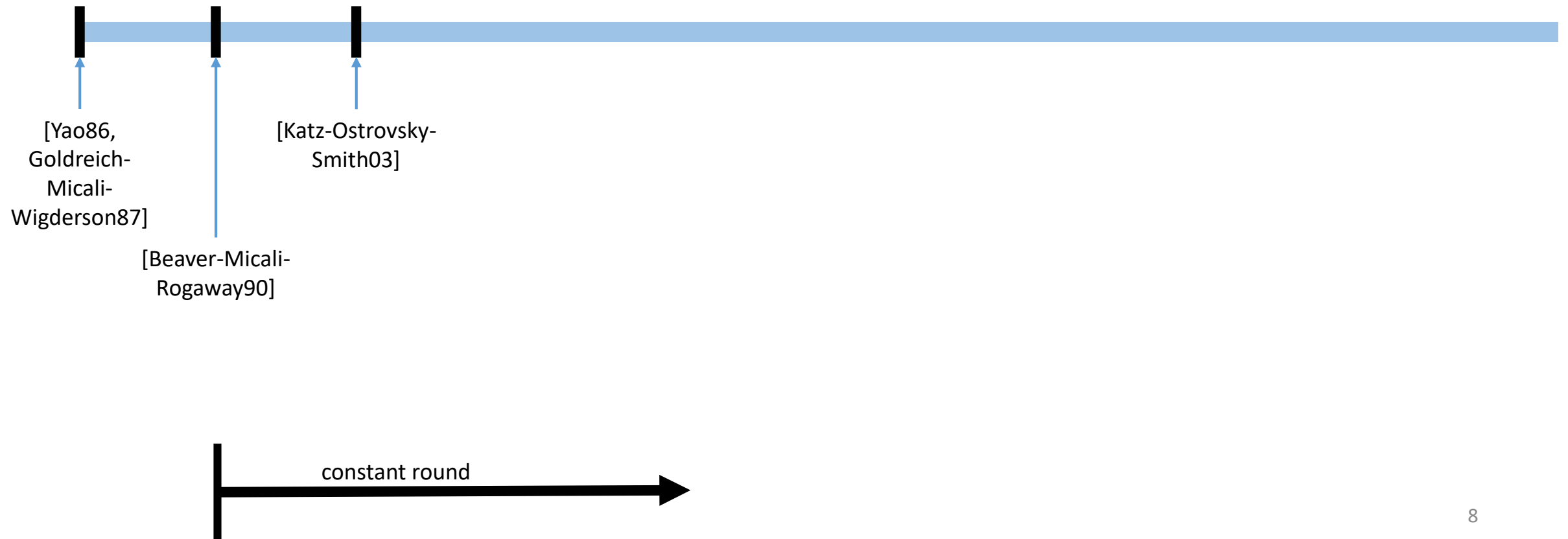
# Timeline



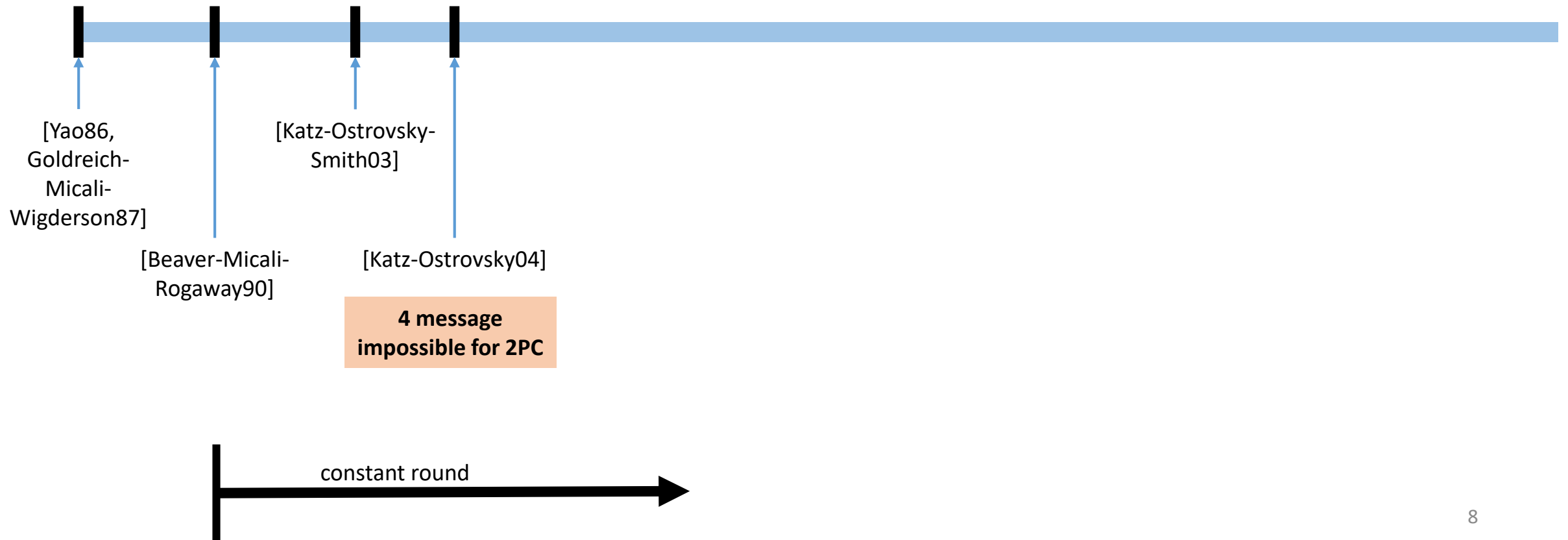
# Timeline



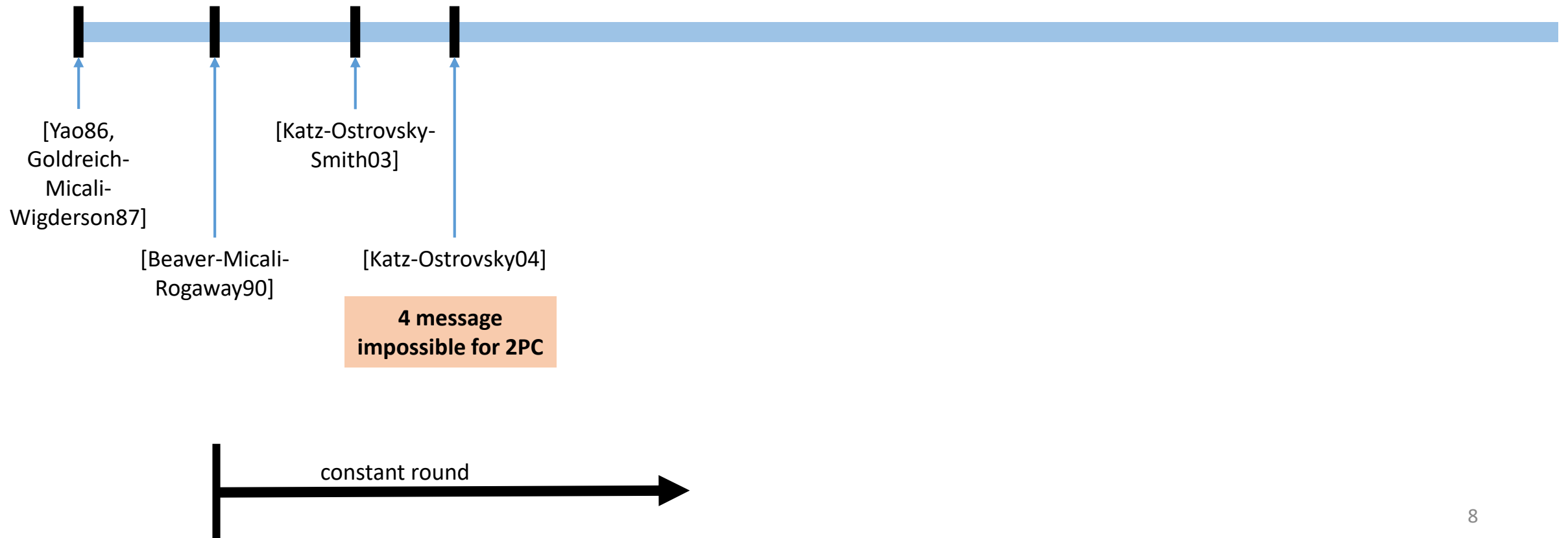
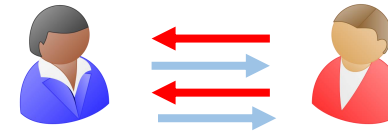
# Timeline



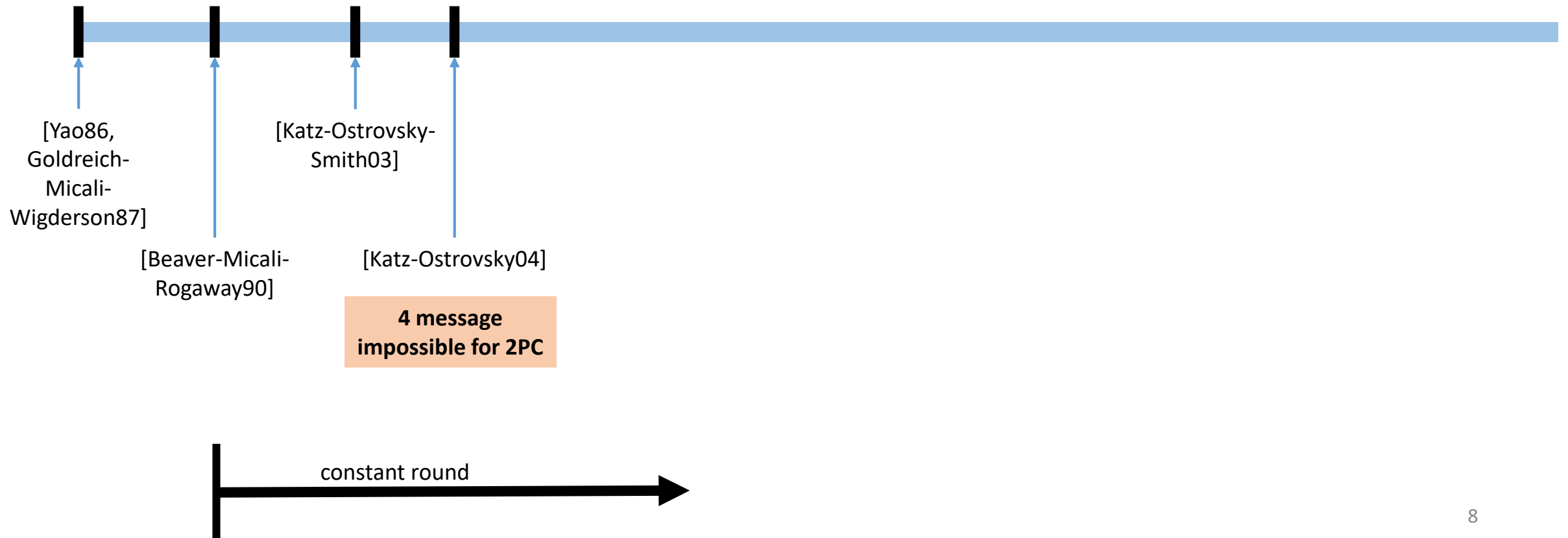
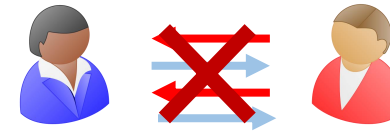
# Timeline



# Timeline

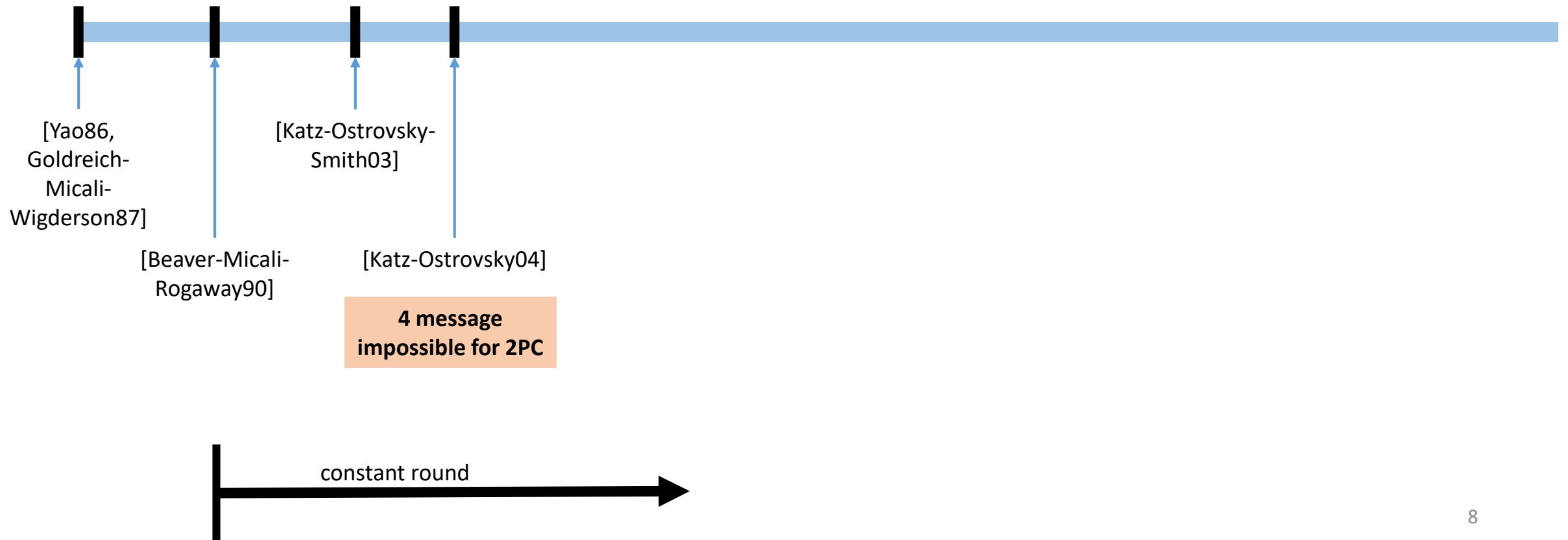


# Timeline

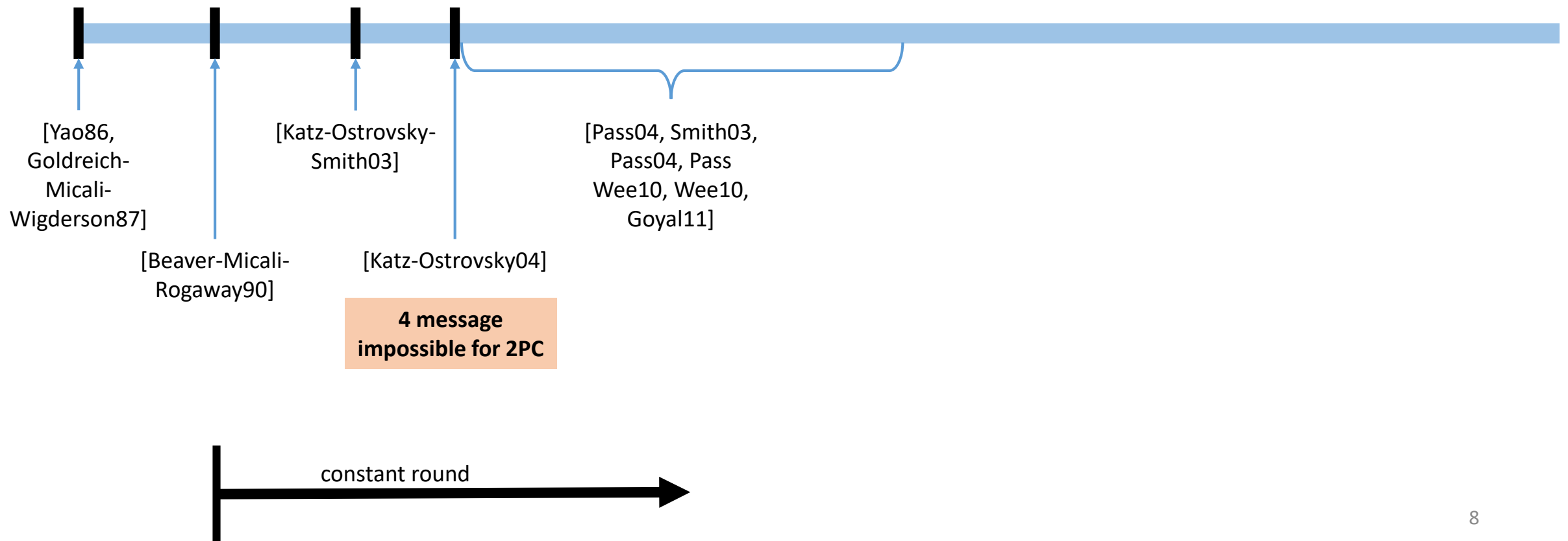




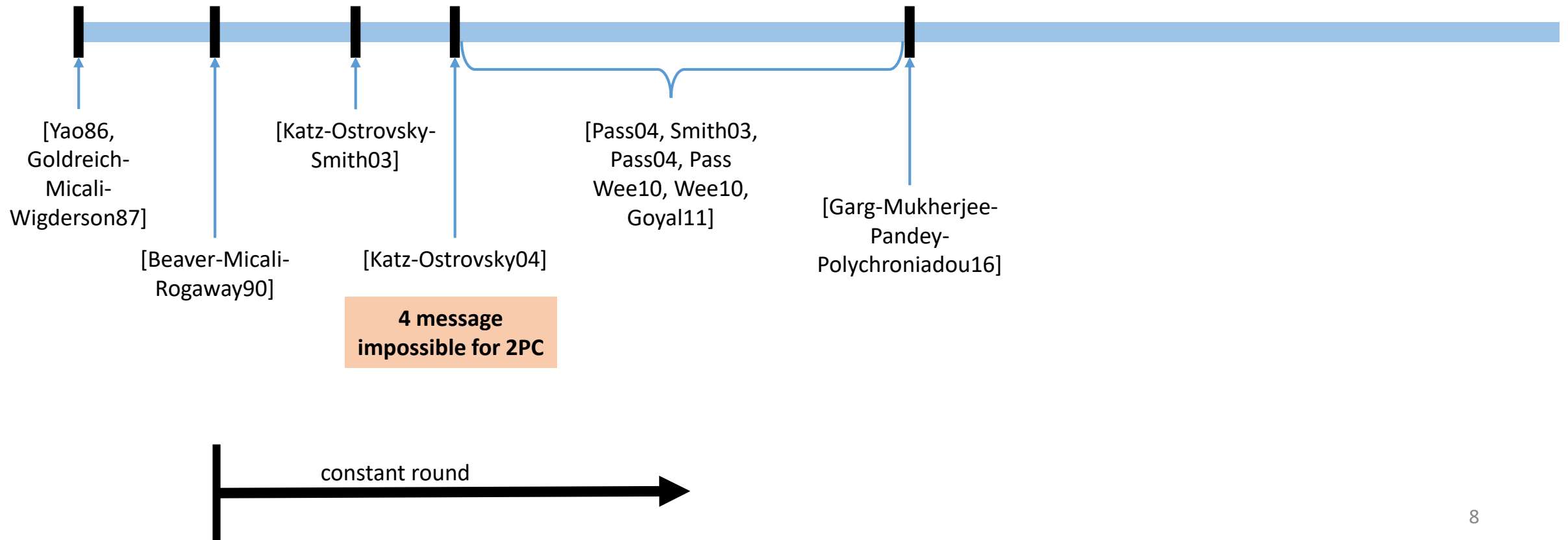
# Timeline



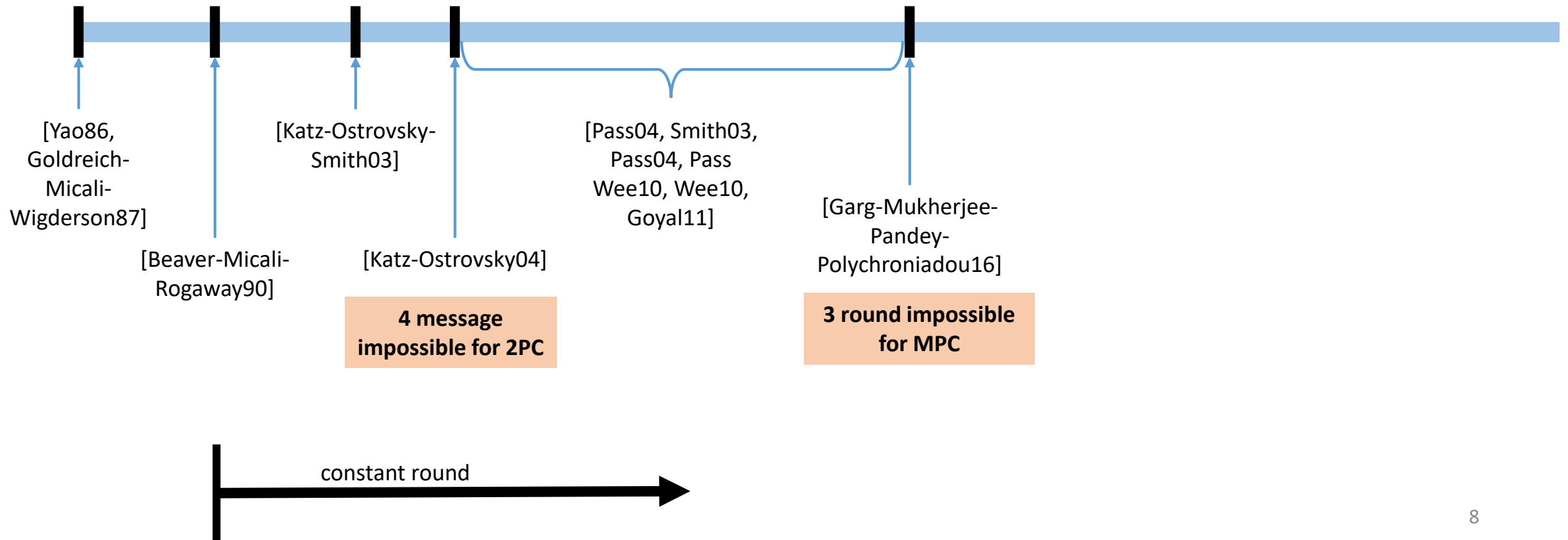
# Timeline



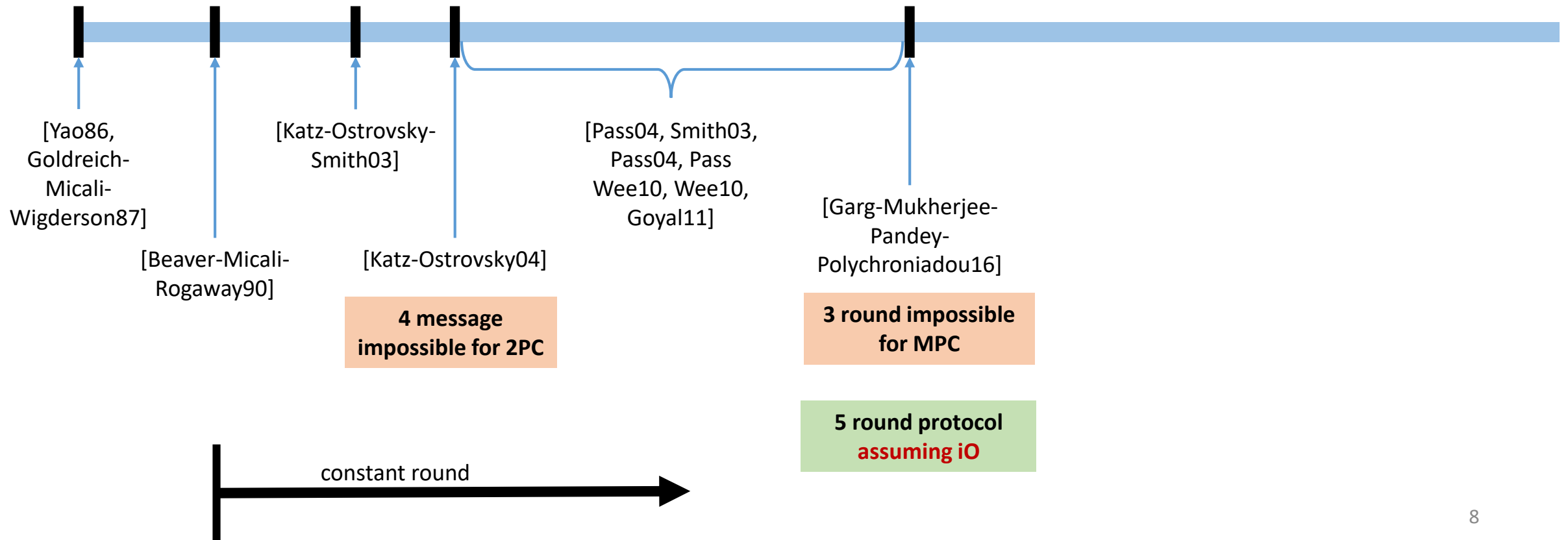
# Timeline



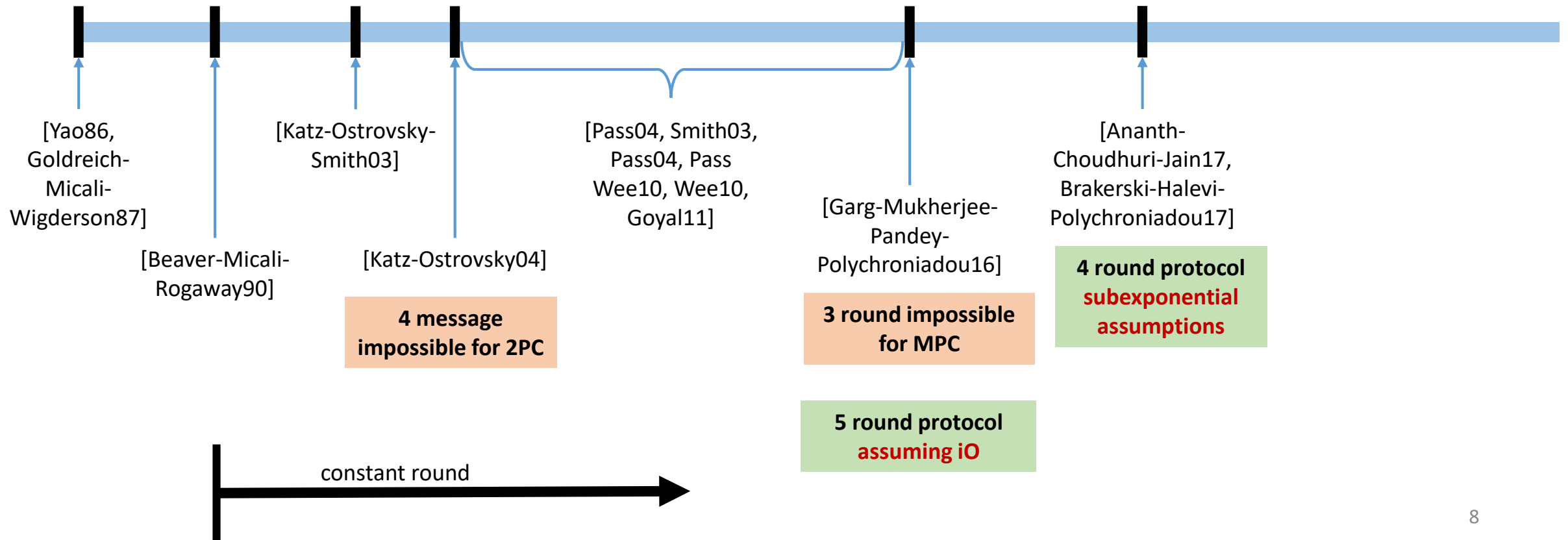
# Timeline



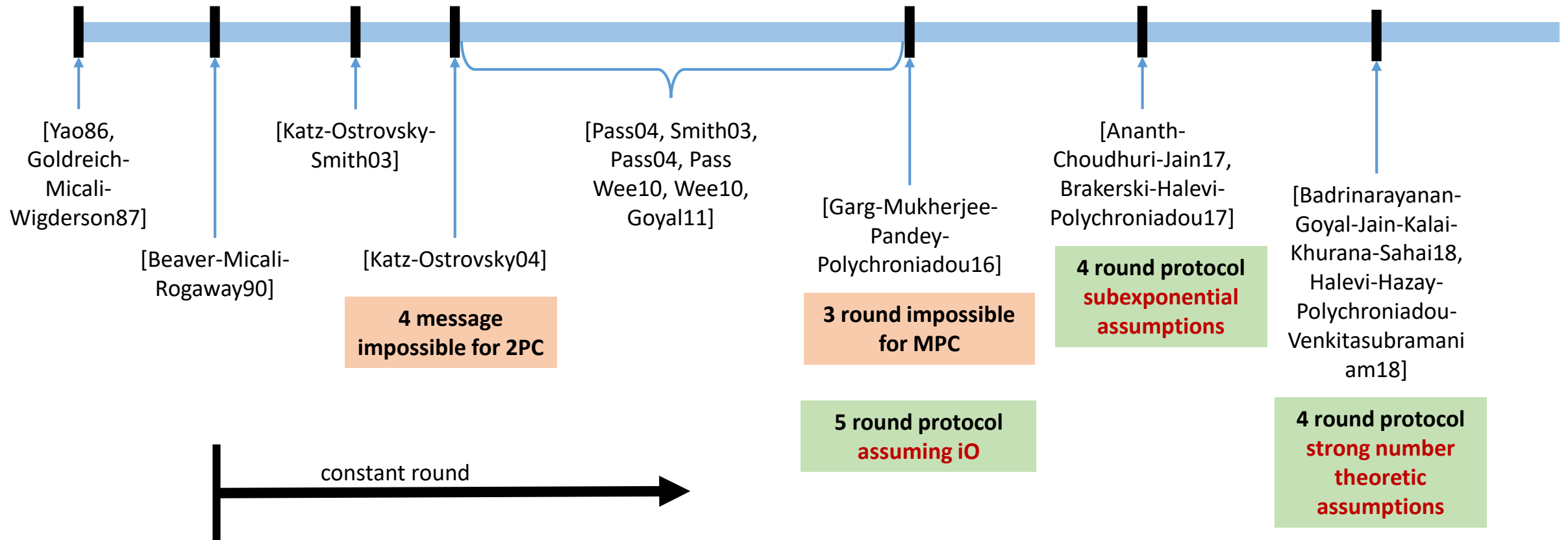
# Timeline



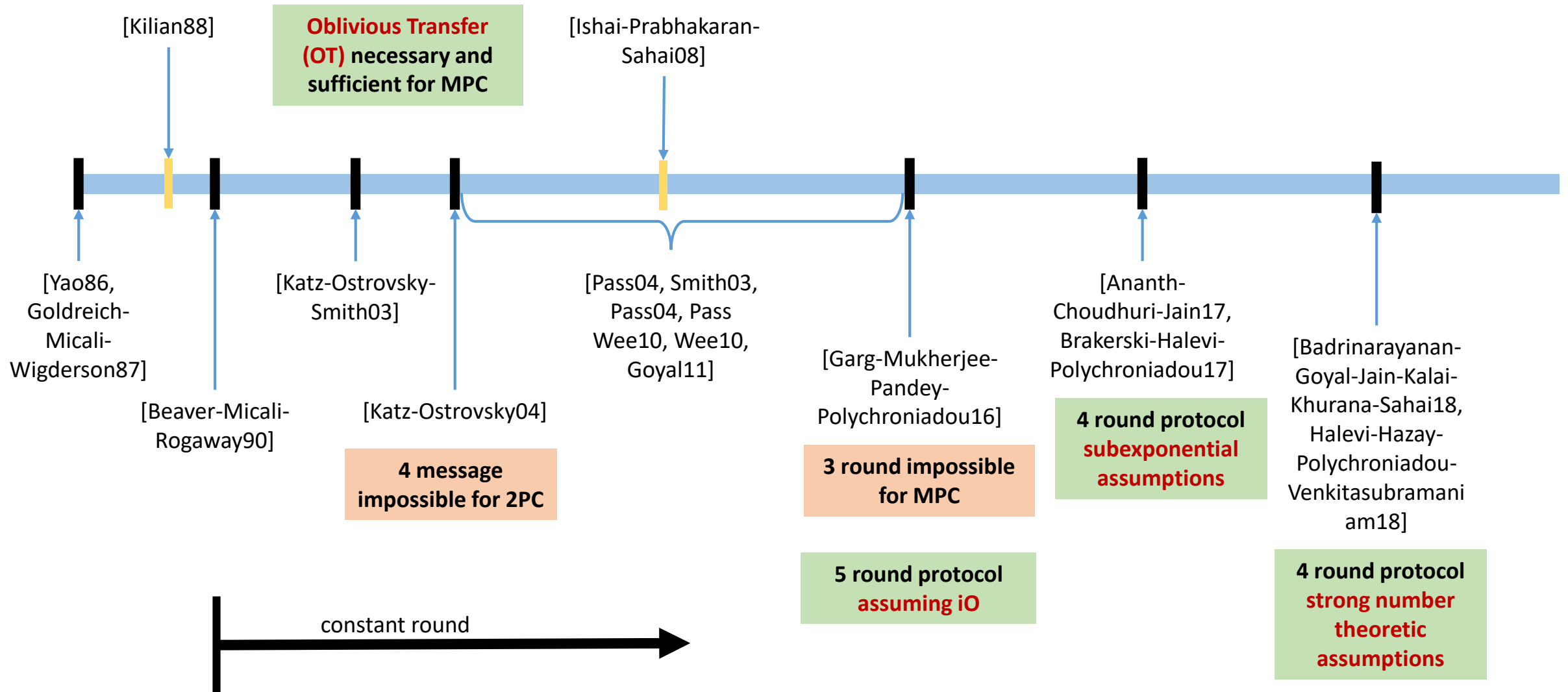
# Timeline



# Timeline

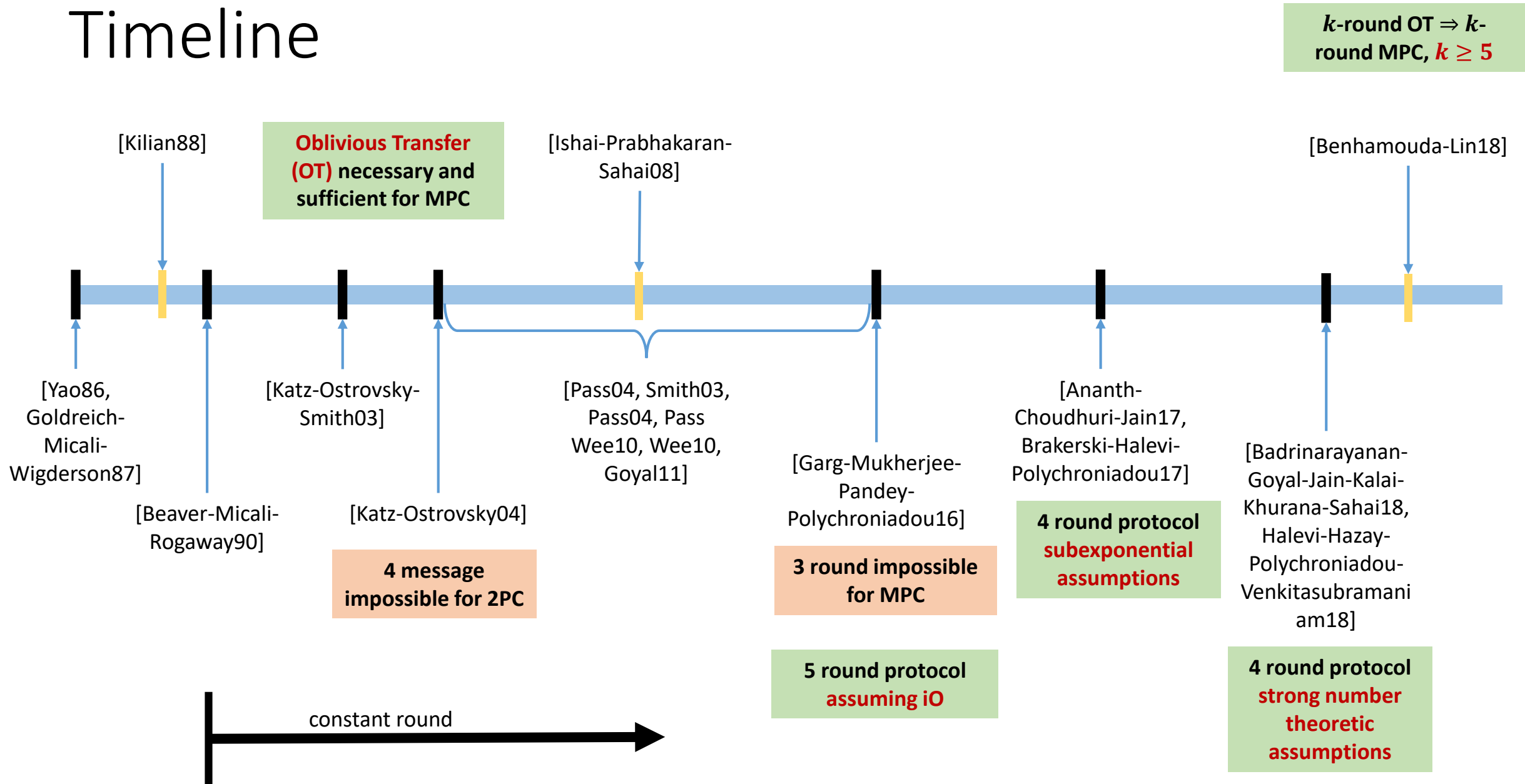


# Timeline





# Timeline



# Our results

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

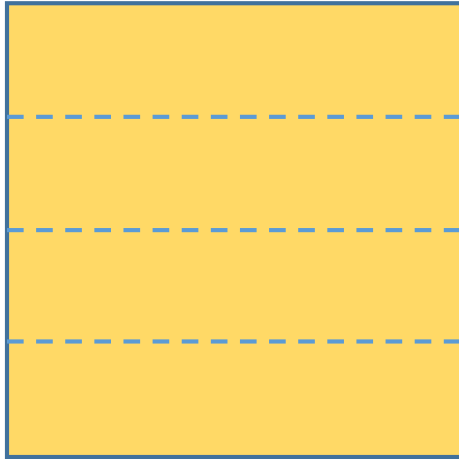
# Our results

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

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

# Challenge: Enforcing Honest Behavior

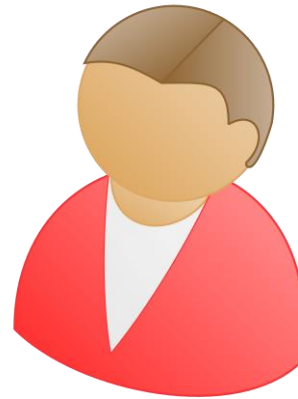
# Challenge: Enforcing Honest Behavior



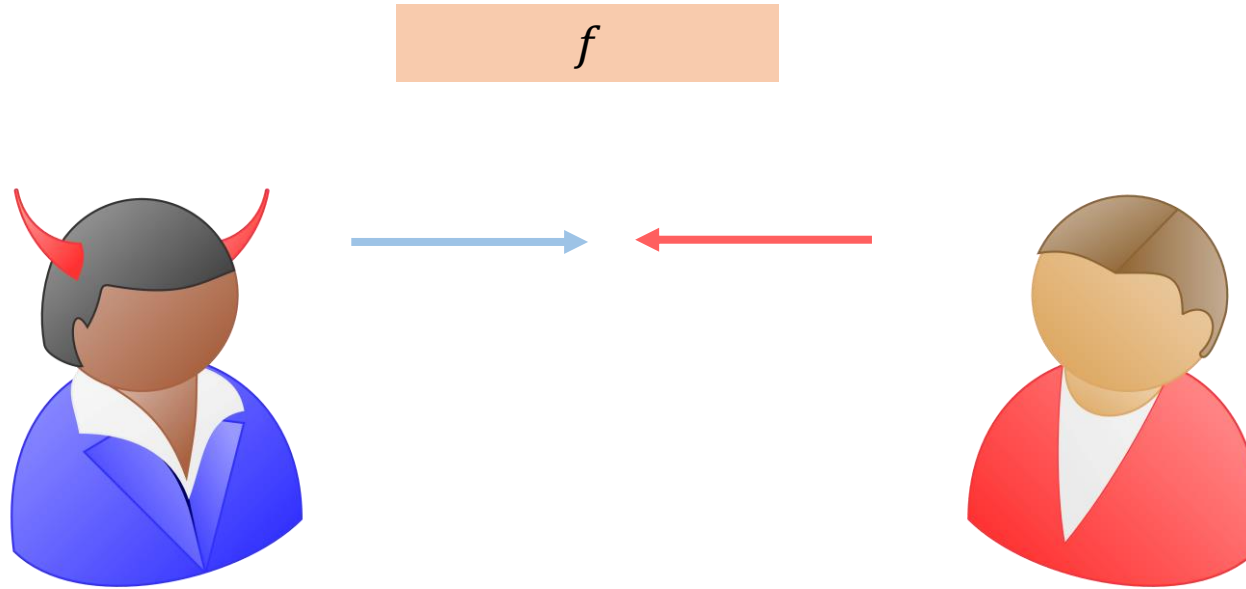
Any four round protocol.

# Challenge: Enforcing Honest Behavior

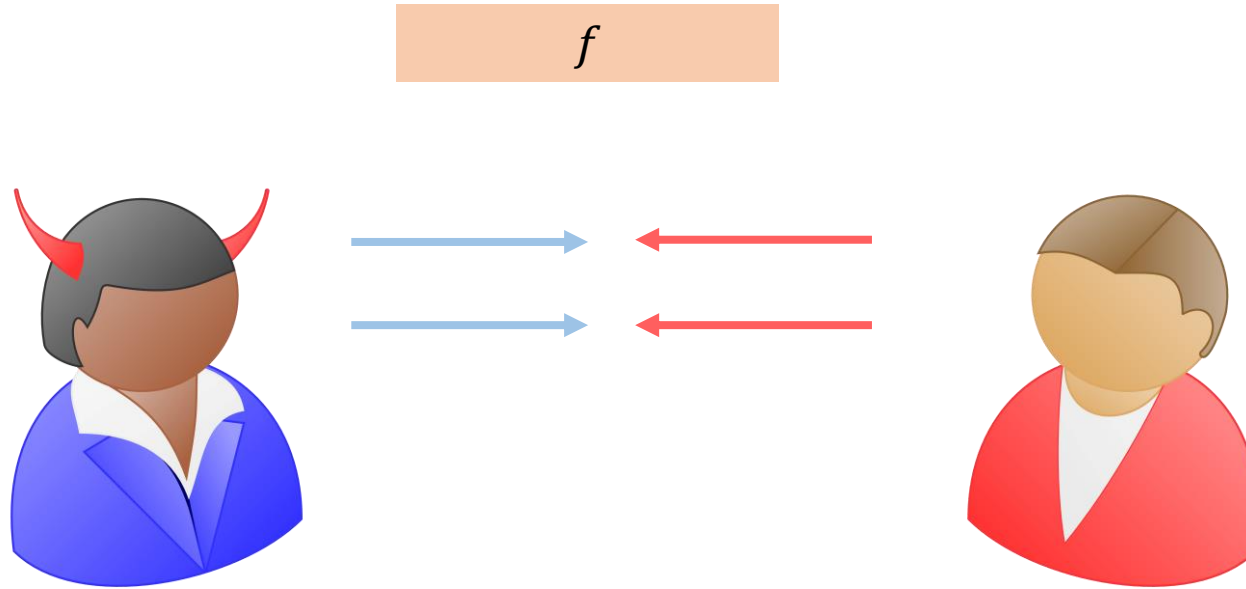
$f$



# Challenge: Enforcing Honest Behavior

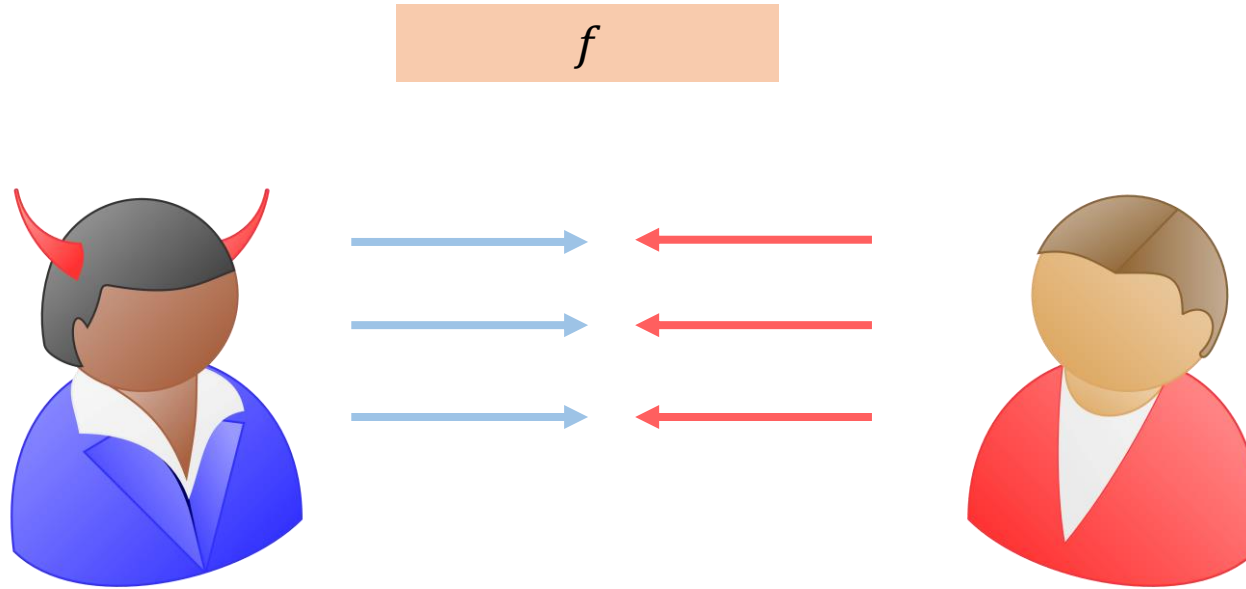


# Challenge: Enforcing Honest Behavior

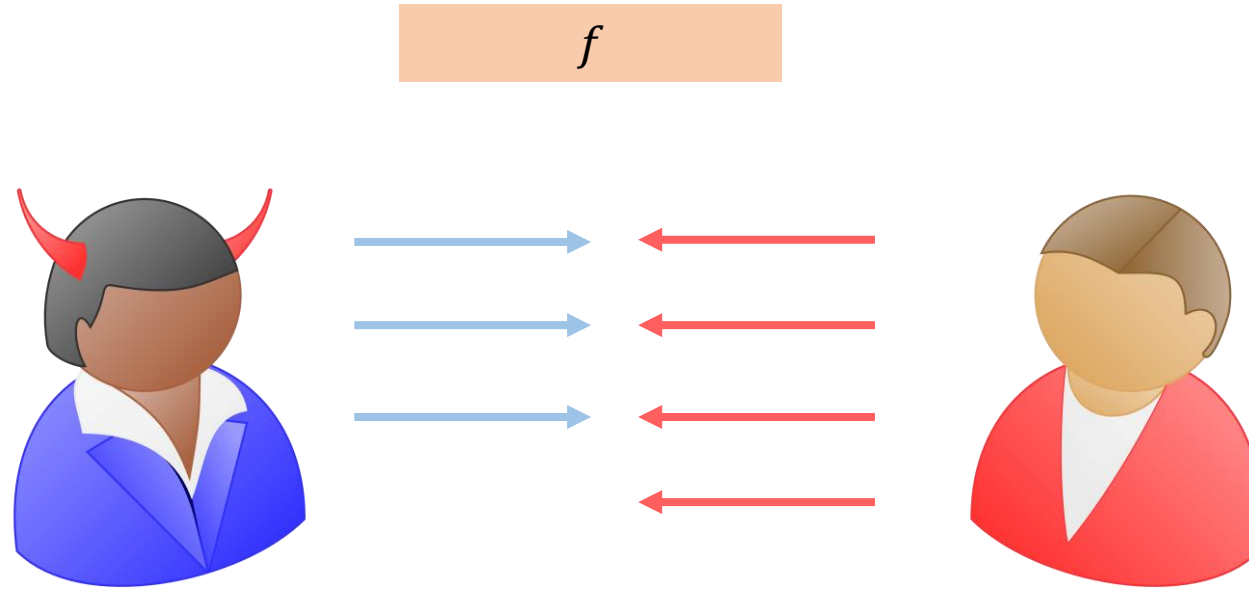




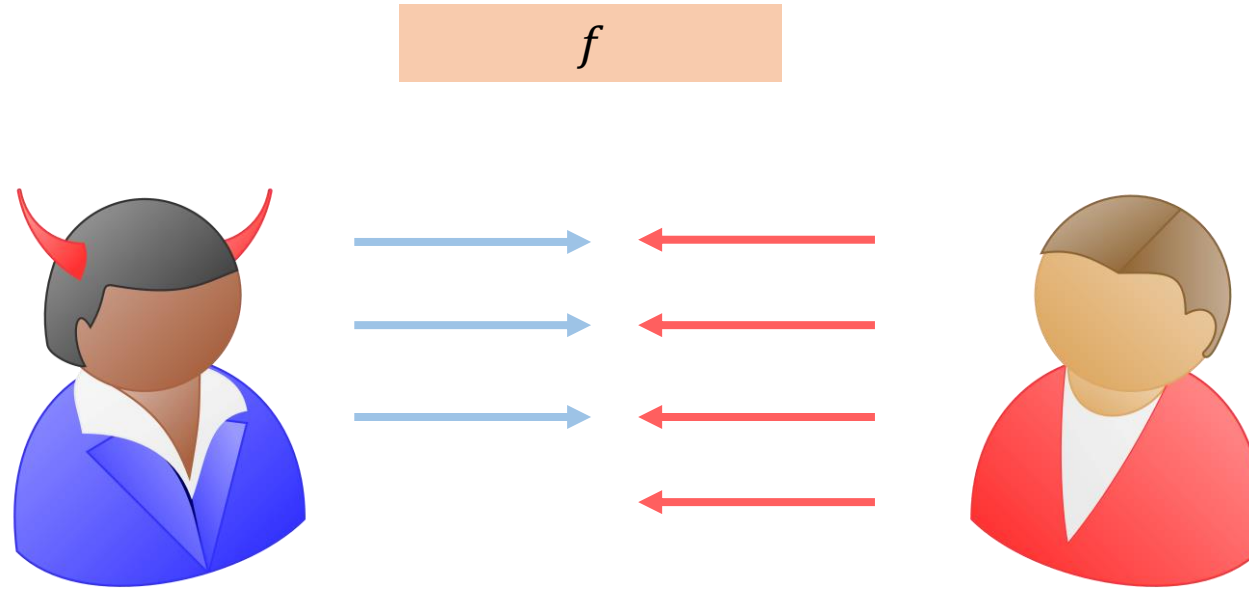
# Challenge: Enforcing Honest Behavior



# Challenge: Enforcing Honest Behavior

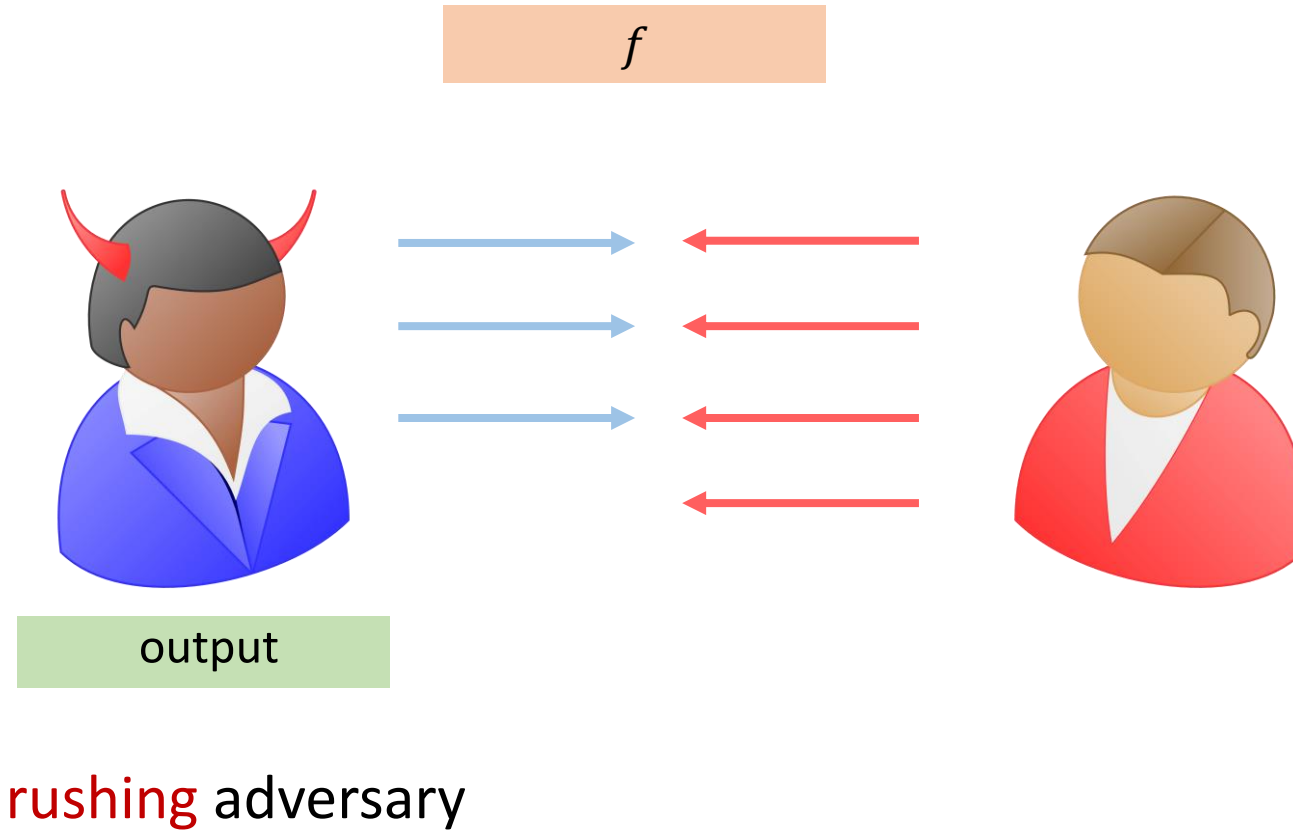


# Challenge: Enforcing Honest Behavior

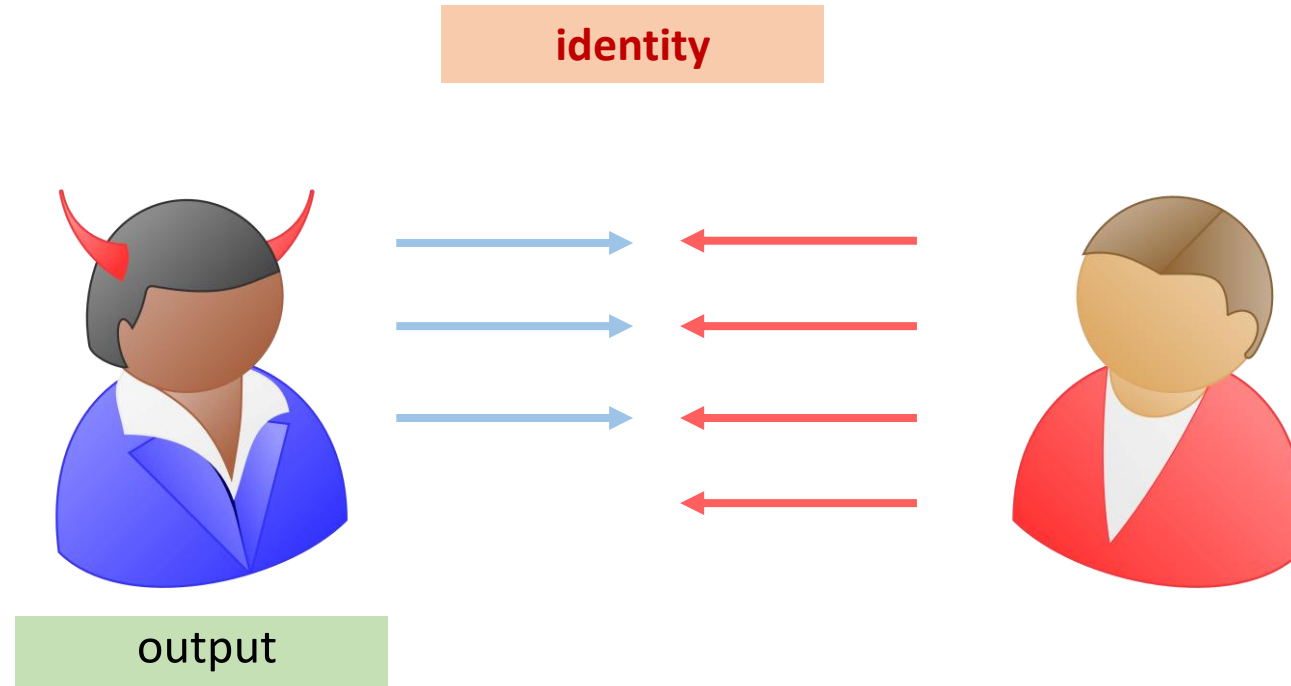


**rushing** adversary

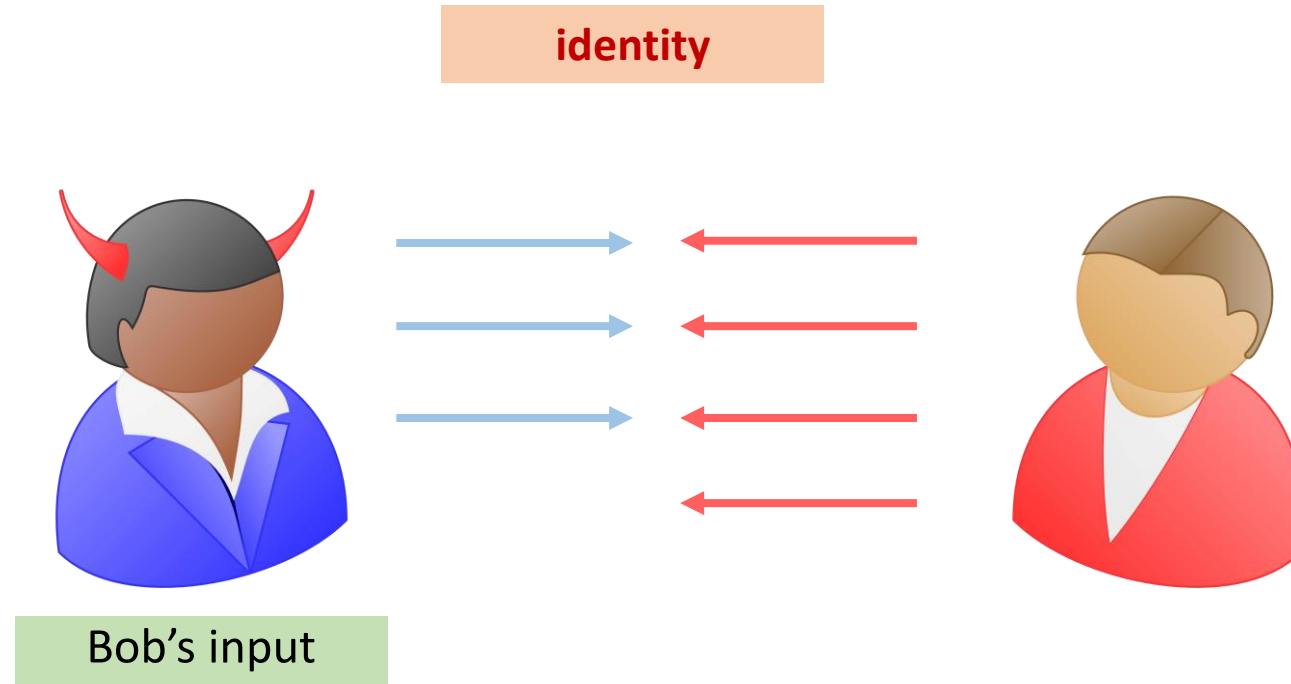
# Challenge: Enforcing Honest Behavior



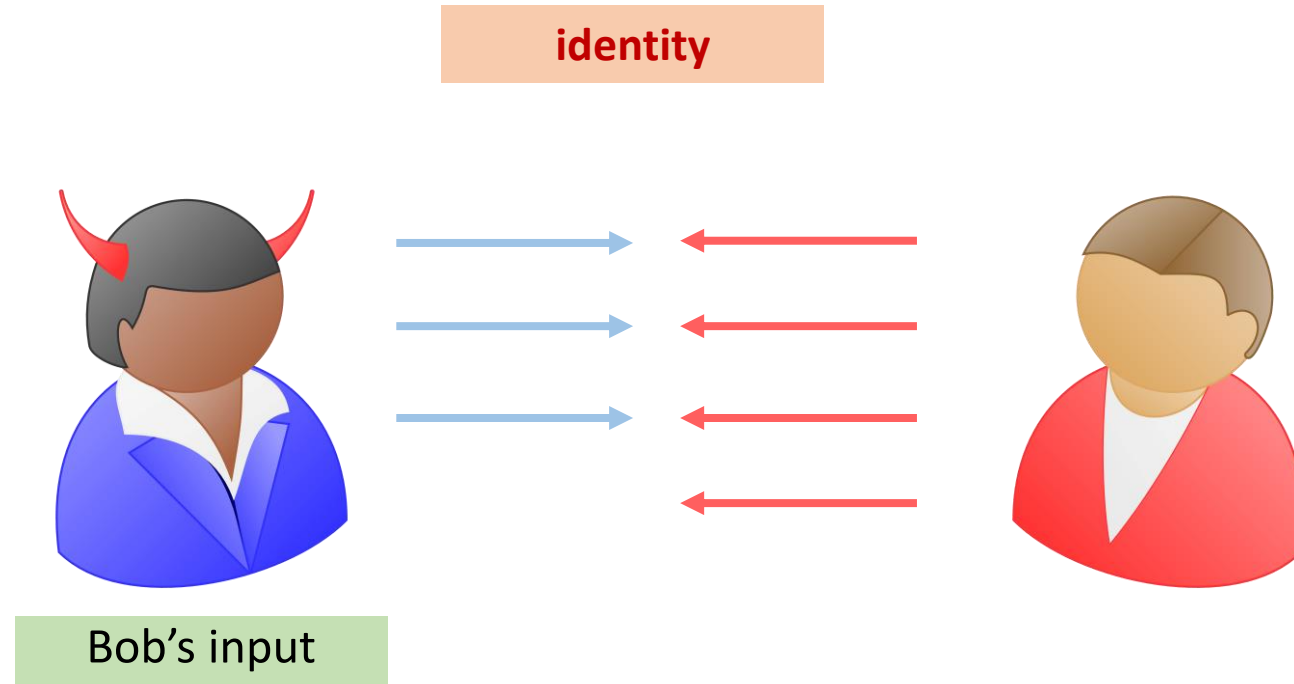
# Challenge: Enforcing Honest Behavior



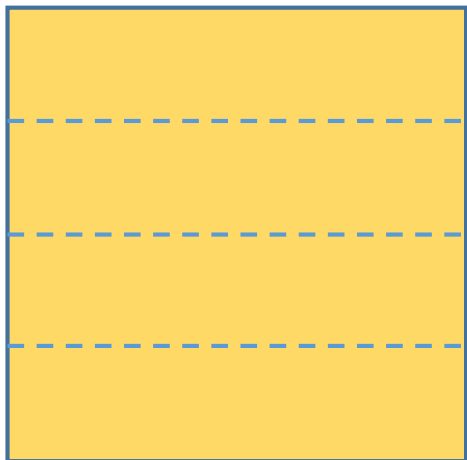
# Challenge: Enforcing Honest Behavior



# Challenge: Enforcing Honest Behavior



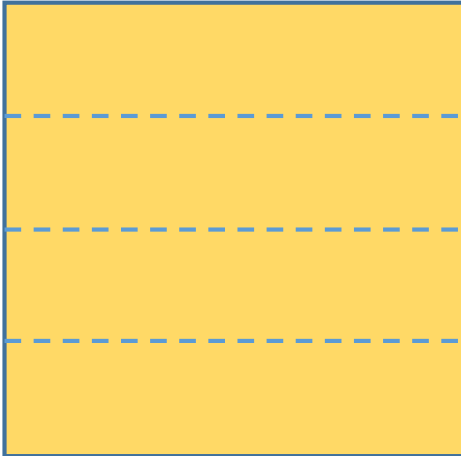
# Our strategy



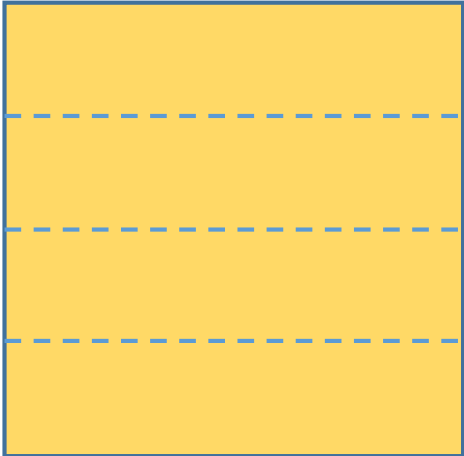


# Our strategy

delayed semi-malicious protocol

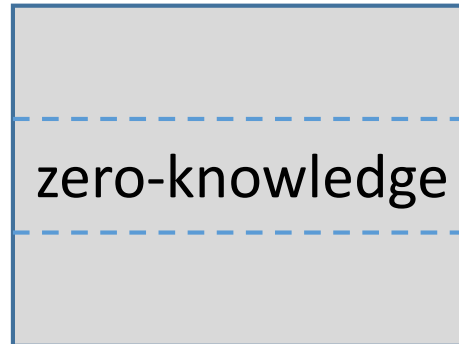
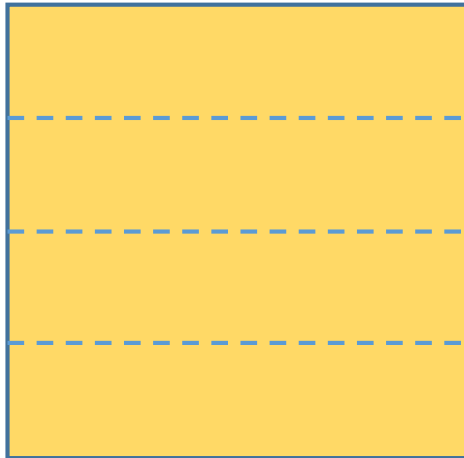


# Our strategy



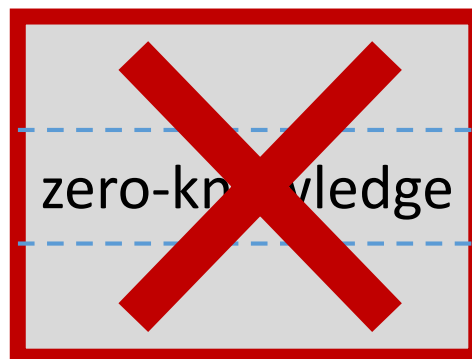
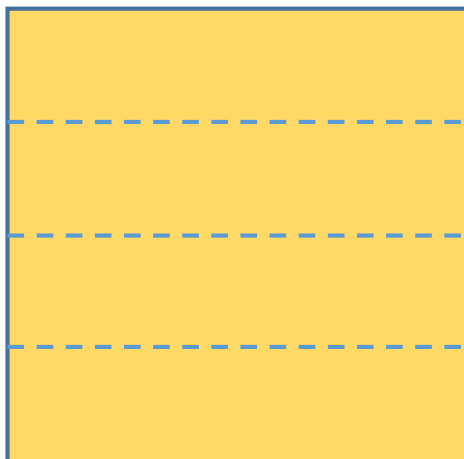
delayed semi-malicious protocol  
known from OT  
[Benhamouda-Lin18]

# Our strategy

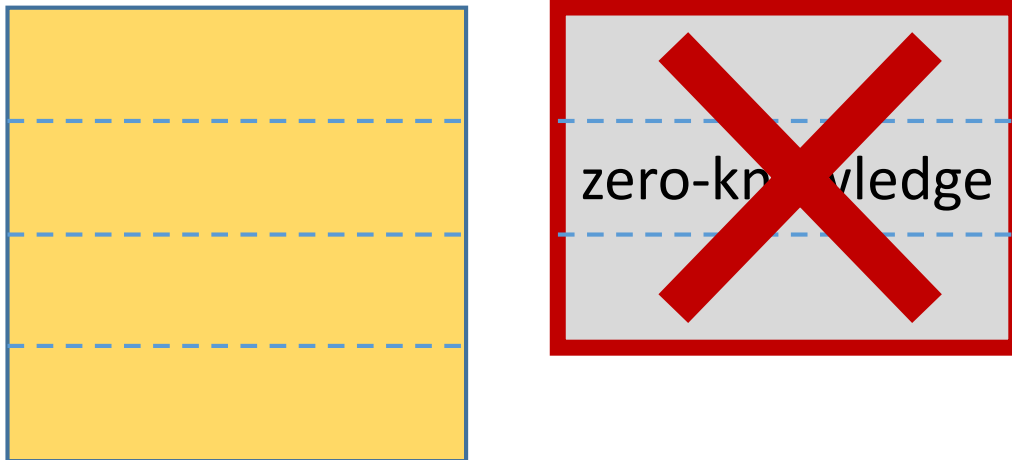


delayed semi-malicious protocol  
known from OT  
[Benhamouda-Lin18]

# Our strategy



# Our strategy



**Idea:** Use conditional disclosure of secrets and (hopefully!) 4 round zero-knowledge proofs.

# Conditional Disclosure of Secrets (CDS)

# Conditional Disclosure of Secrets (CDS)

message

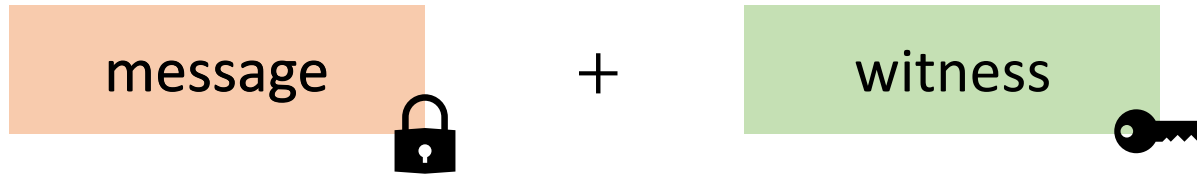
# Conditional Disclosure of Secrets (CDS)

message

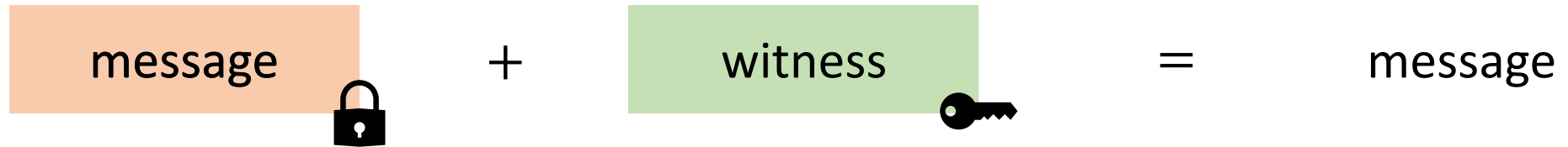




# Conditional Disclosure of Secrets (CDS)

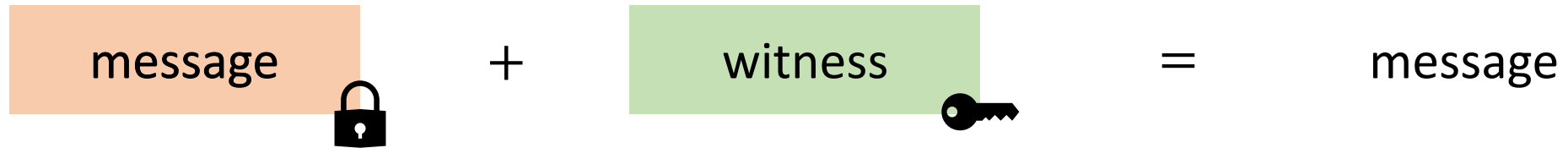


# Conditional Disclosure of Secrets (CDS)



If **witness** satisfies **condition**.

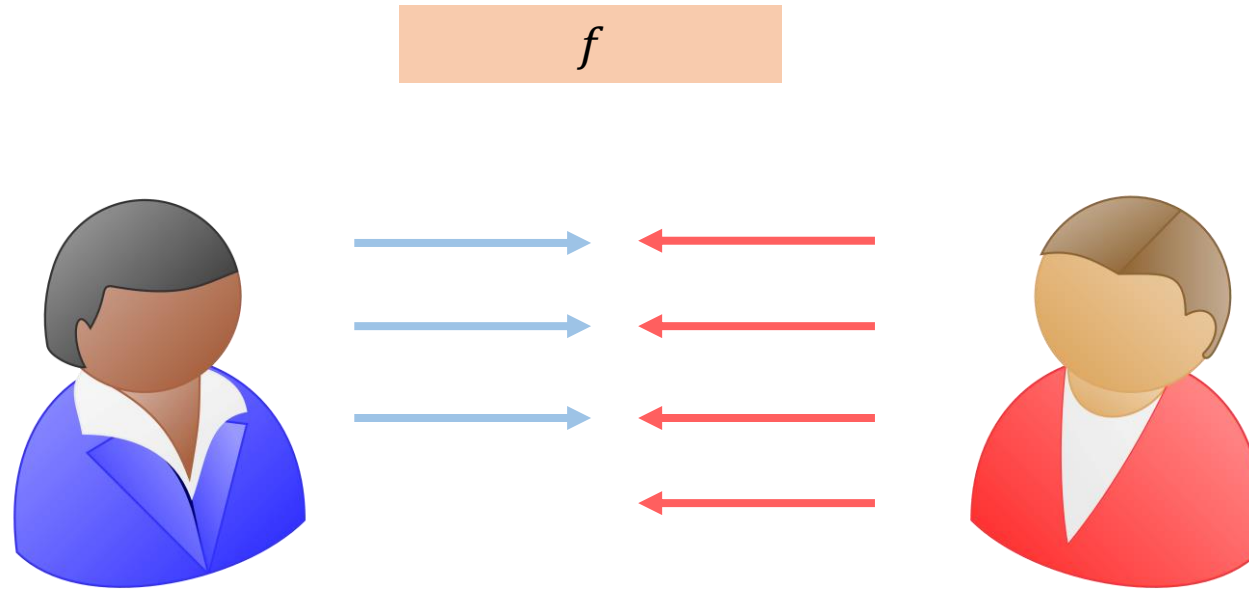
# Conditional Disclosure of Secrets (CDS)



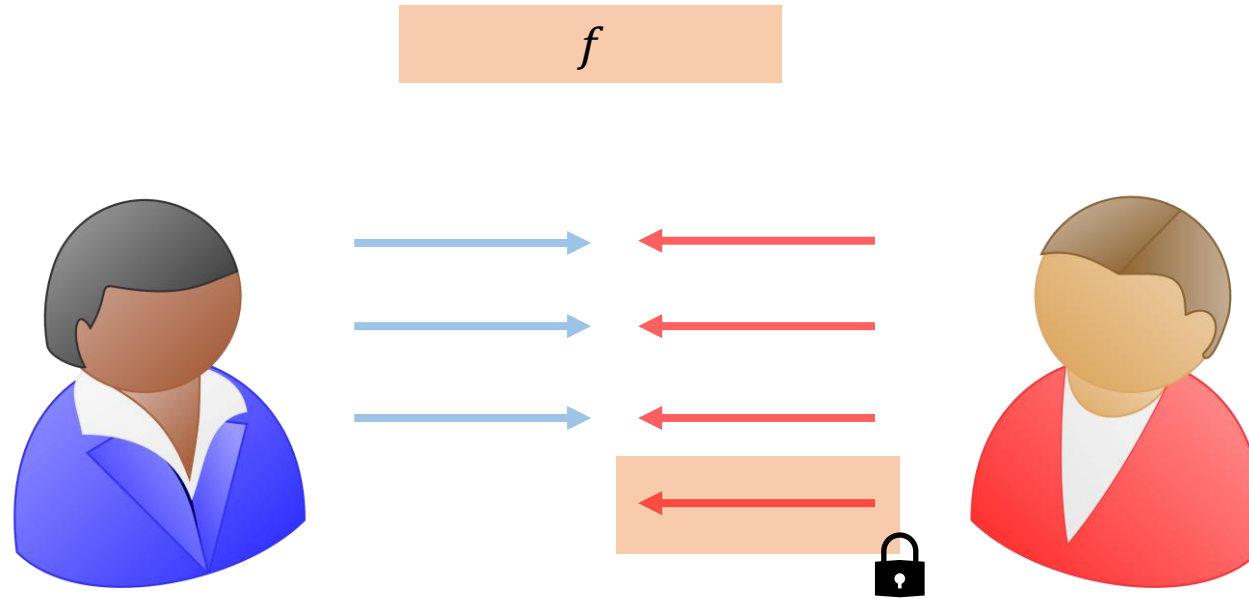
If **witness** satisfies **condition**.

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

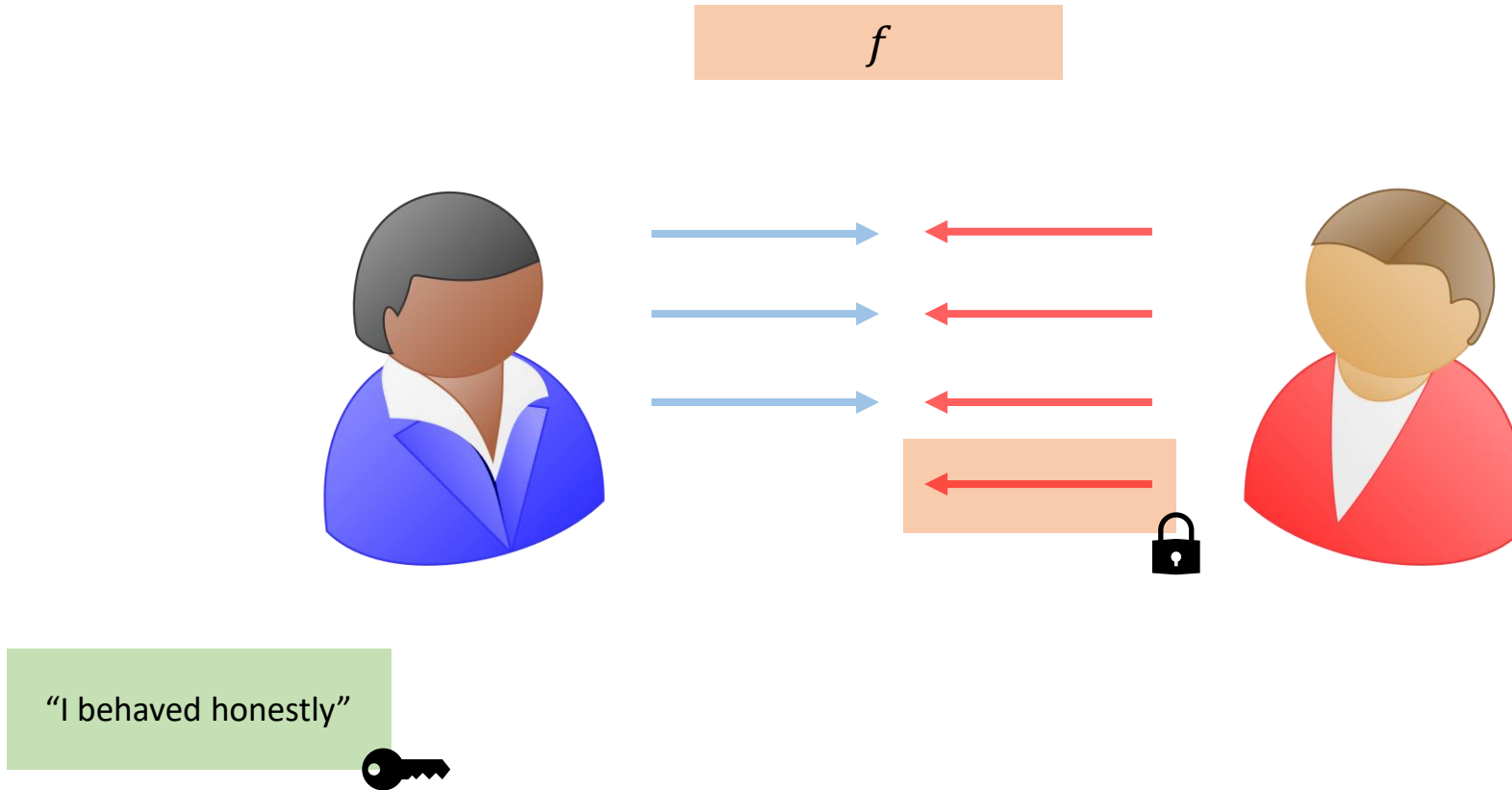
# CDS as safety net



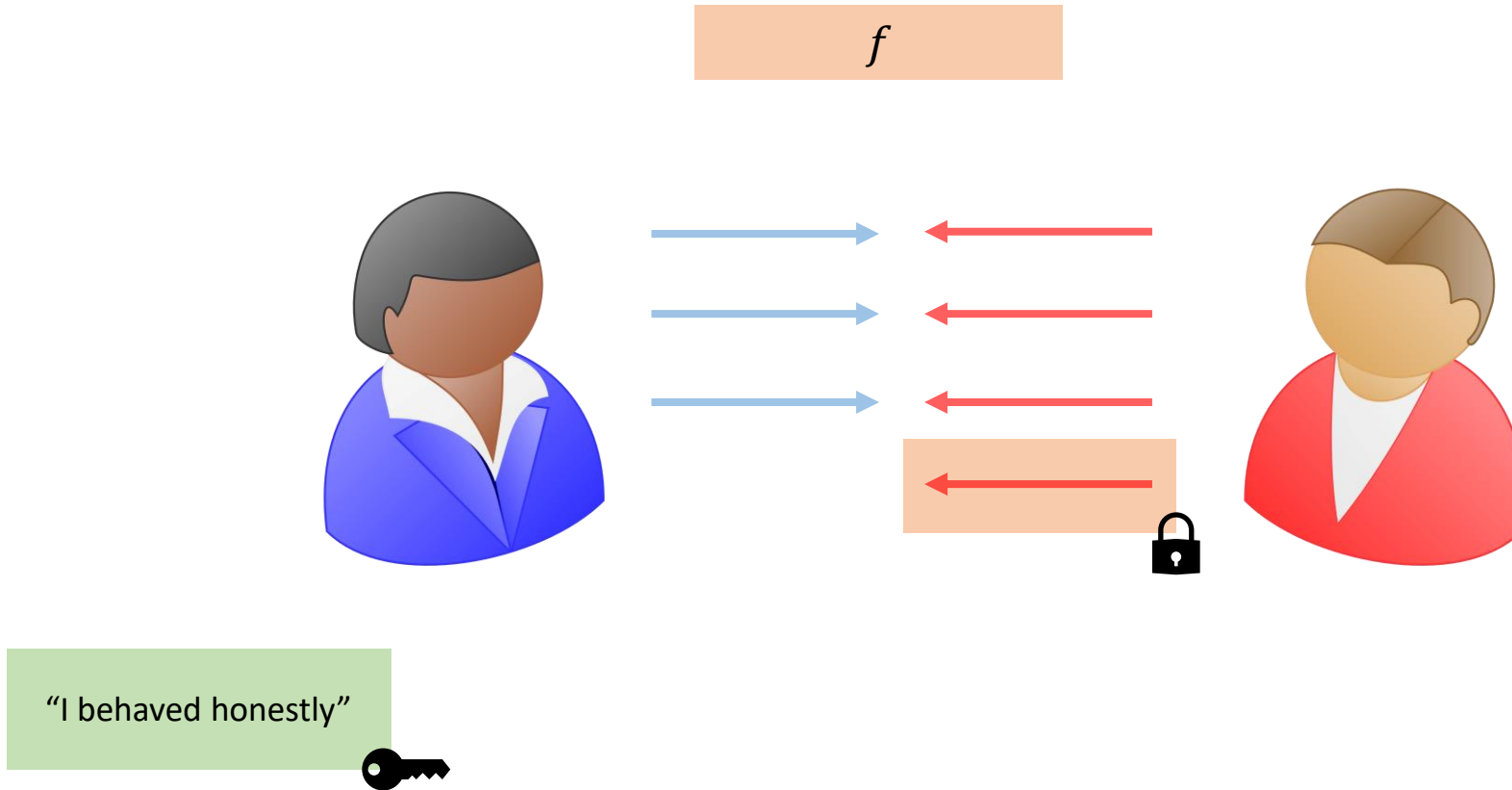
# CDS as safety net



# CDS as safety net

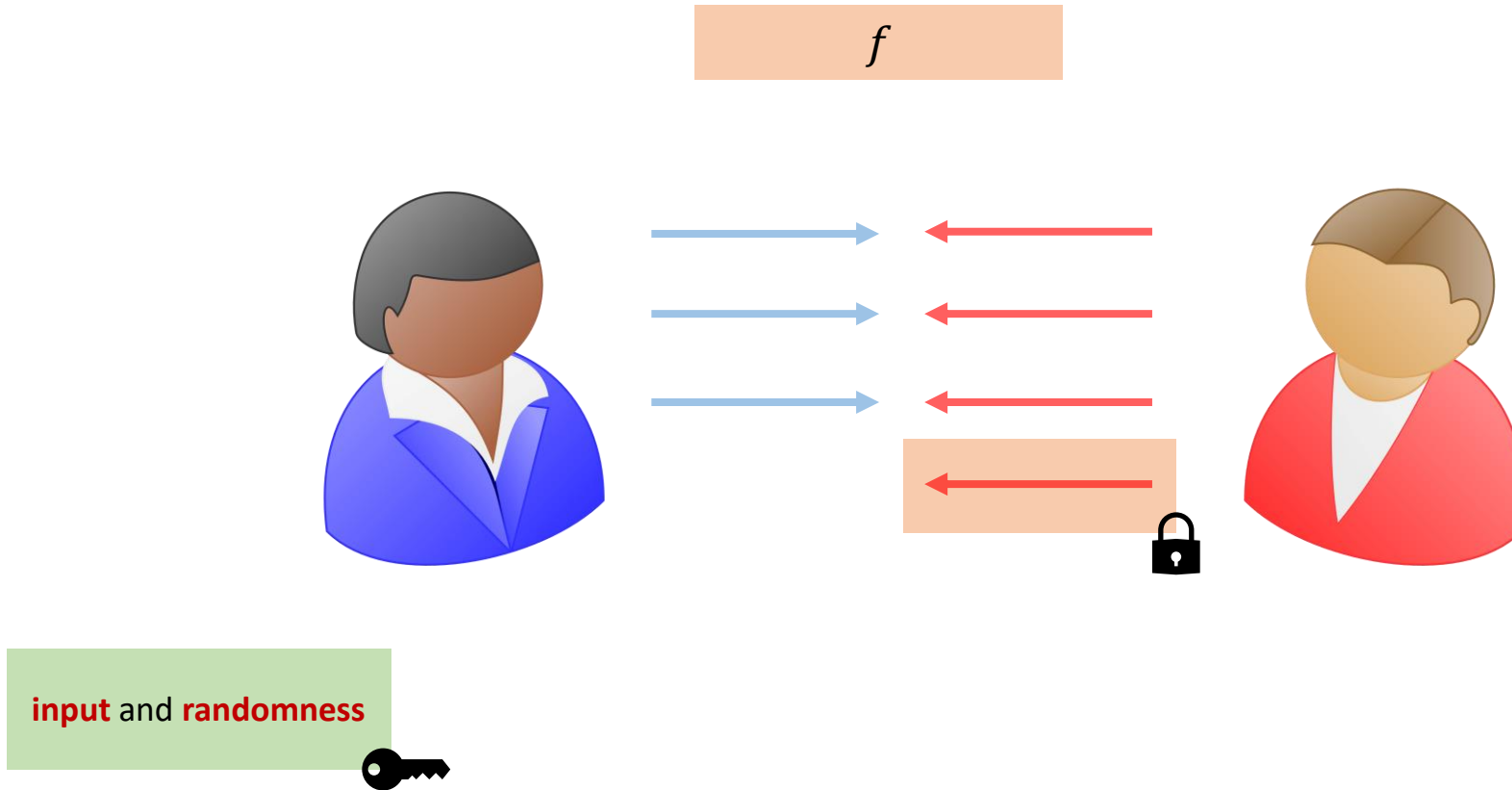


# CDS as safety net



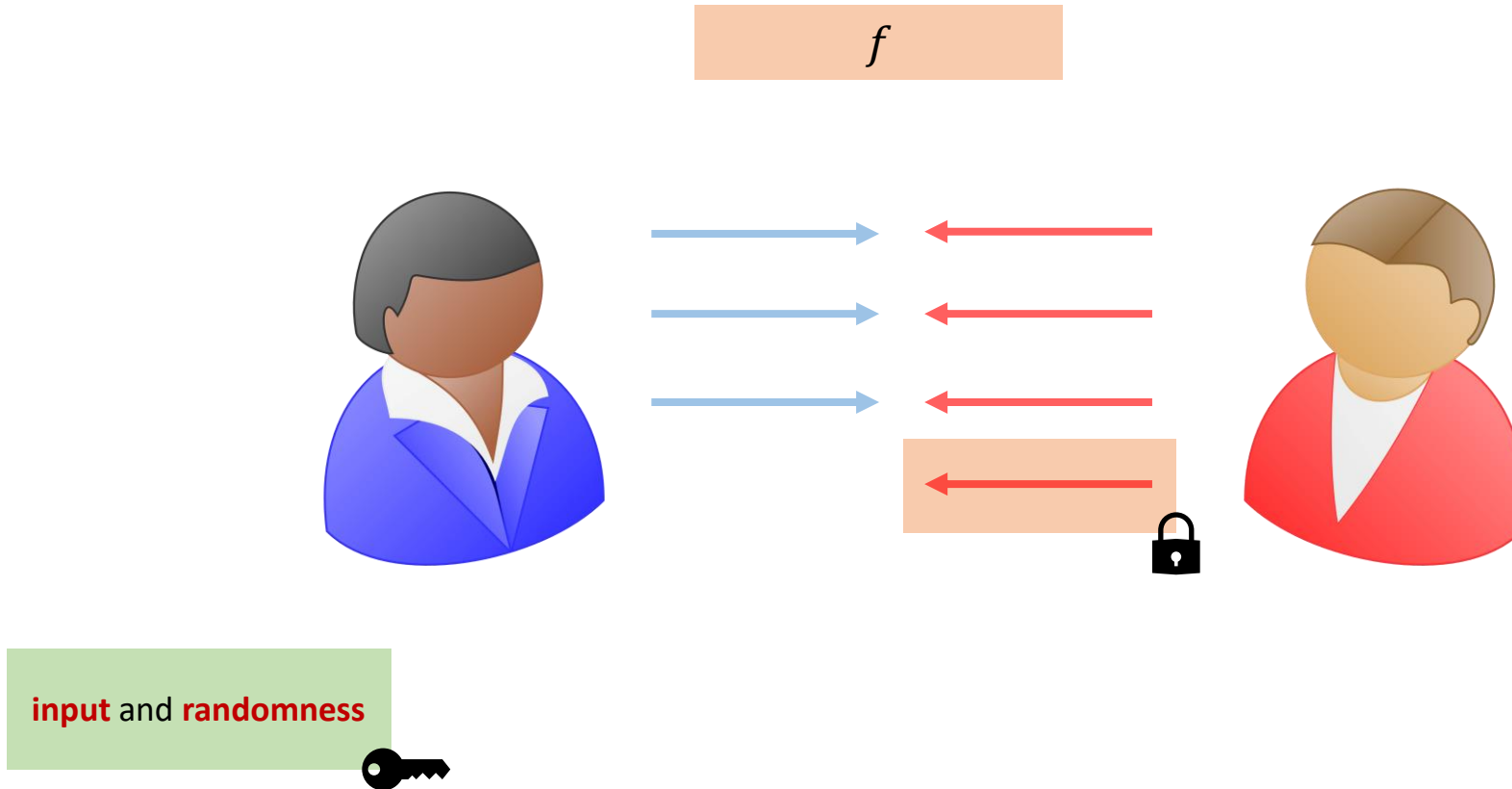
How do we **prove honest behavior**?

# CDS as safety net



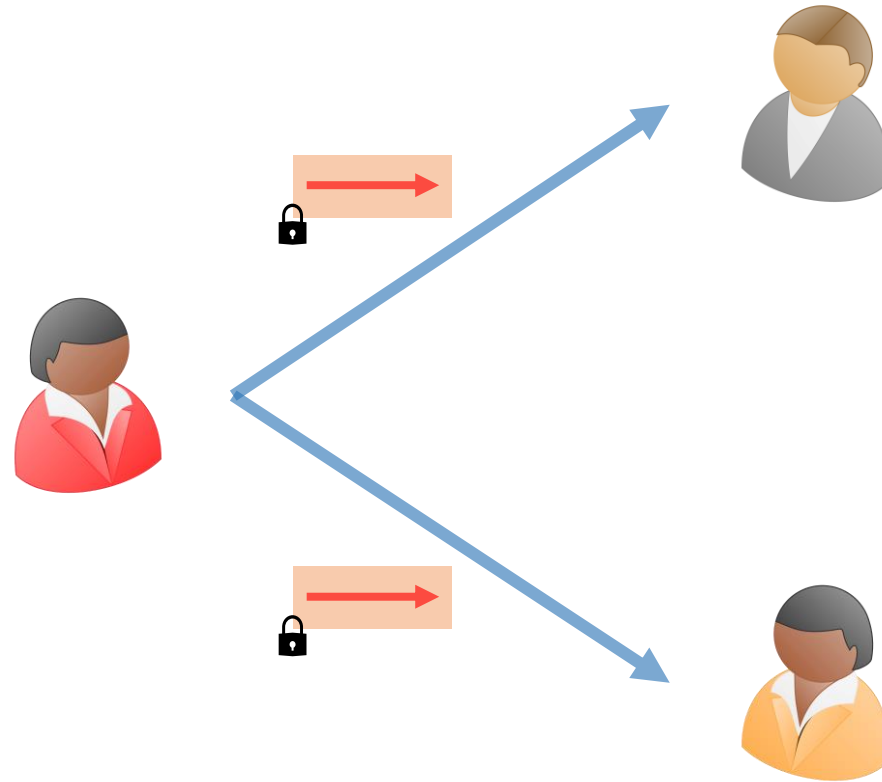


# CDS as safety net

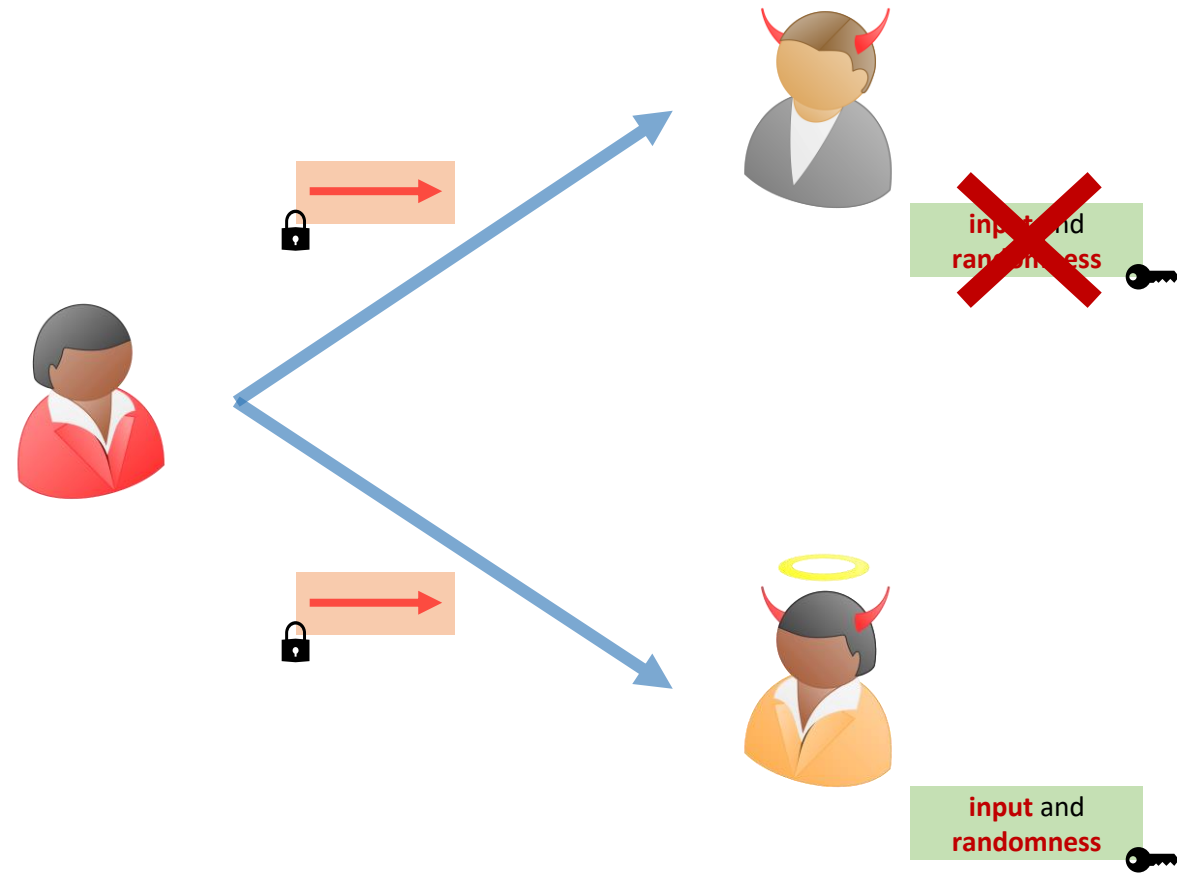


Does this work with **more than 2 parties?**

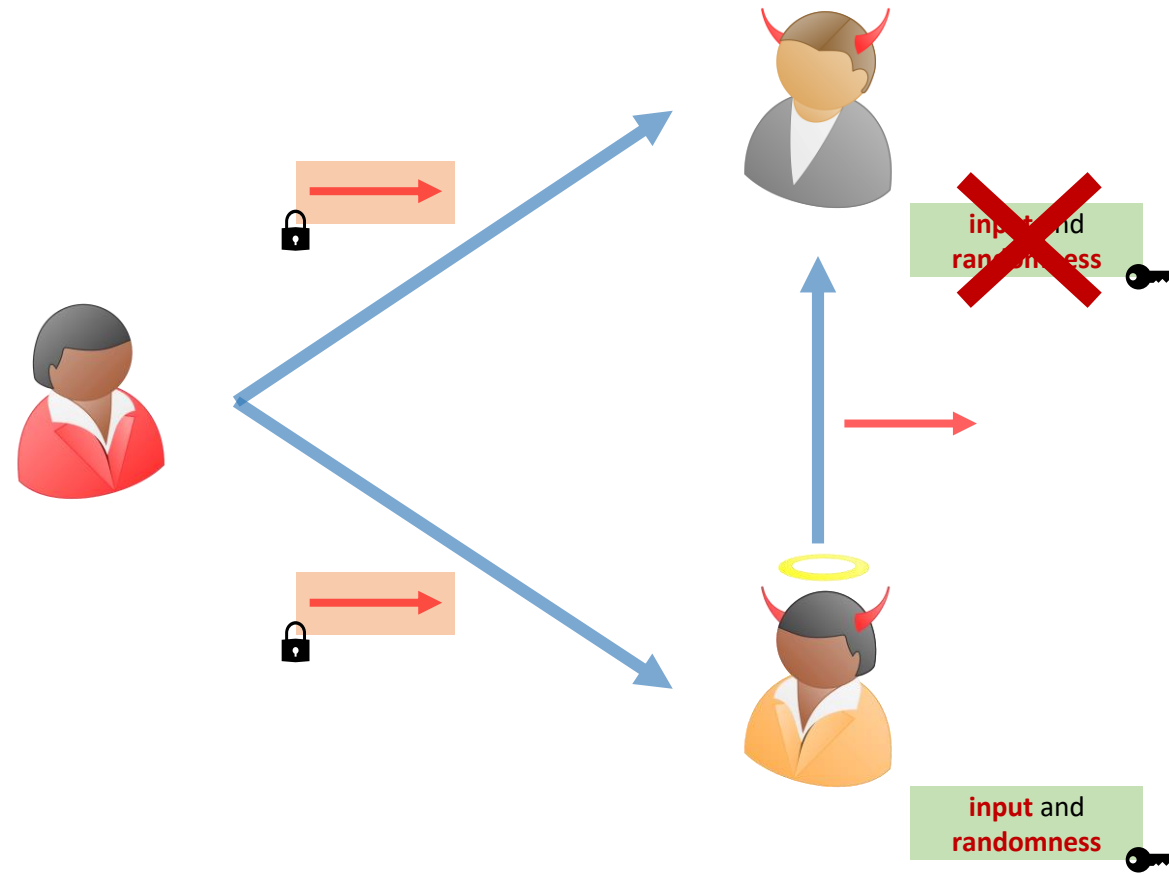
# CDS as safety net



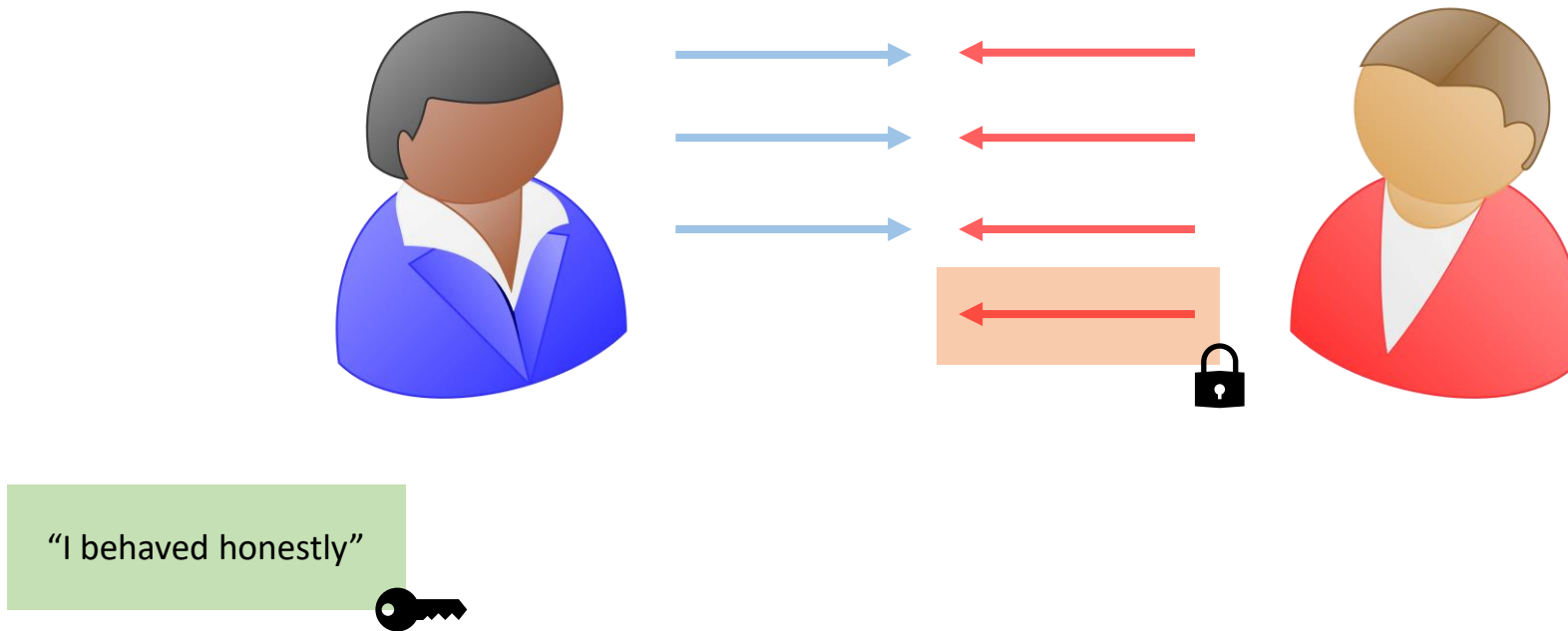
# CDS as safety net



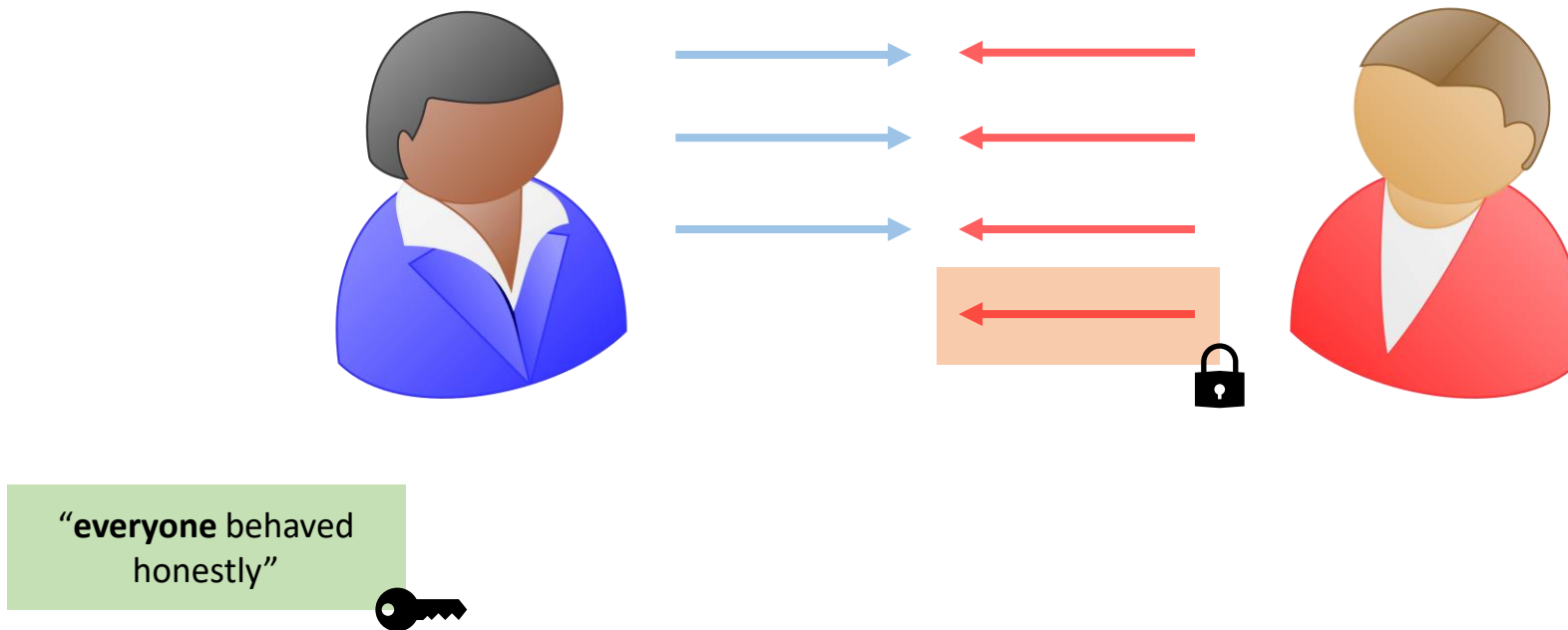
# CDS as safety net



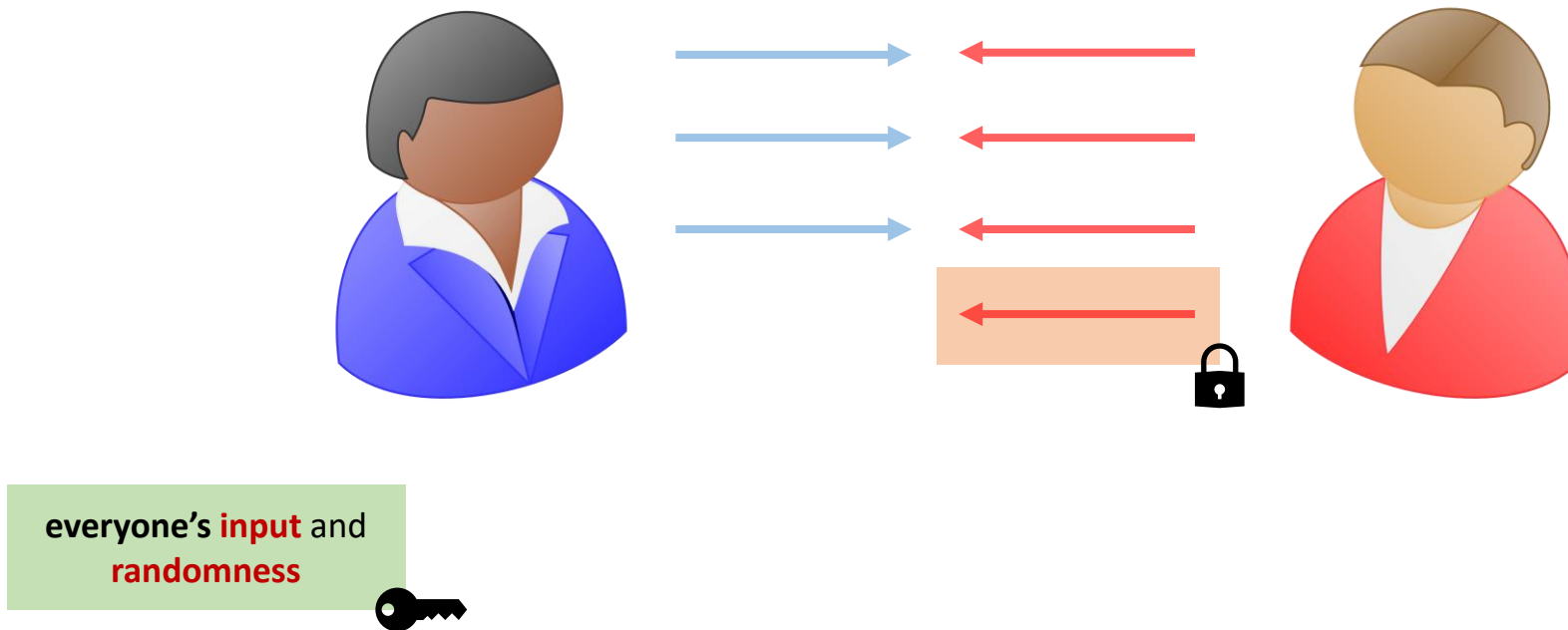
# CDS as safety net



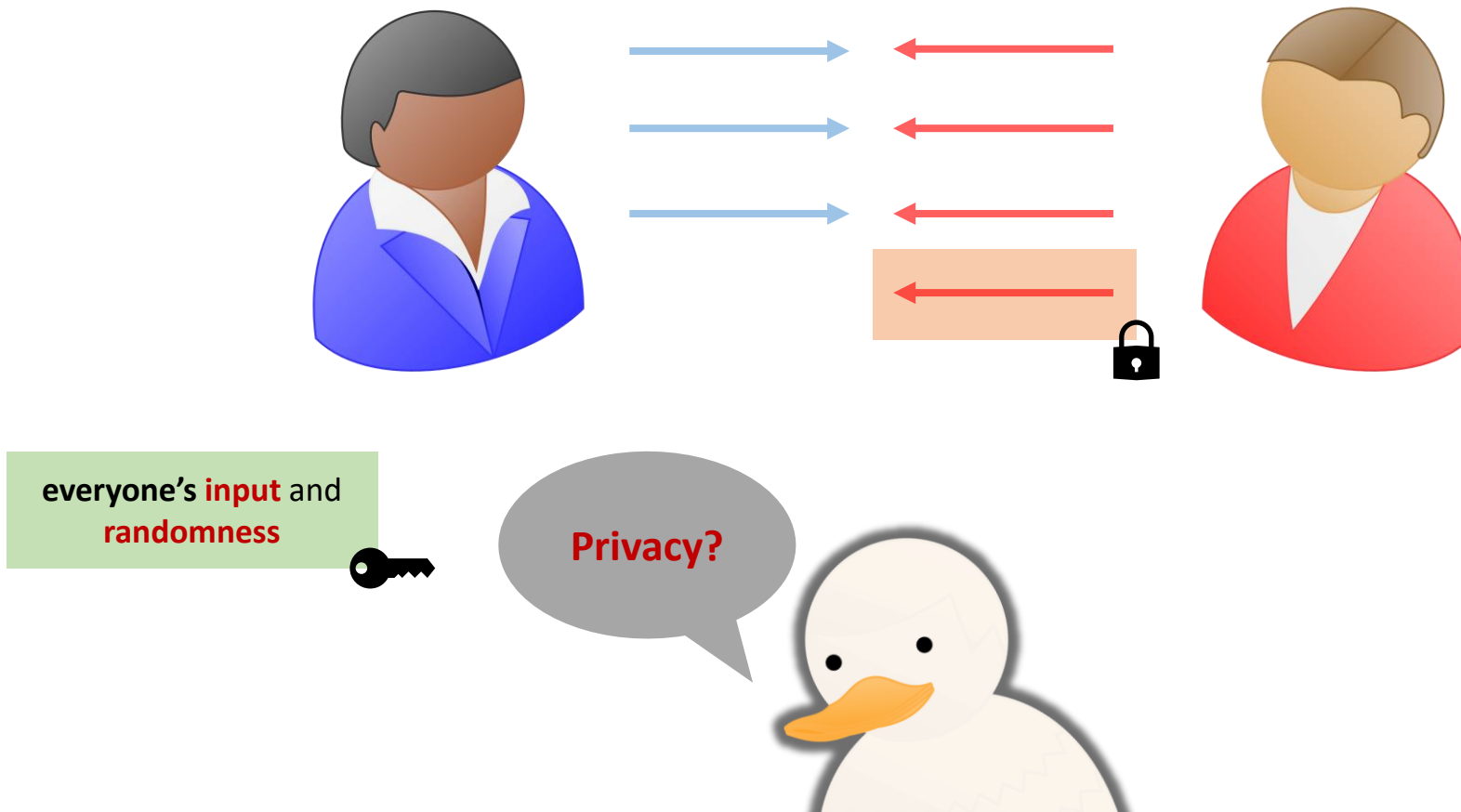
# CDS as safety net



# CDS as safety net

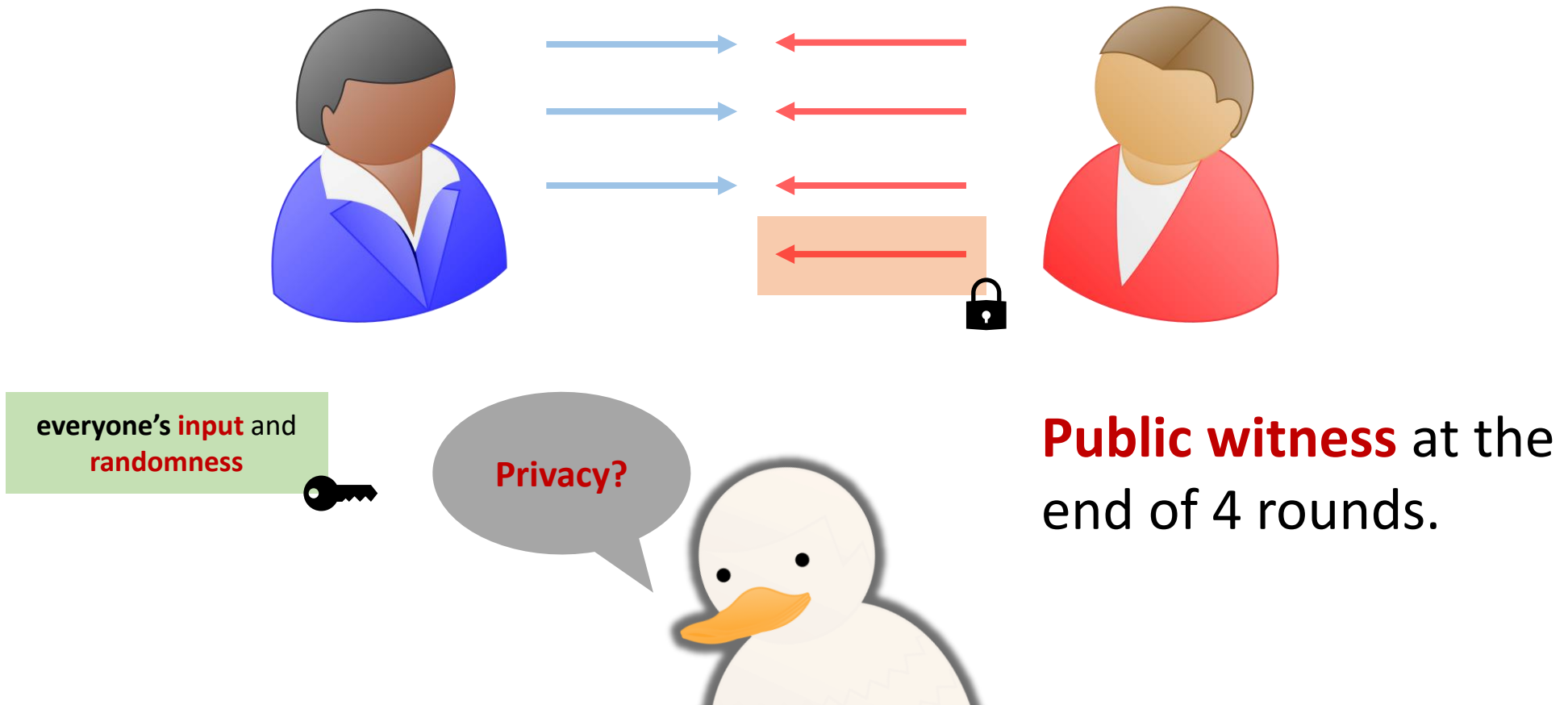


# CDS as safety net

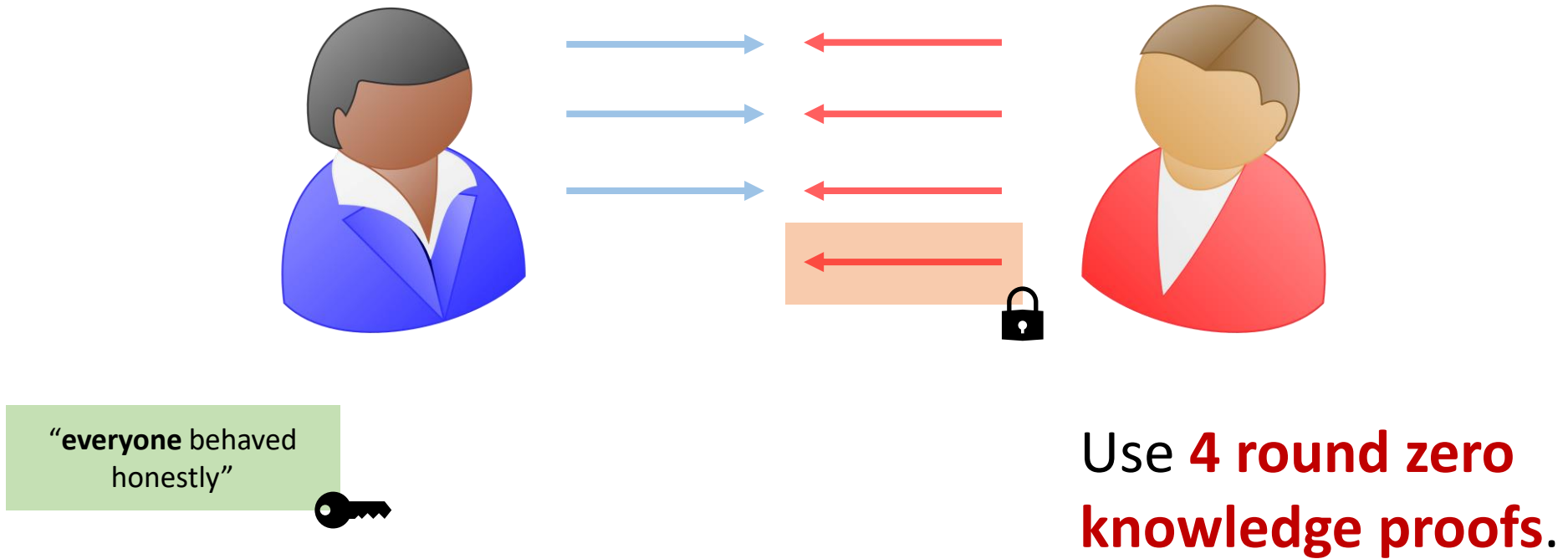




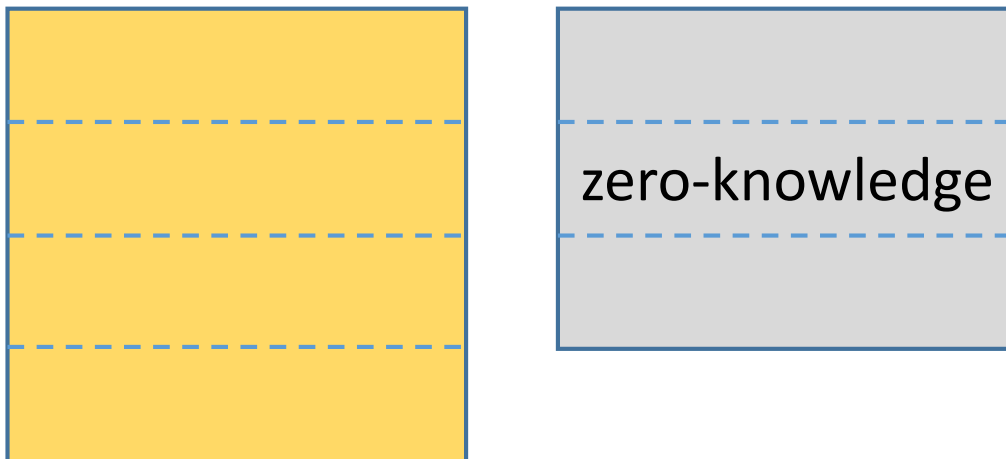
# CDS as safety net



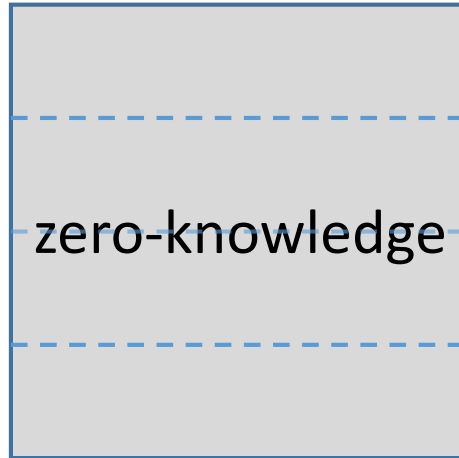
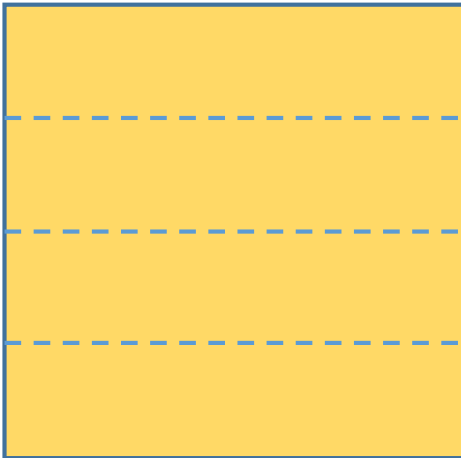
# CDS as safety net



# Our strategy

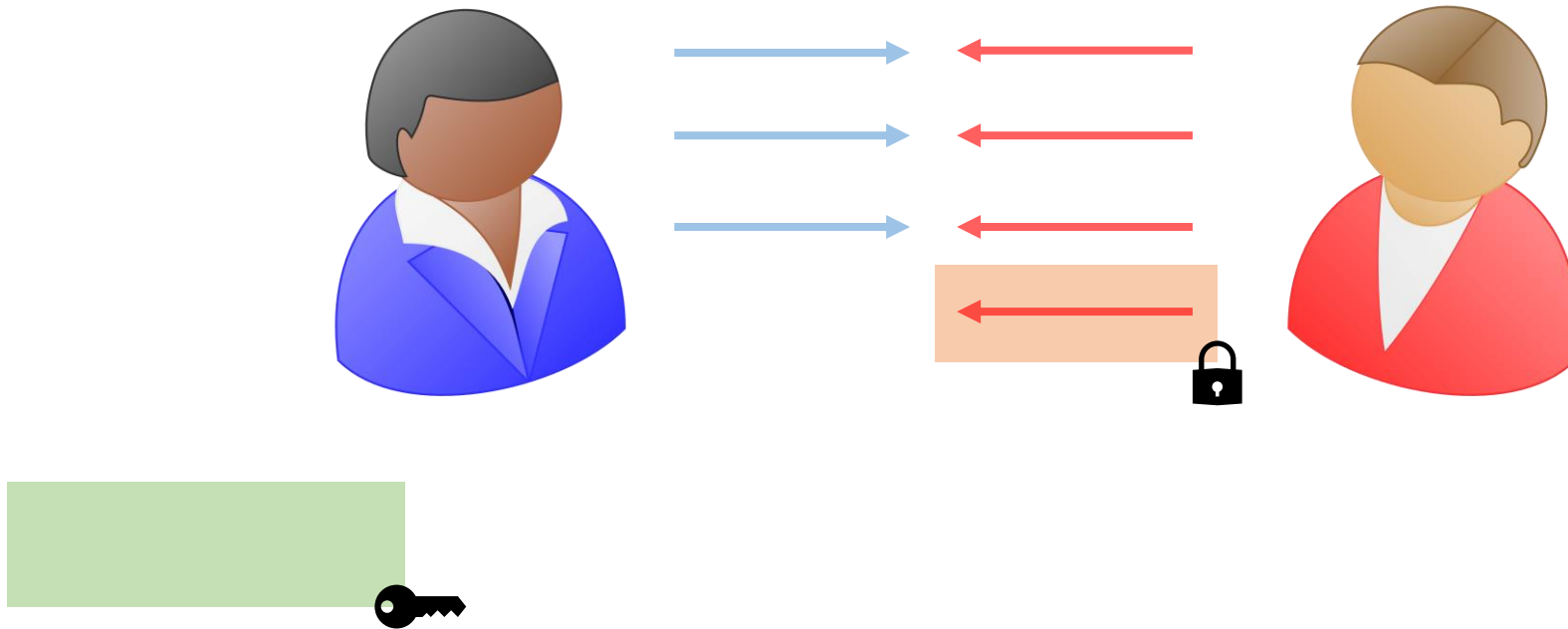


# Our strategy

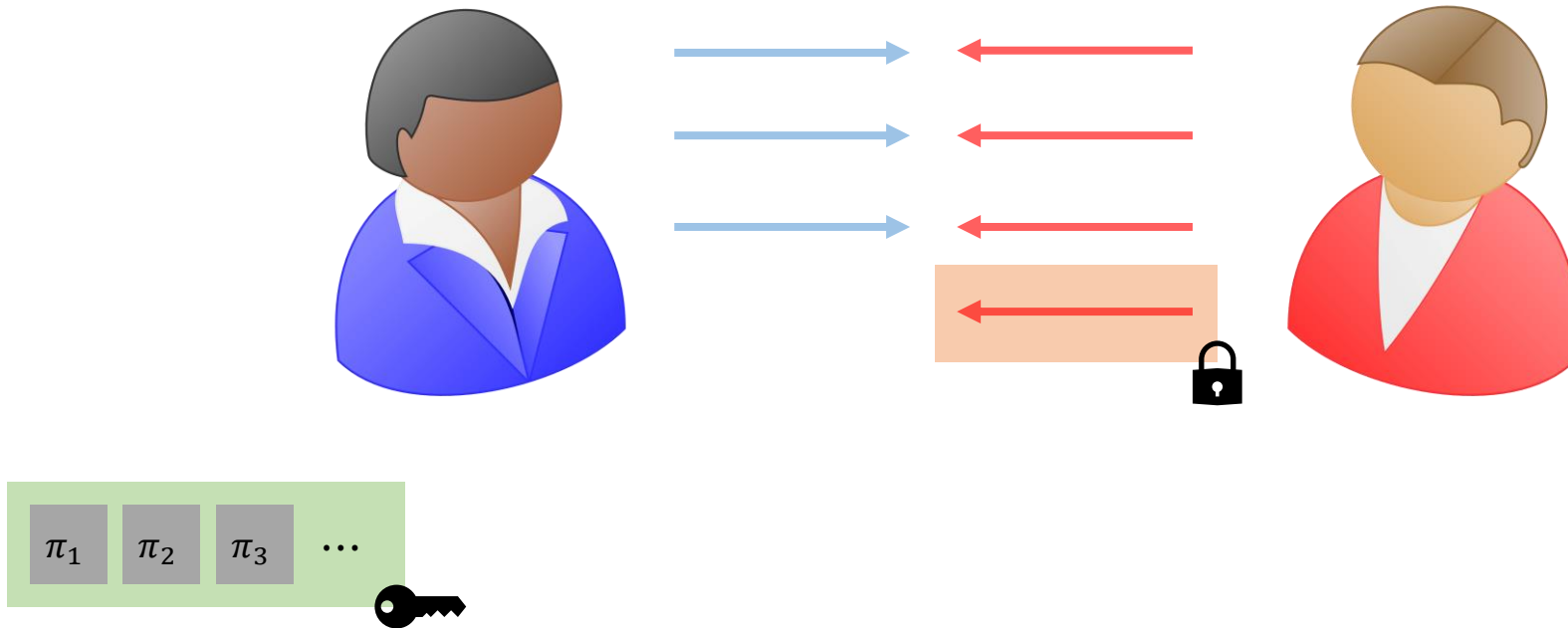


behaved honestly in  
the first 3 rounds

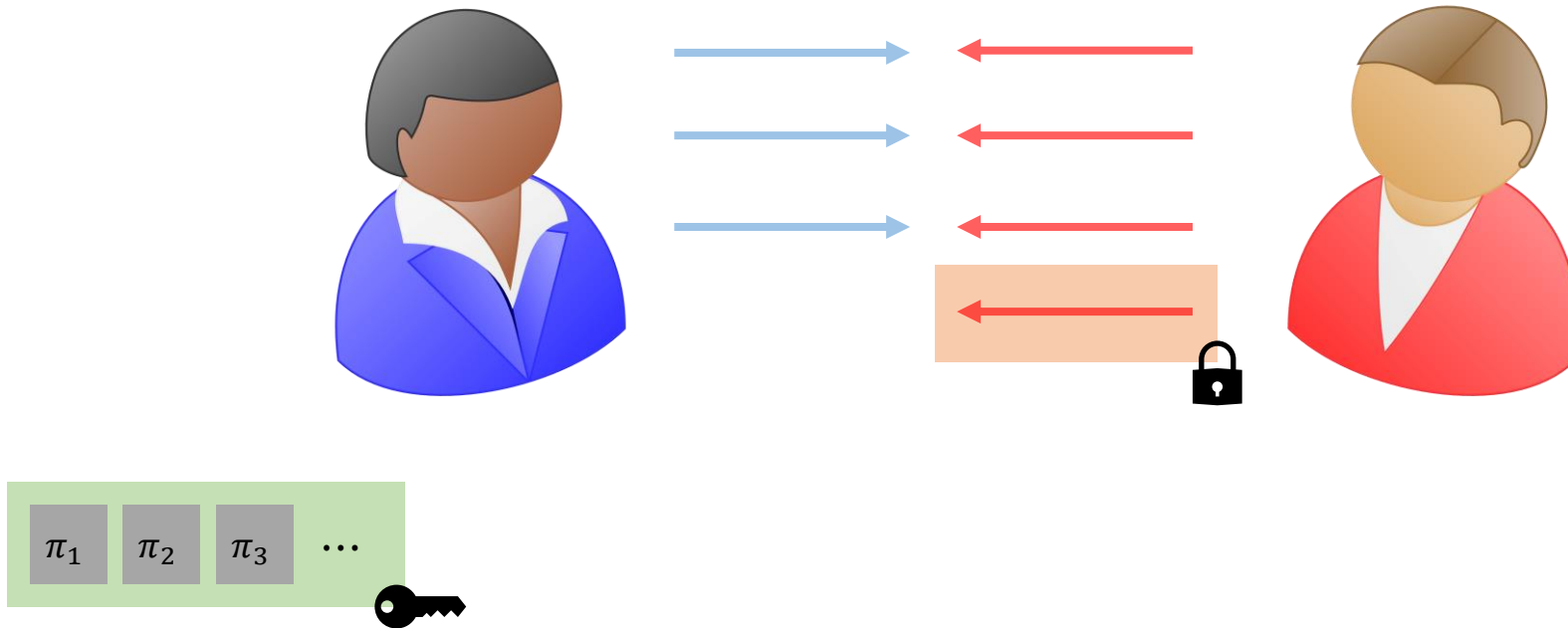
# CDS as safety net



# CDS as safety net

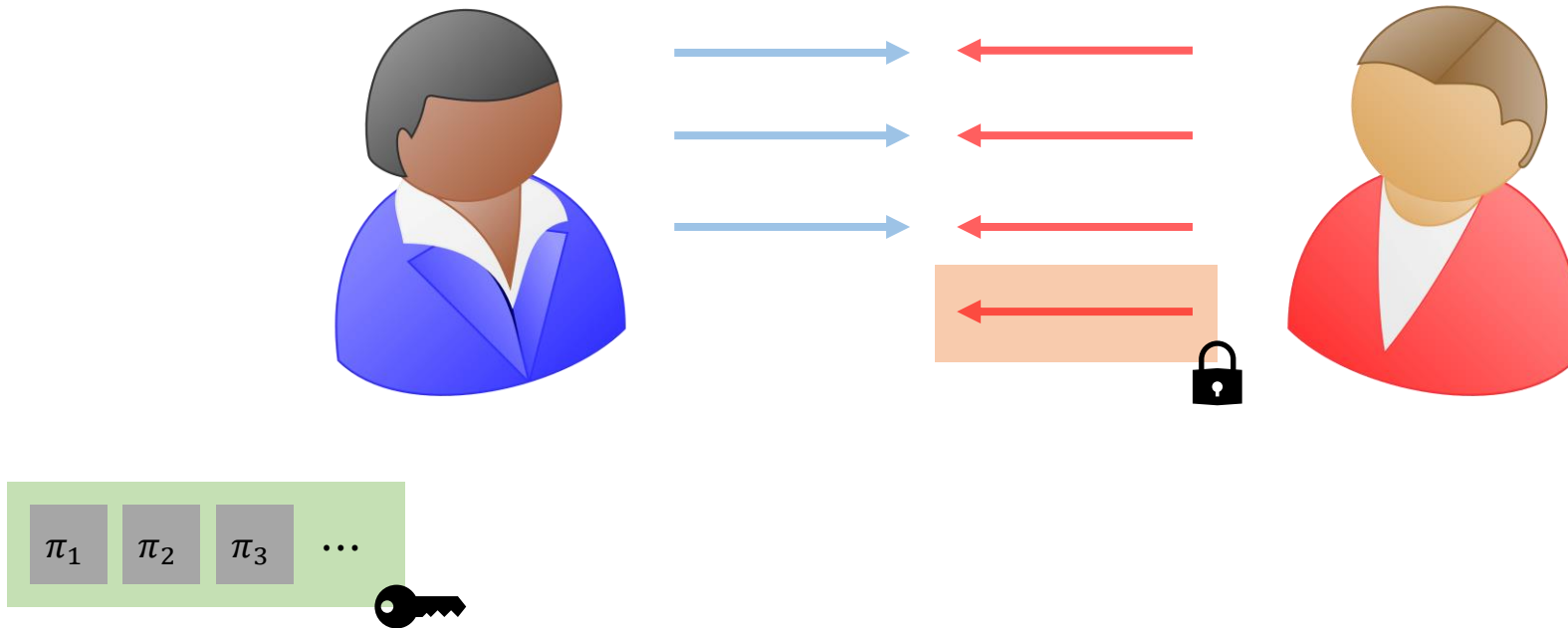


# CDS as safety net



**Witness Encryption**

# CDS as safety net



**Witness Encryption** only known from **iO**.



# Interactive Witness Encryption

# Interactive Witness Encryption

Oblivious Transfer (OT)

# Interactive Witness Encryption

Oblivious Transfer (OT)

Garbled Circuit

# Interactive Witness Encryption

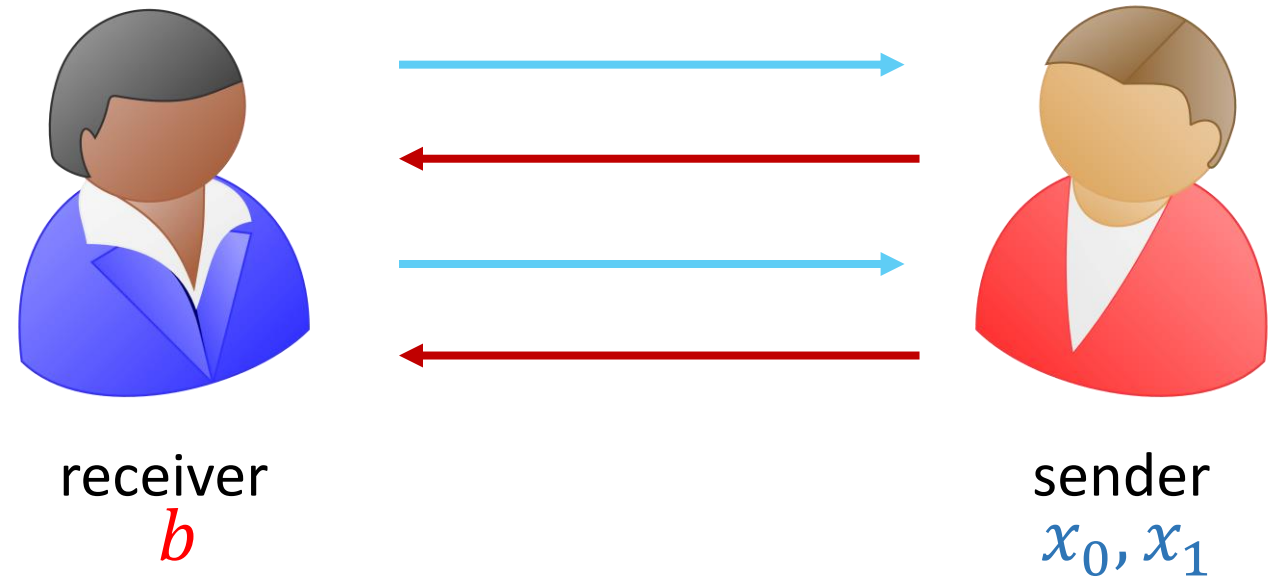
**Oblivious Transfer (OT)**

Garbled Circuit

# Interactive Witness Encryption

## Oblivious Transfer (OT)

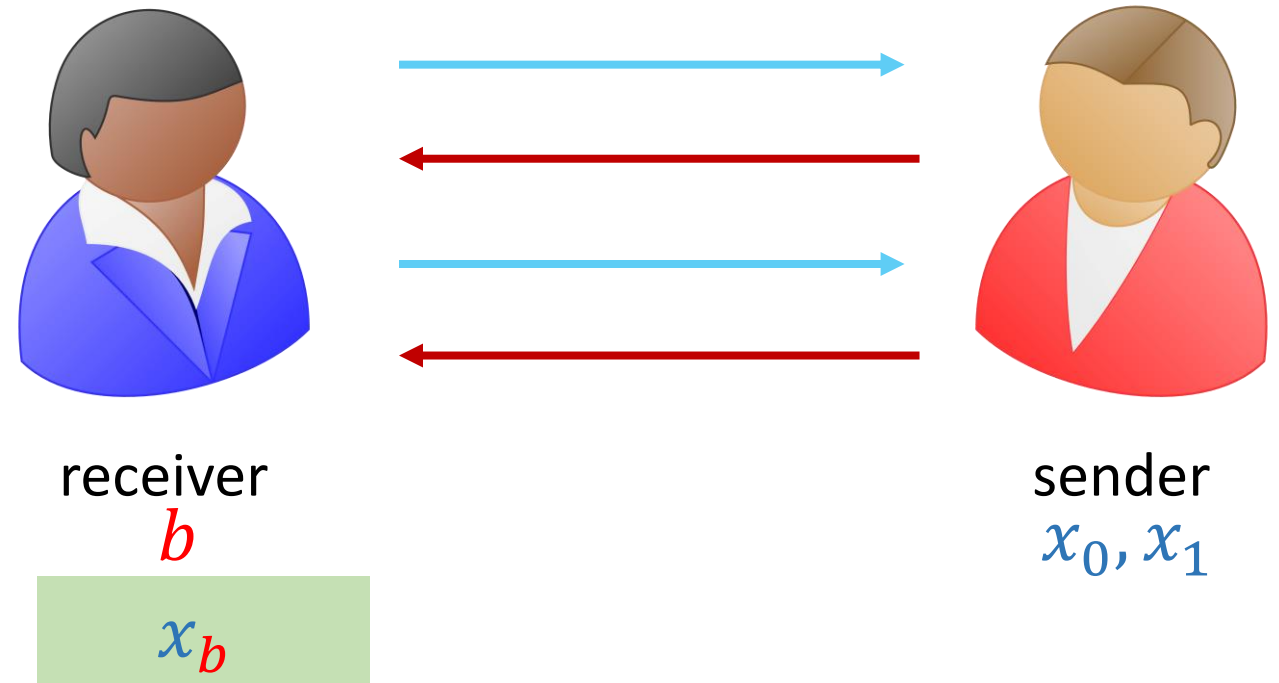
Garbled Circuit



# Interactive Witness Encryption

## Oblivious Transfer (OT)

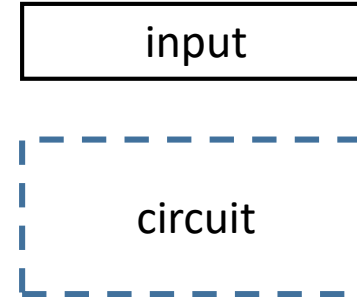
Garbled Circuit



# Interactive Witness Encryption

Oblivious Transfer (OT)

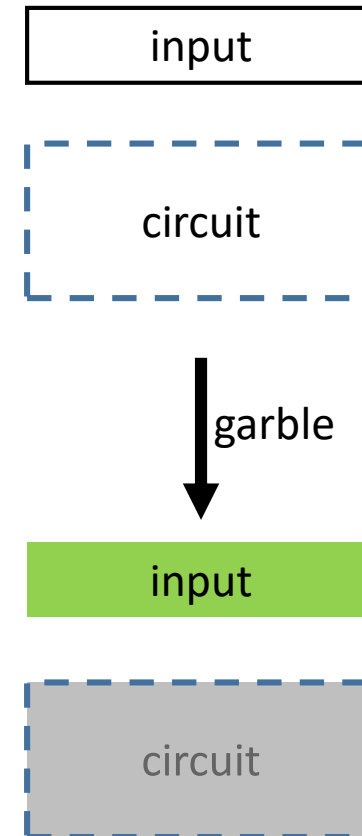
**Garbled Circuit**



# Interactive Witness Encryption

Oblivious Transfer (OT)

**Garbled Circuit**

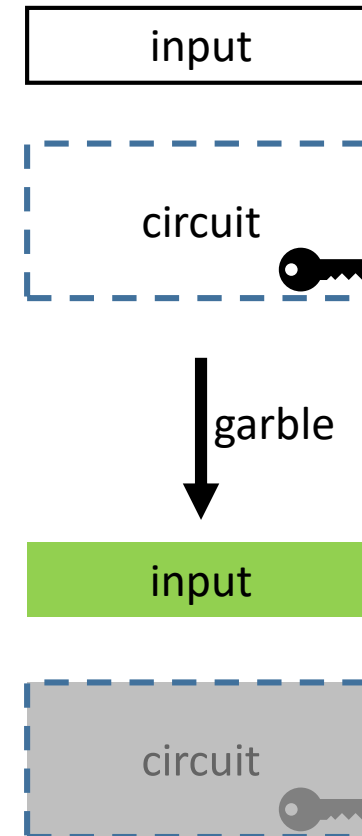




# Interactive Witness Encryption

Oblivious Transfer (OT)

**Garbled Circuit**



# Interactive Witness Encryption

witness

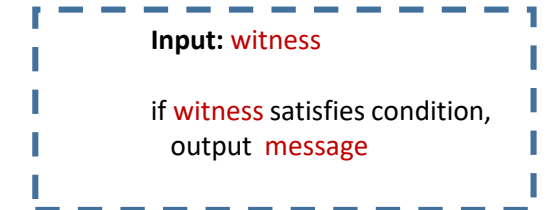


receiver



sender

message



# Interactive Witness Encryption

witness

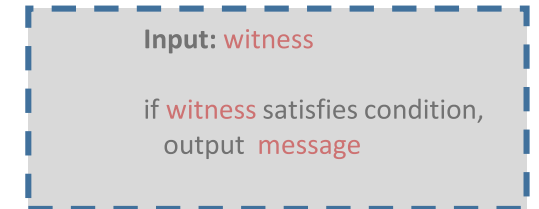


receiver

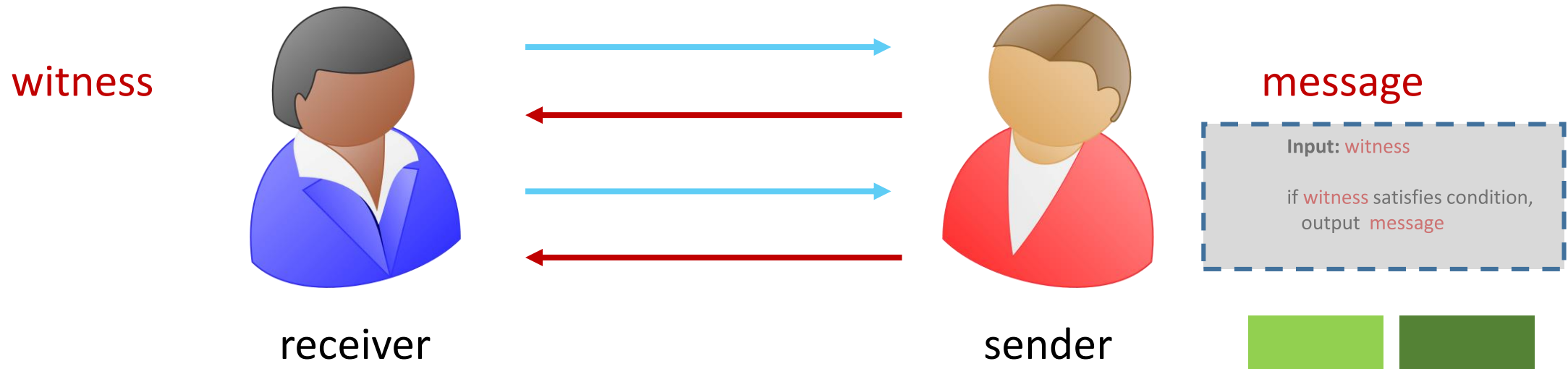


sender

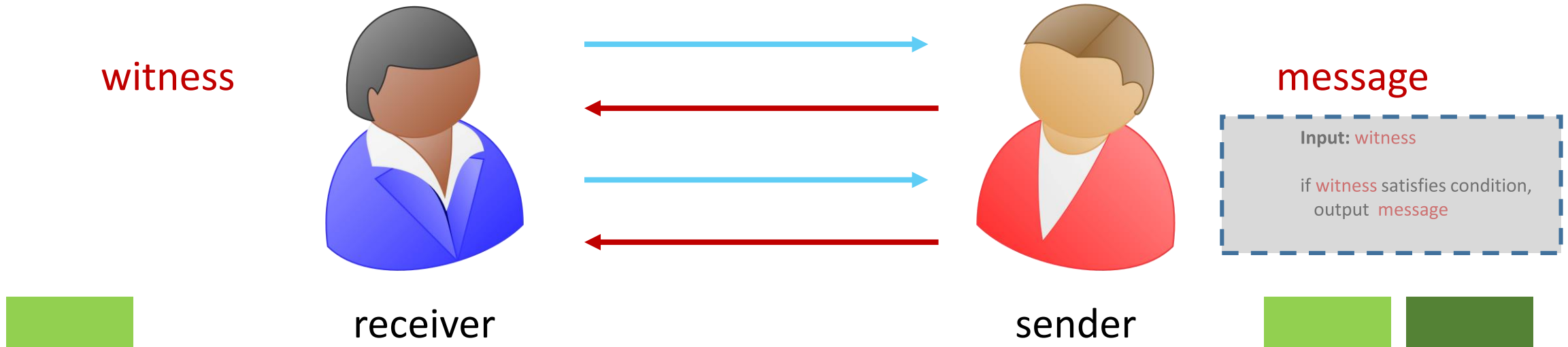
message



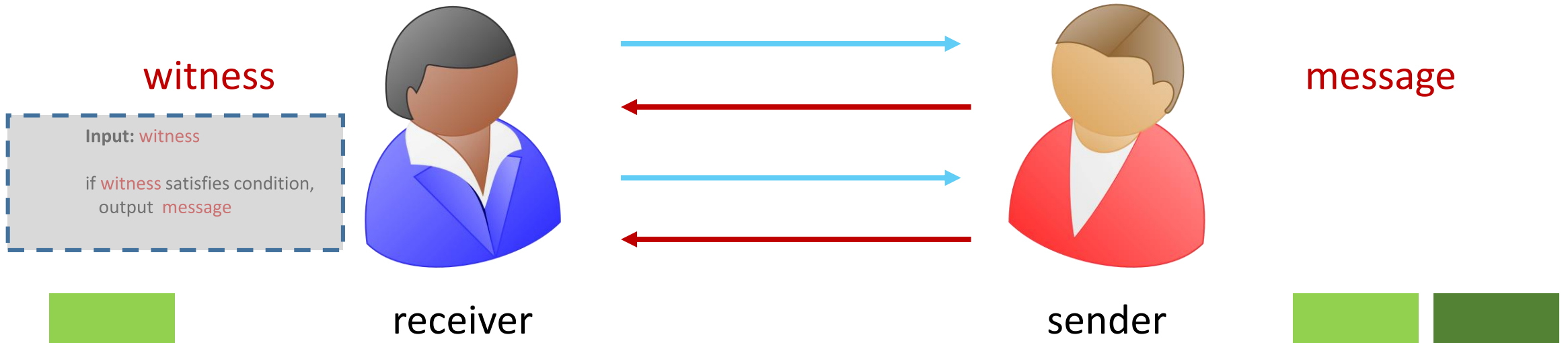
# Interactive Witness Encryption



# Interactive Witness Encryption

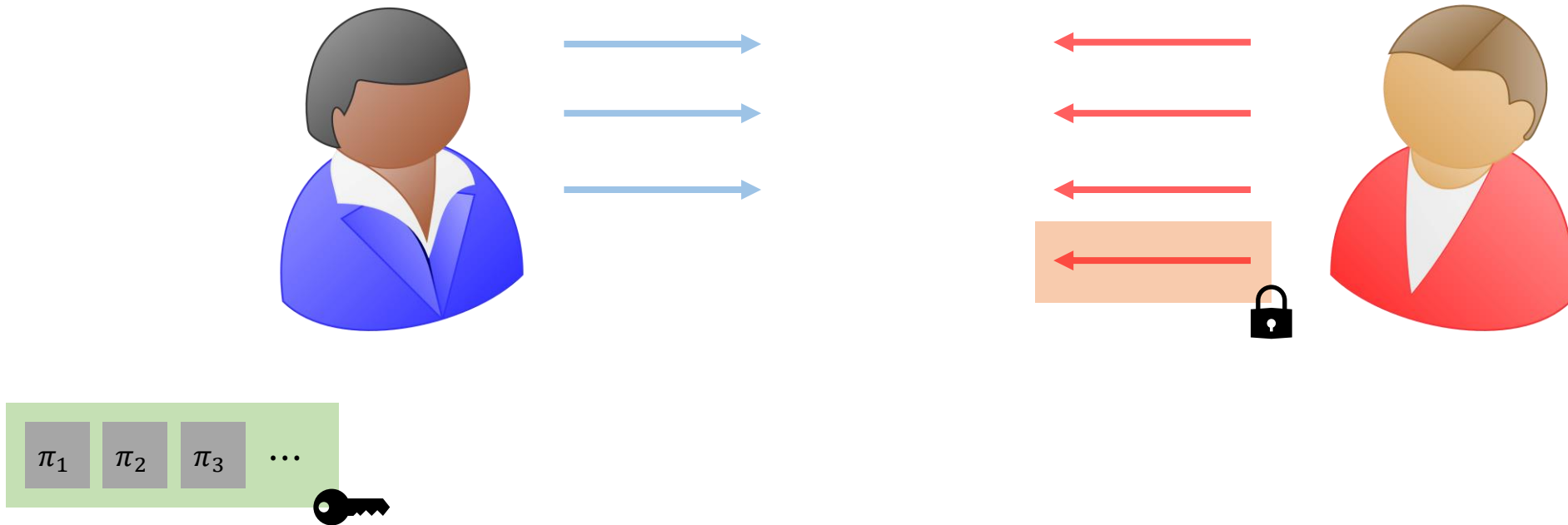


# Interactive Witness Encryption



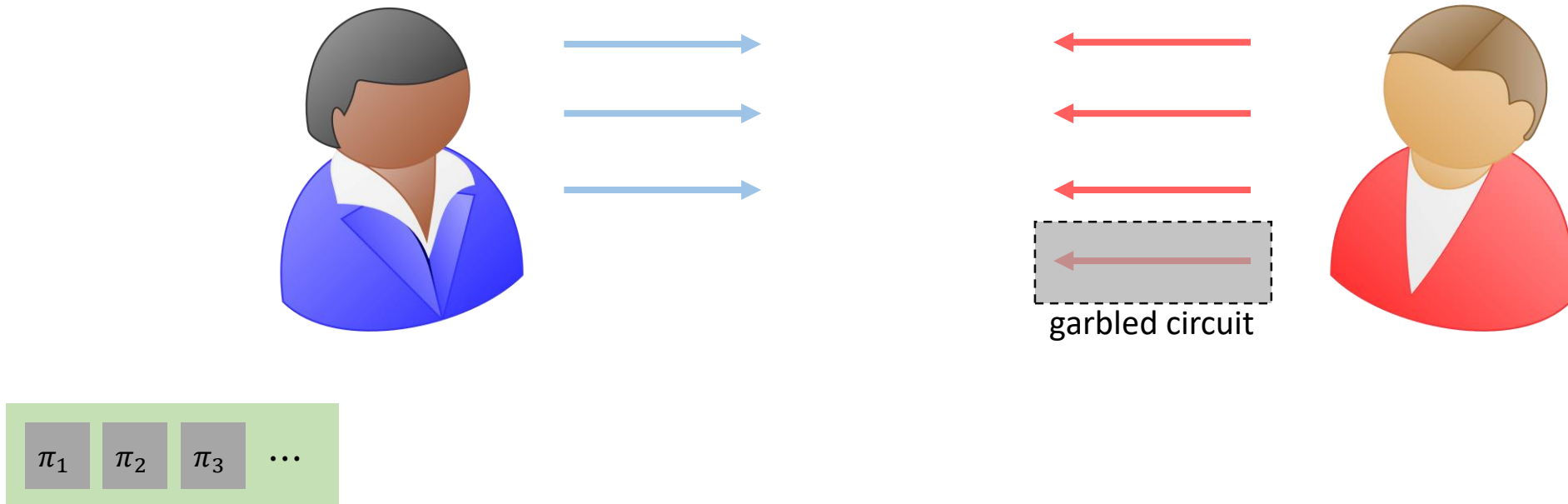
# Interactive Witness Encryption

# Interactive Witness Encryption

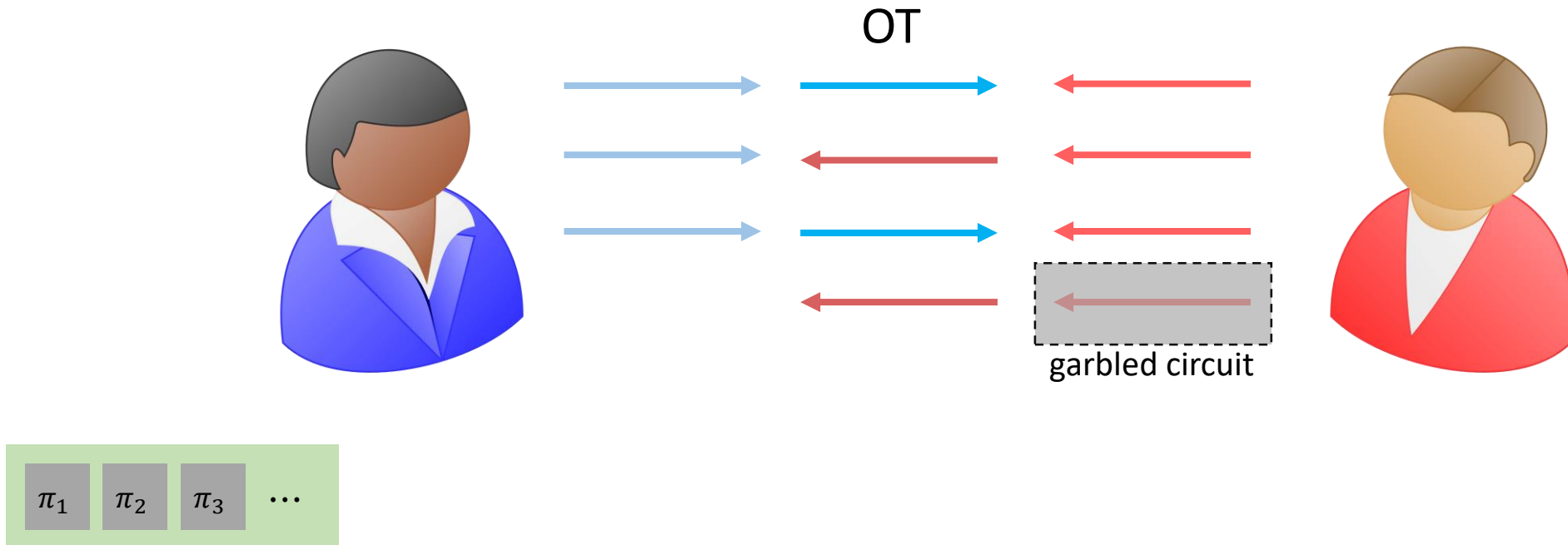




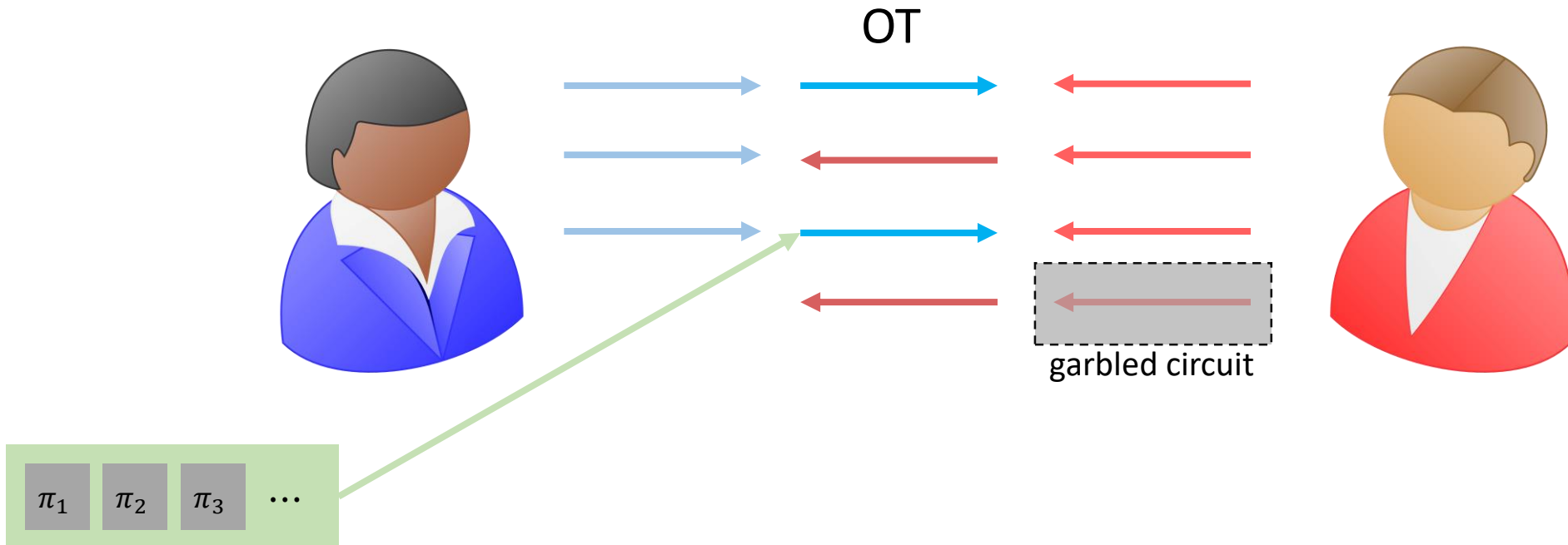
# Interactive Witness Encryption



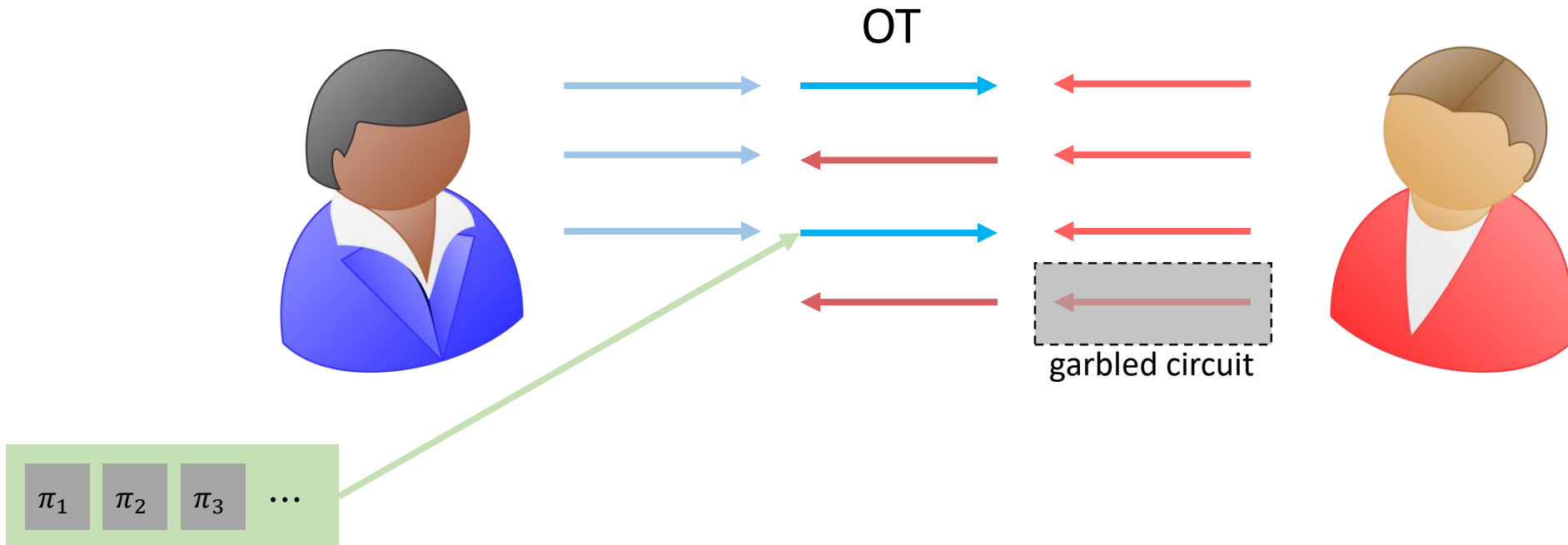
# Interactive Witness Encryption



# Interactive Witness Encryption



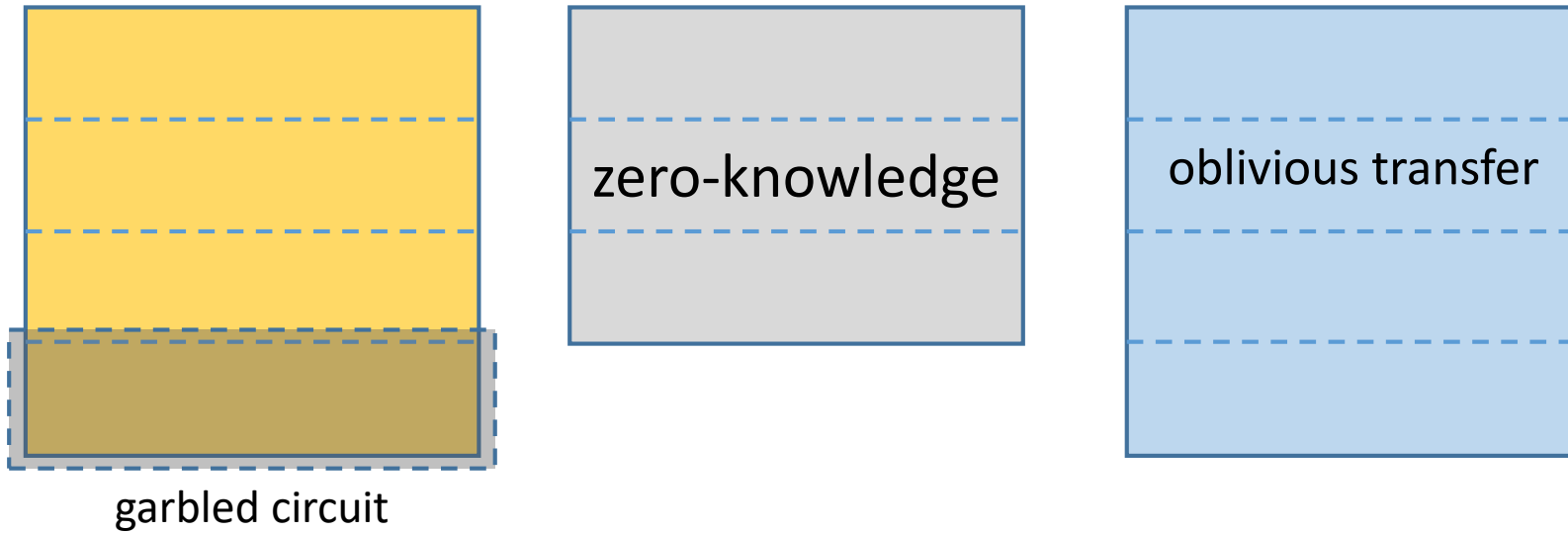
# Interactive Witness Encryption



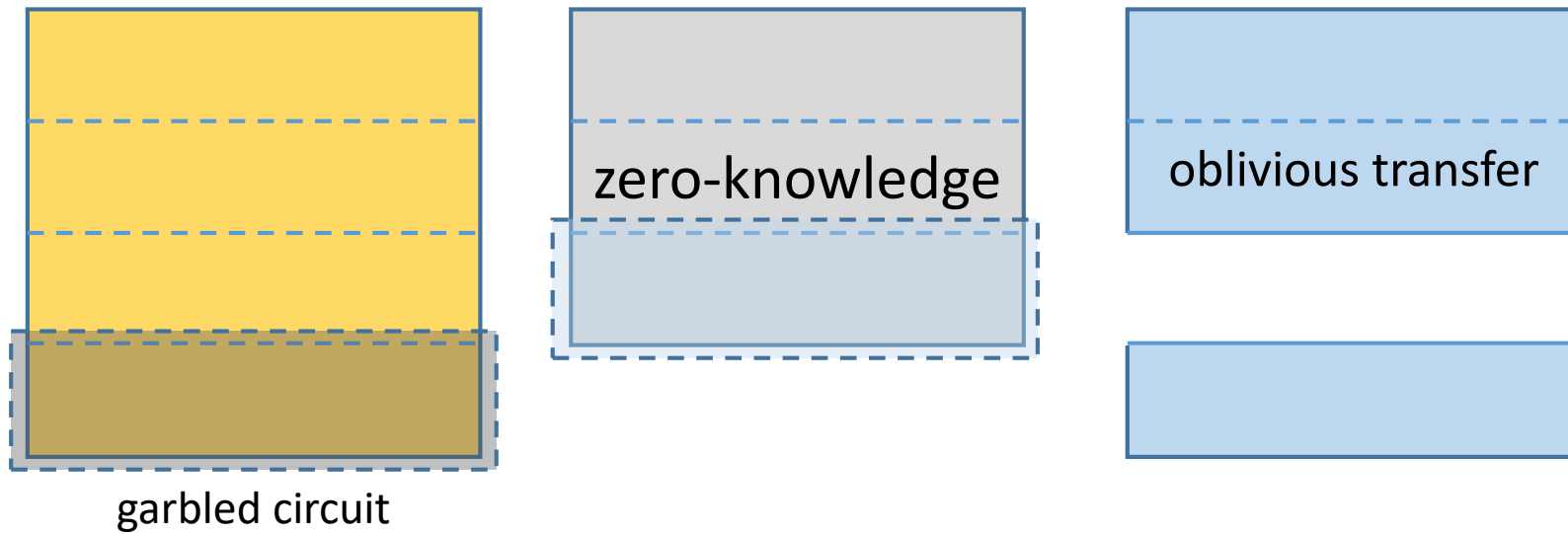
Requires **3 round zero-knowledge proofs!**



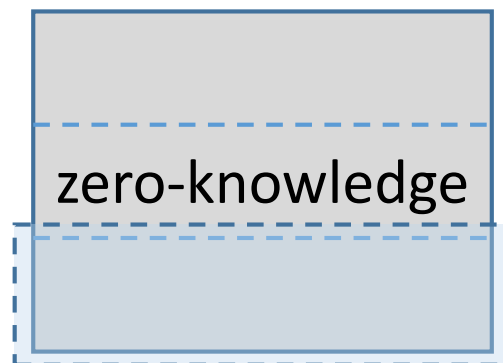
# Our strategy



# Our strategy

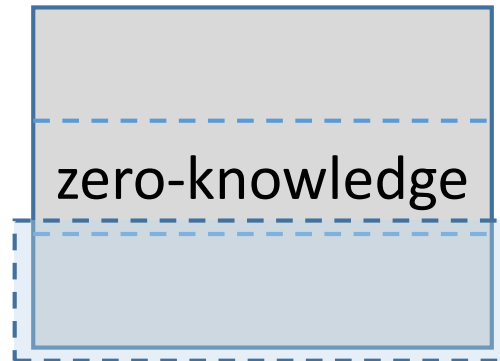


# Our strategy



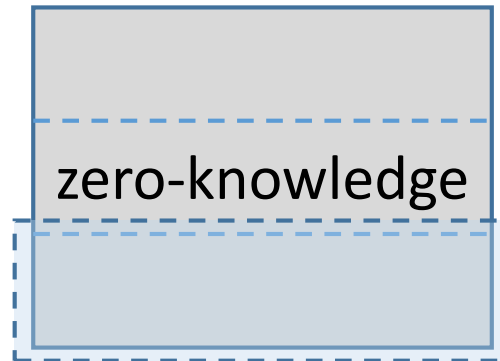


# Our strategy



**simultaneous message** model

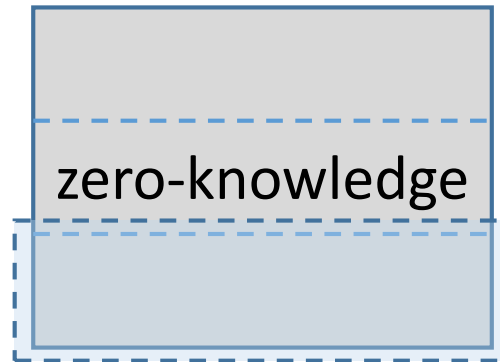
# Our strategy



**simultaneous message** model

third round **hidden** until the fourth round

# Our strategy



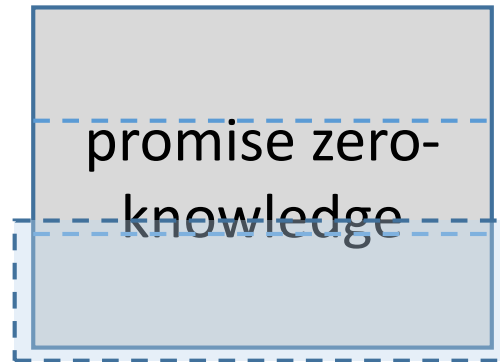
**simultaneous message** model

third round **hidden** until the fourth round

Want **3 round** zero-knowledge protocol in the **simultaneous message** model secure against **verifiers who do not abort**.

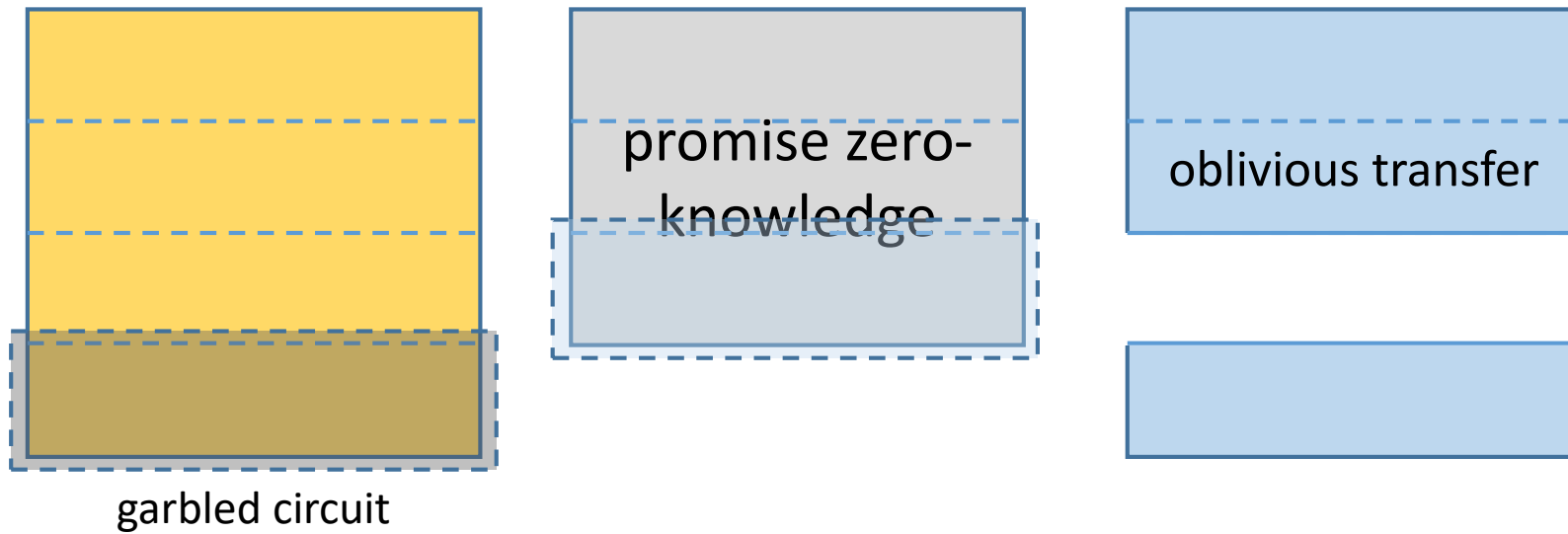
# Promise Zero-Knowledge

[Badrinarayanan-Goyal-Jain-Kalai-Khurana-Sahai18]

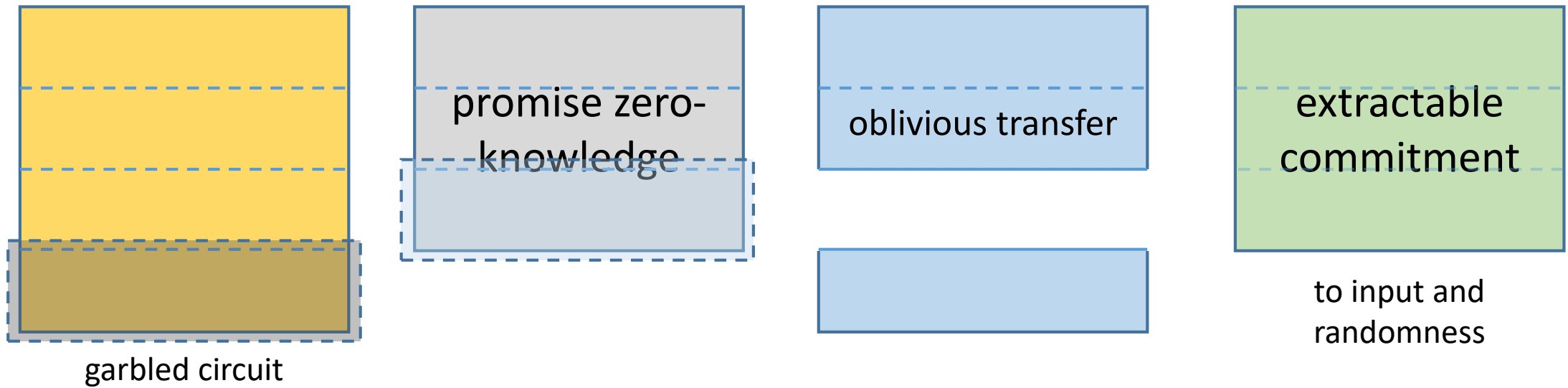


**3 round** zero-knowledge protocol in the **simultaneous message** model secure against **verifiers who do not abort** assuming **OT**.

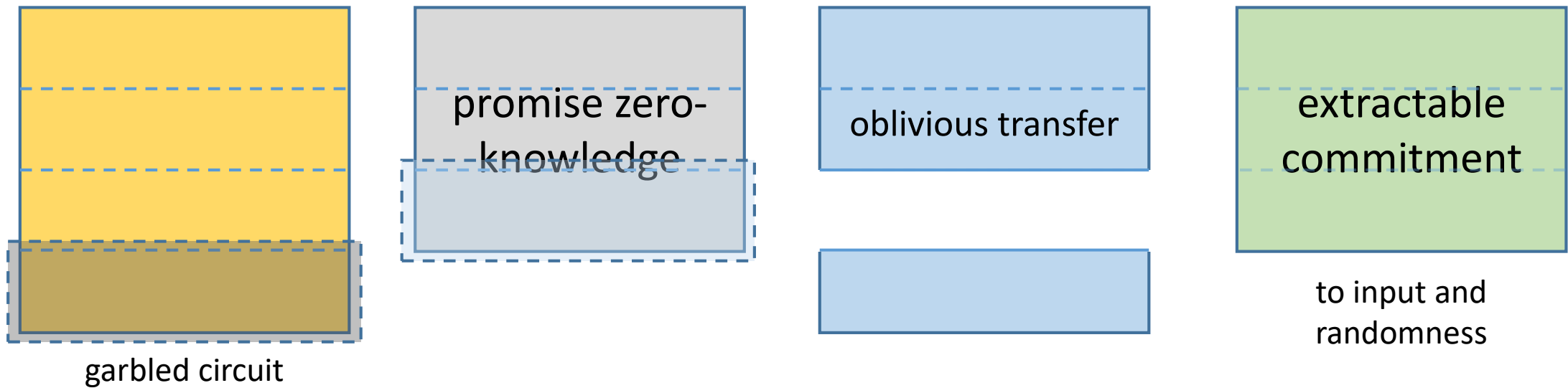
# Our strategy



# Our strategy

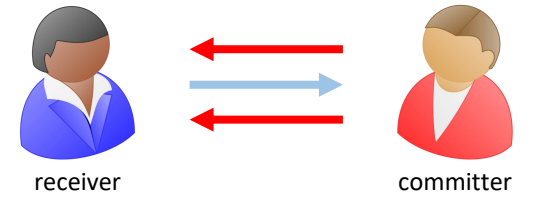


# Our strategy



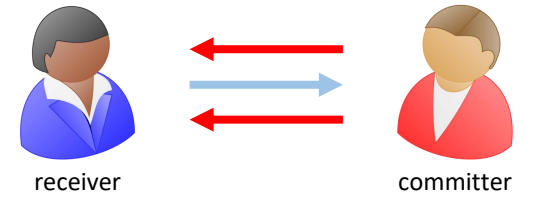
Extraction by **rewinding**

# Extraction by Rewinding

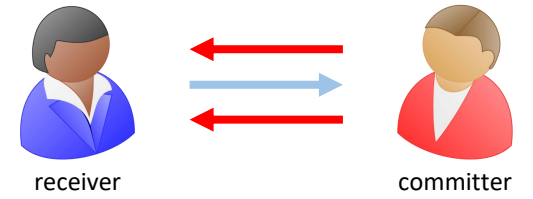




# Extraction by Rewinding

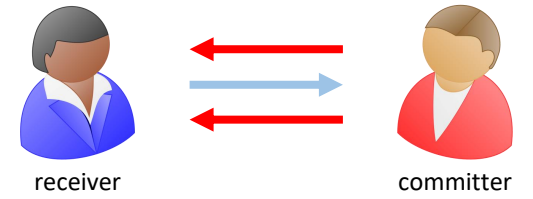


# Extraction by Rewinding



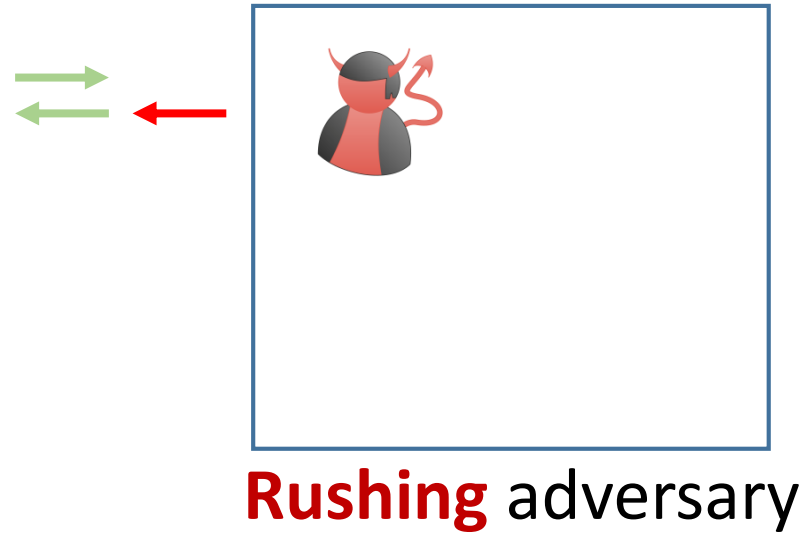
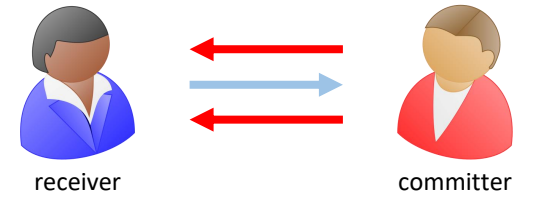
**Rushing** adversary

# Extraction by Rewinding

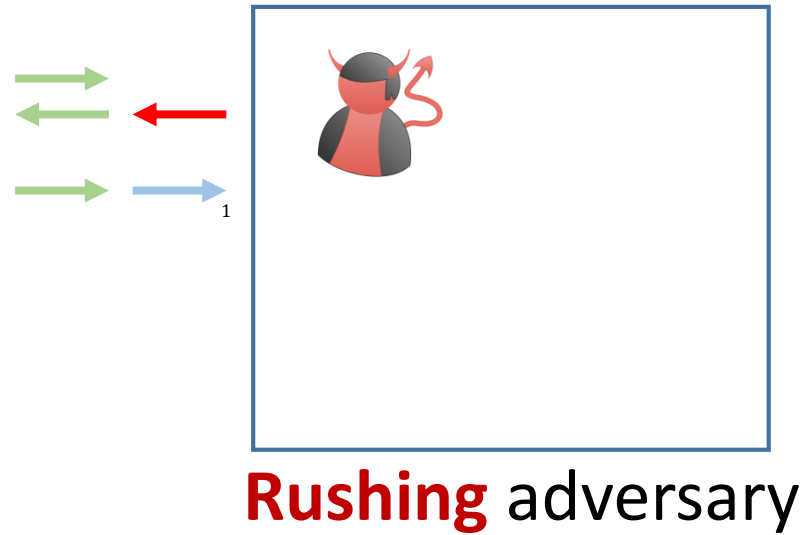
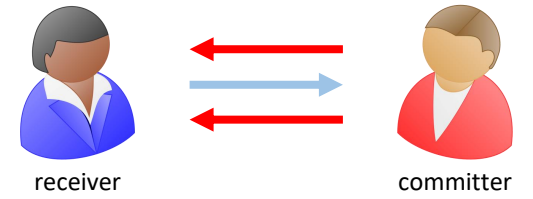


**Rushing** adversary

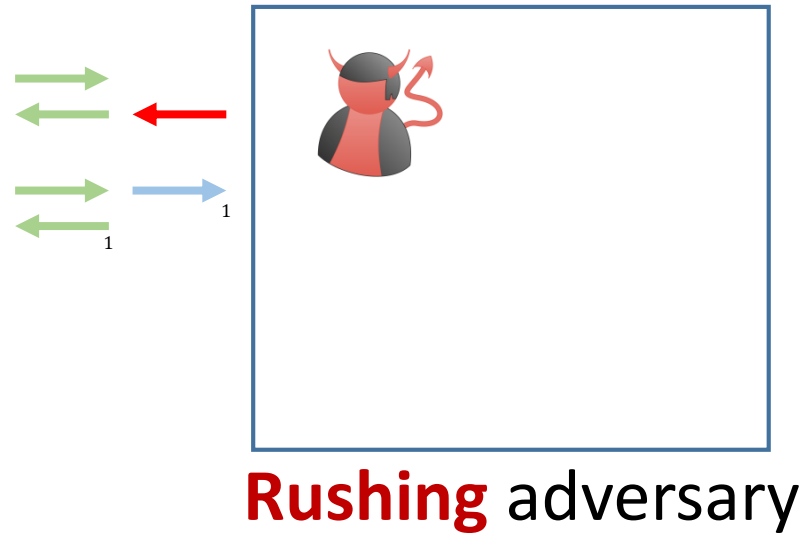
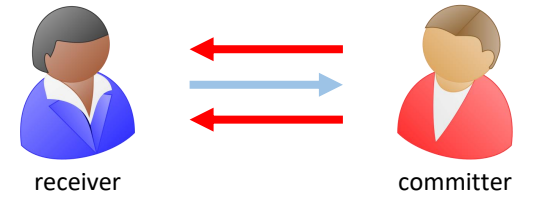
# Extraction by Rewinding



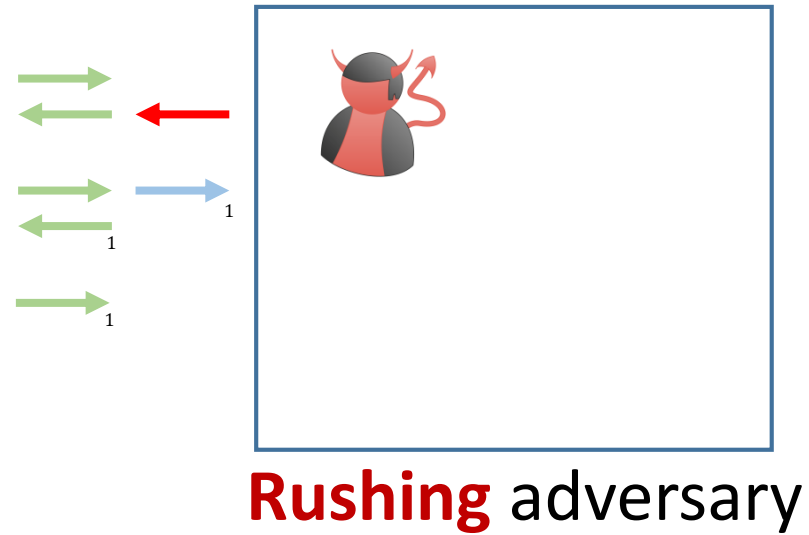
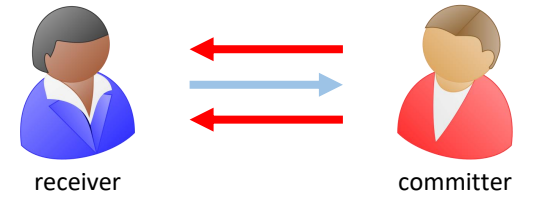
# Extraction by Rewinding



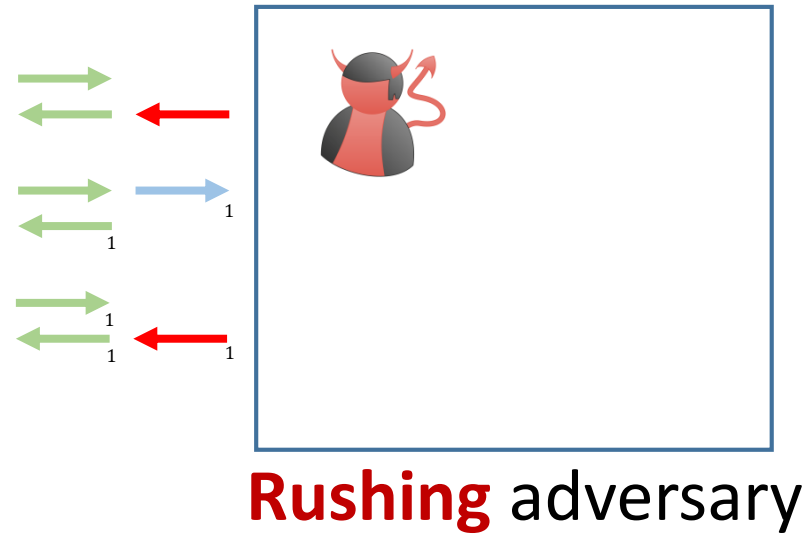
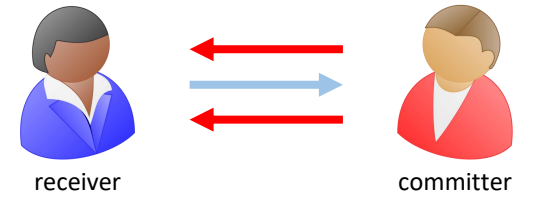
# Extraction by Rewinding



# Extraction by Rewinding

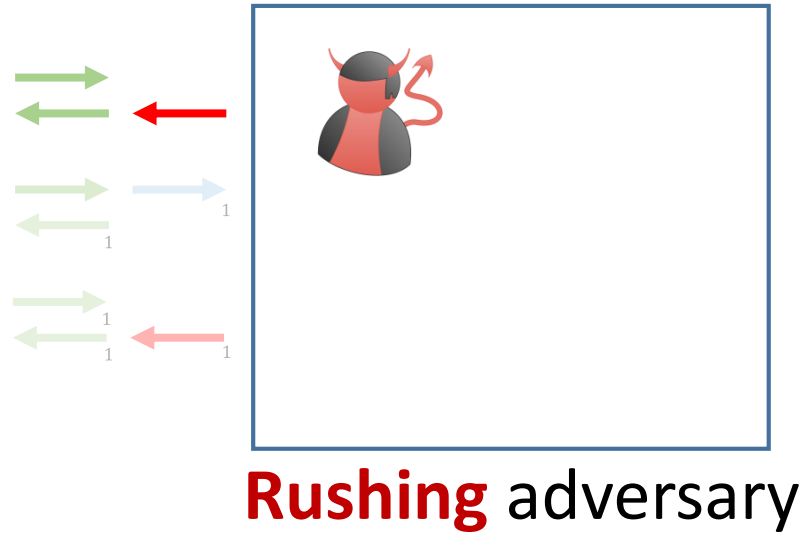
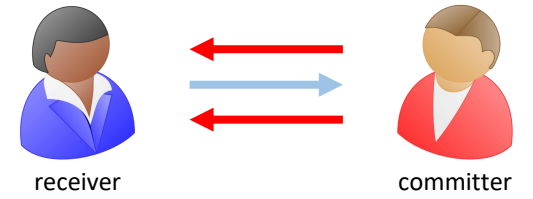


# Extraction by Rewinding

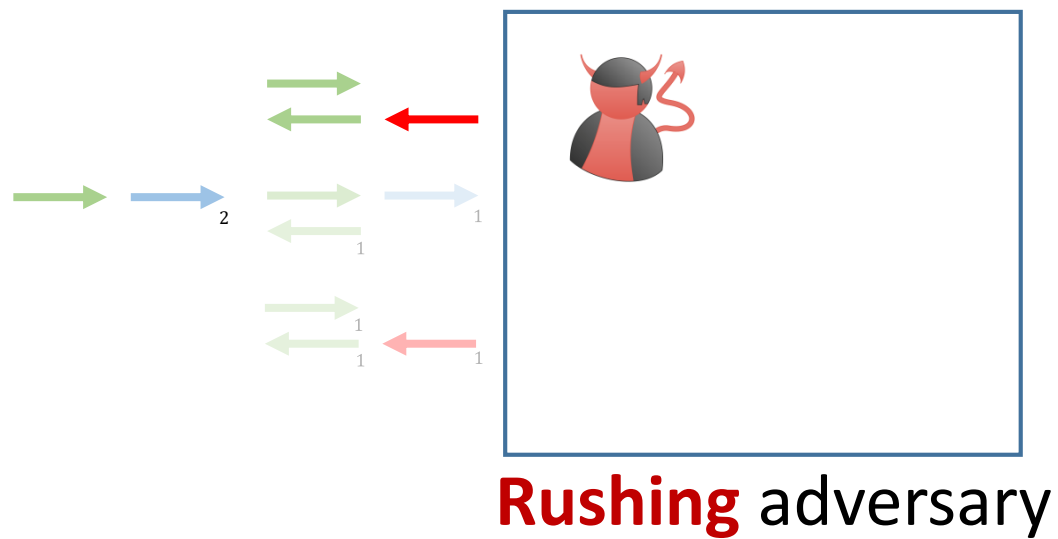
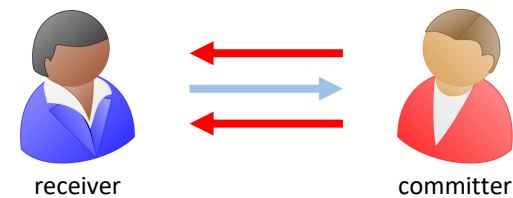




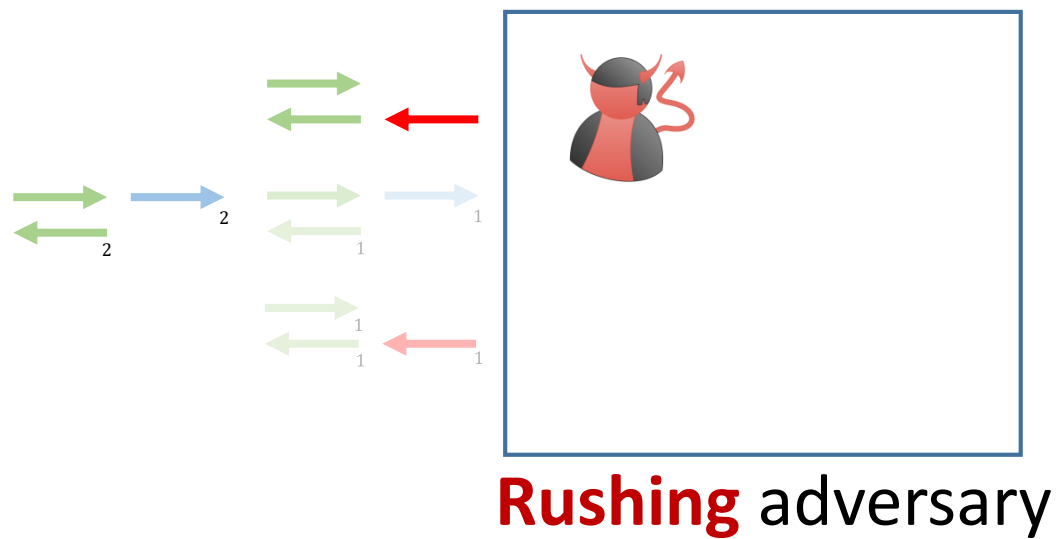
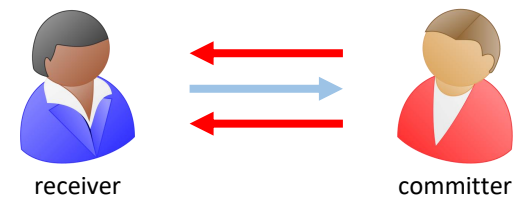
# Extraction by Rewinding



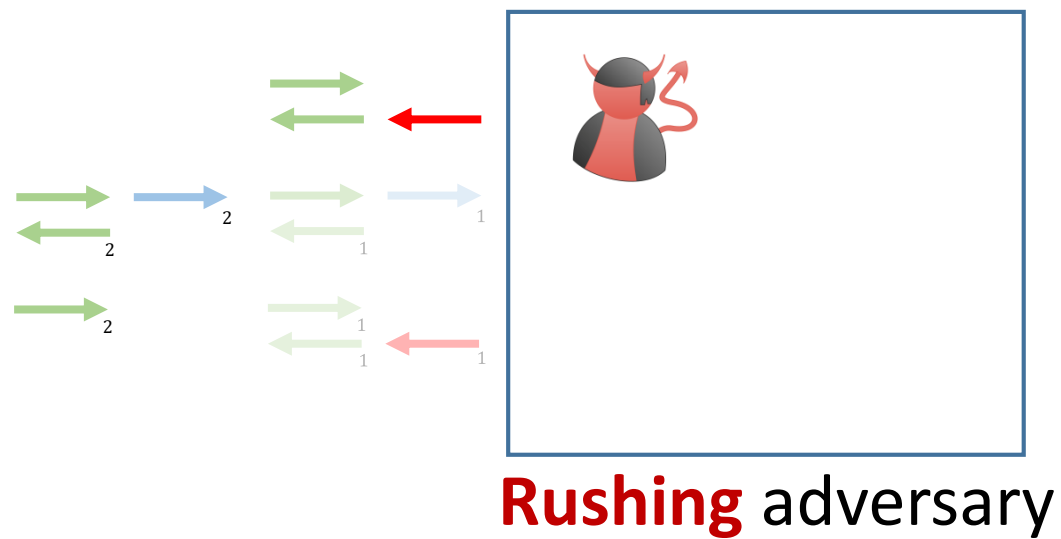
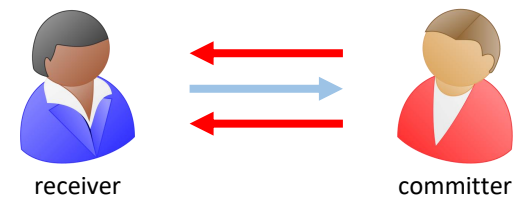
# Extraction by Rewinding



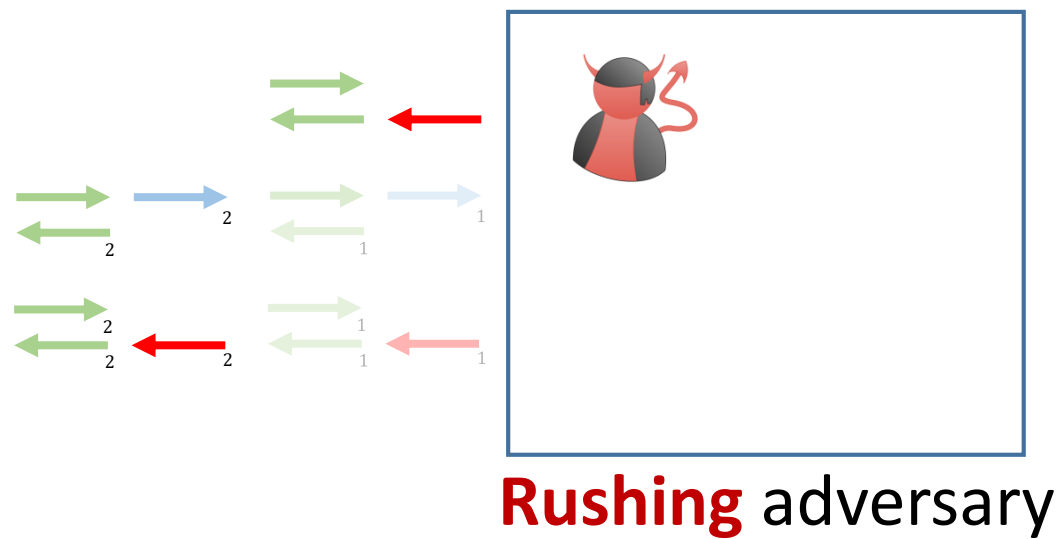
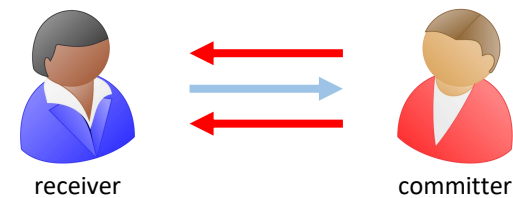
# Extraction by Rewinding



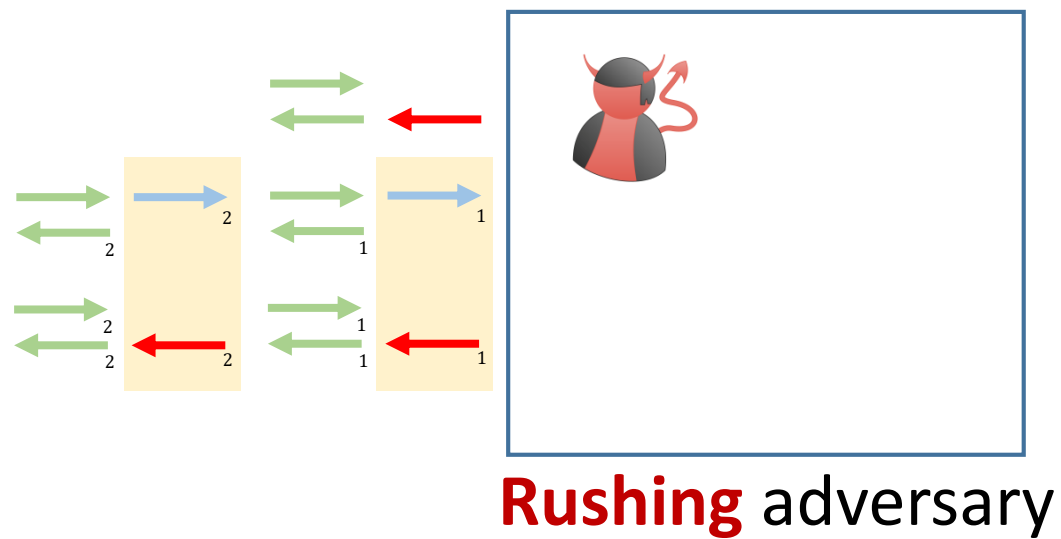
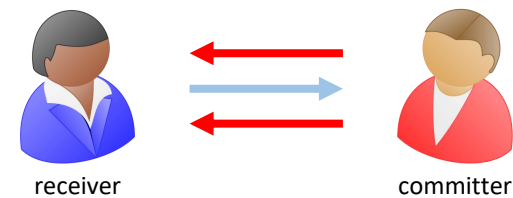
# Extraction by Rewinding



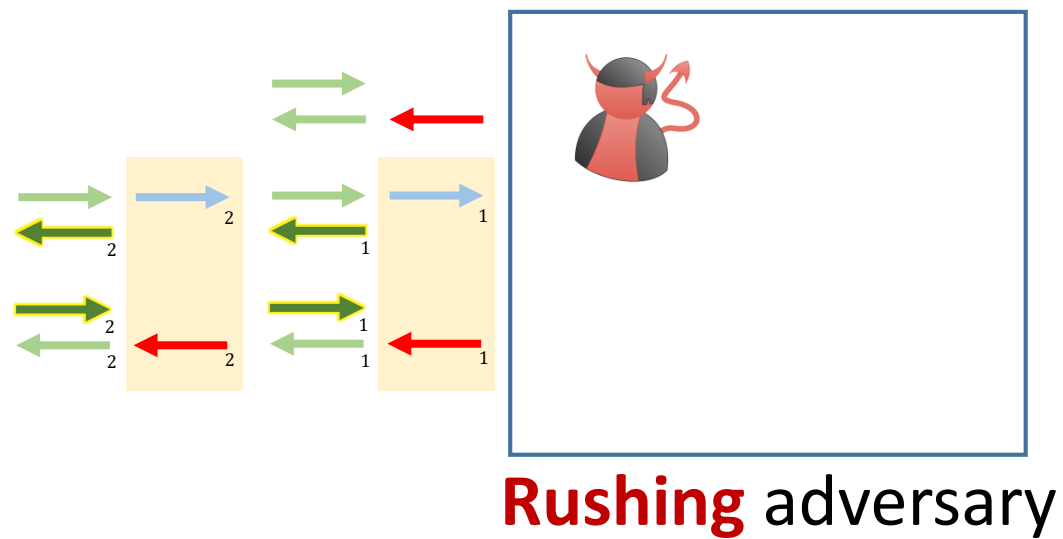
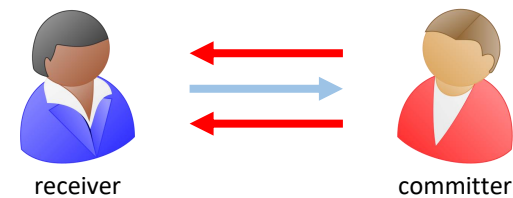
# Extraction by Rewinding



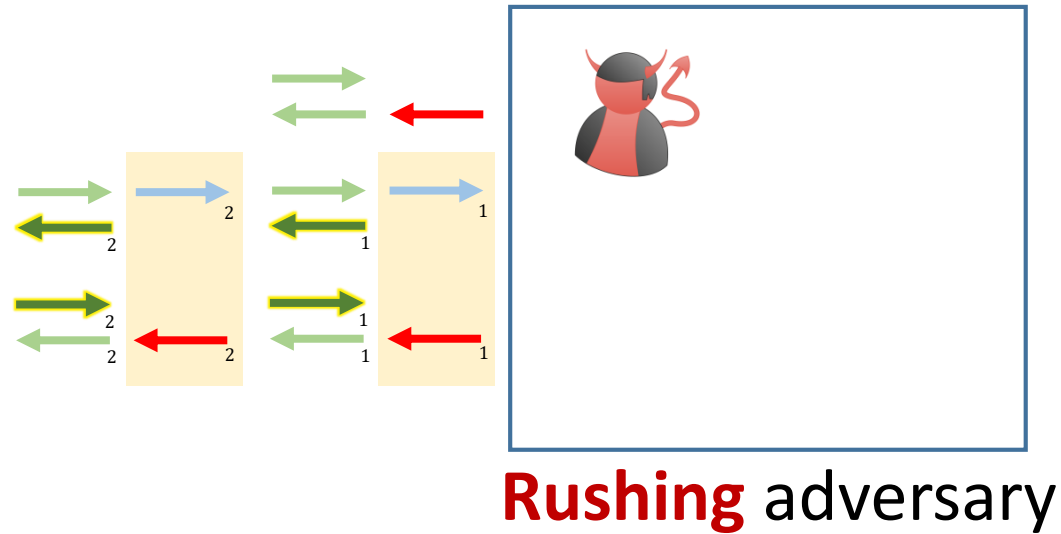
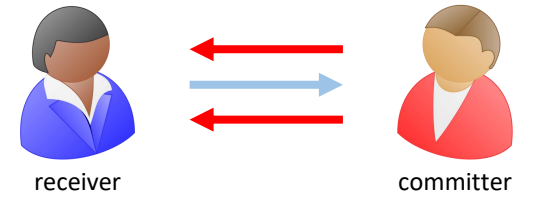
# Extraction by Rewinding



# Extraction by Rewinding



# Extraction by Rewinding



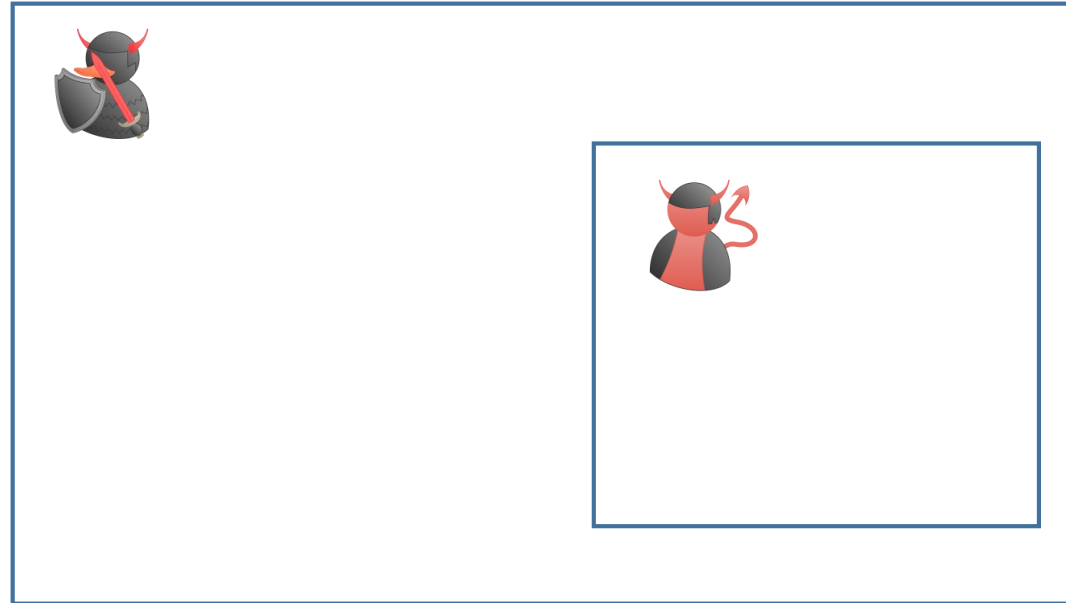
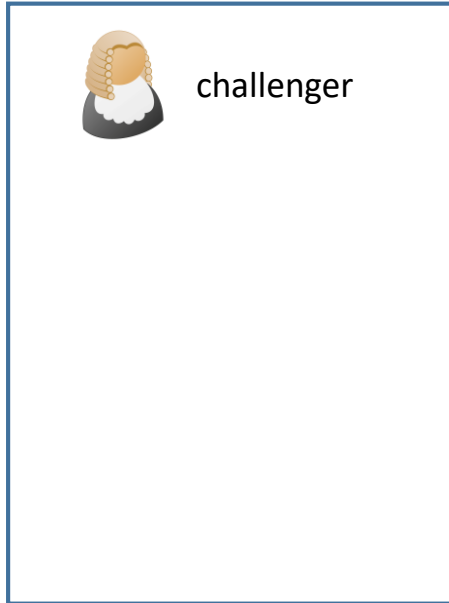
Is this **side effect of rewinding** a problem?



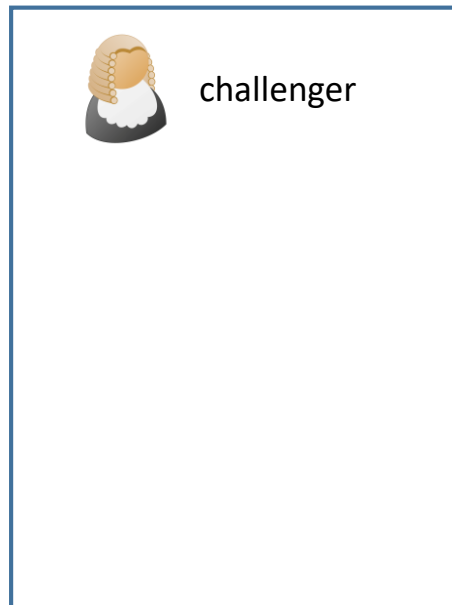


if  then 

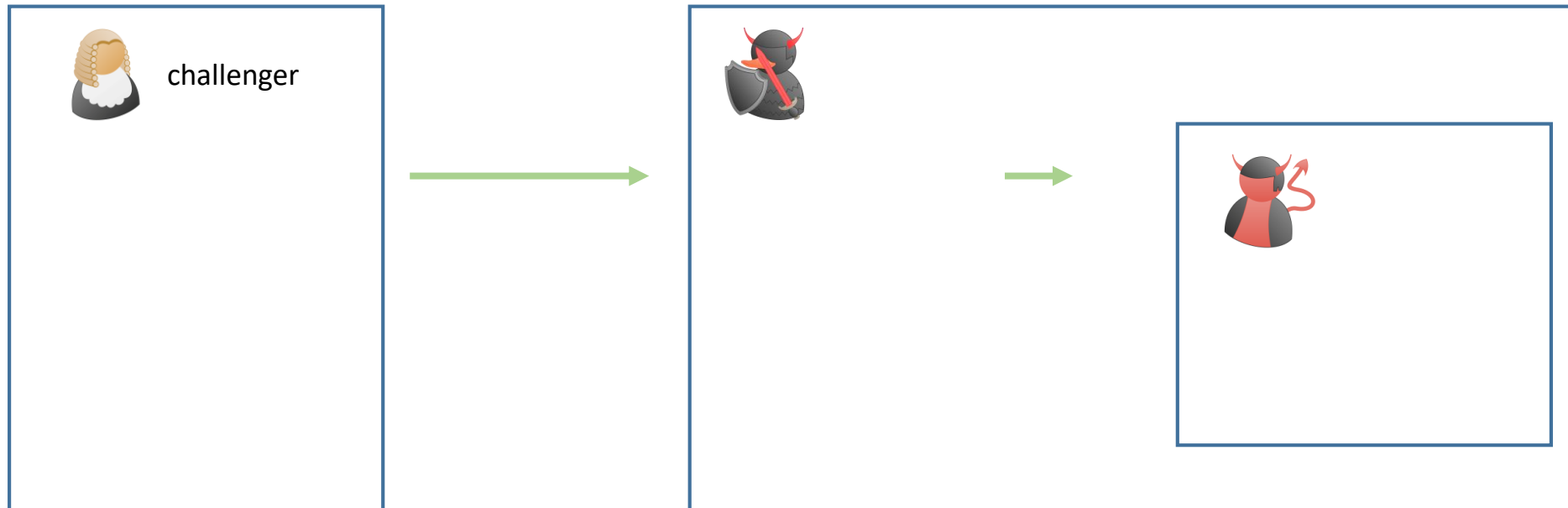
if  then 



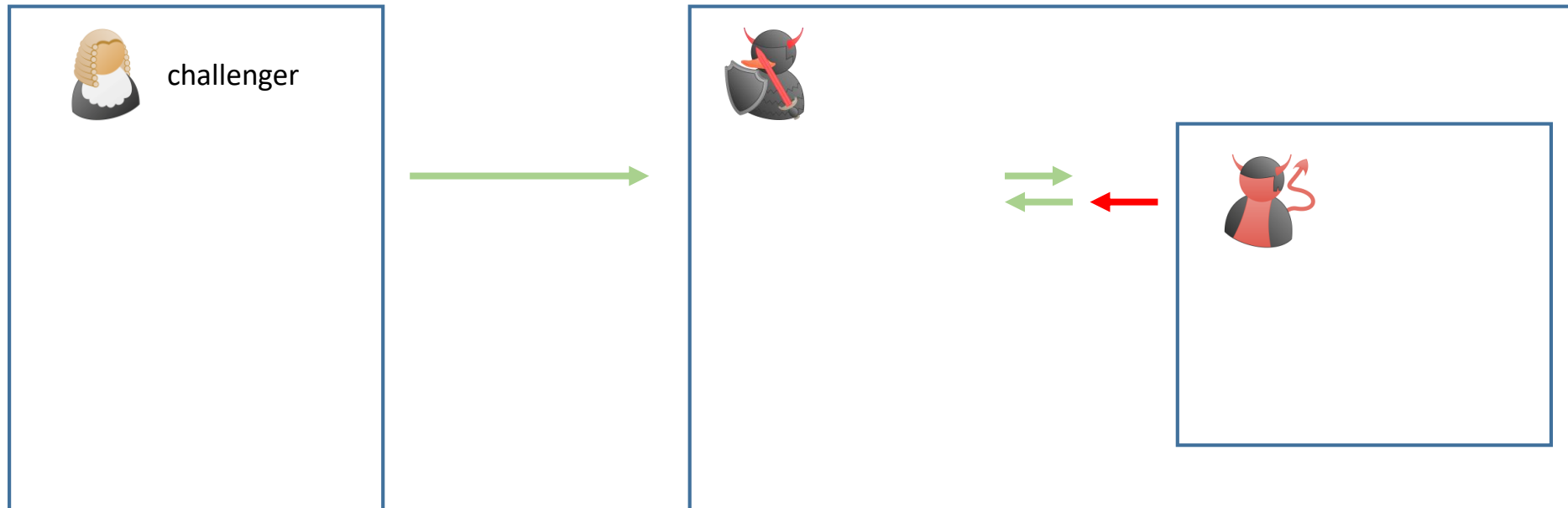
if  then 



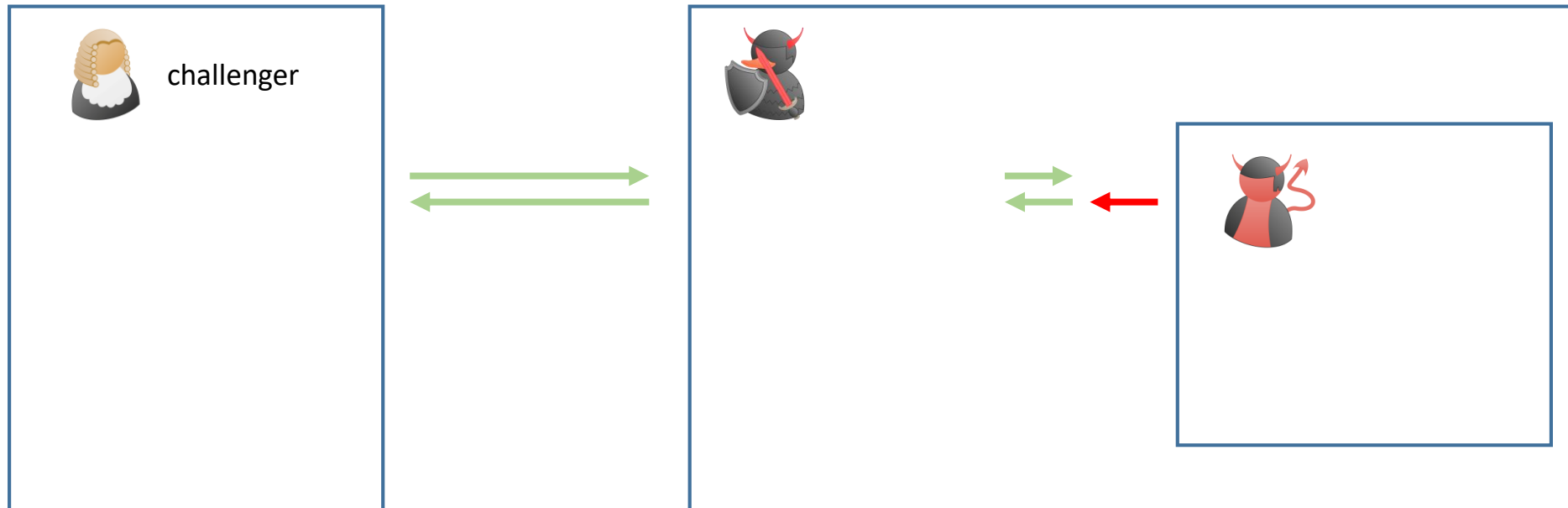
if  then 



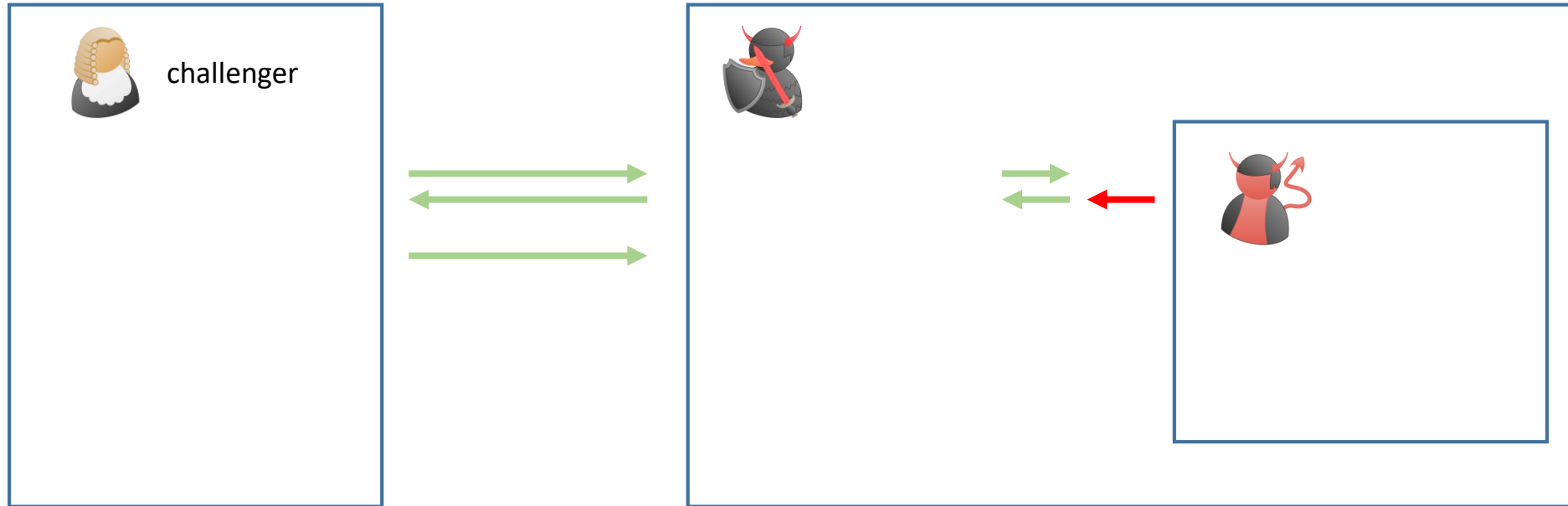
if  then 



if  then 

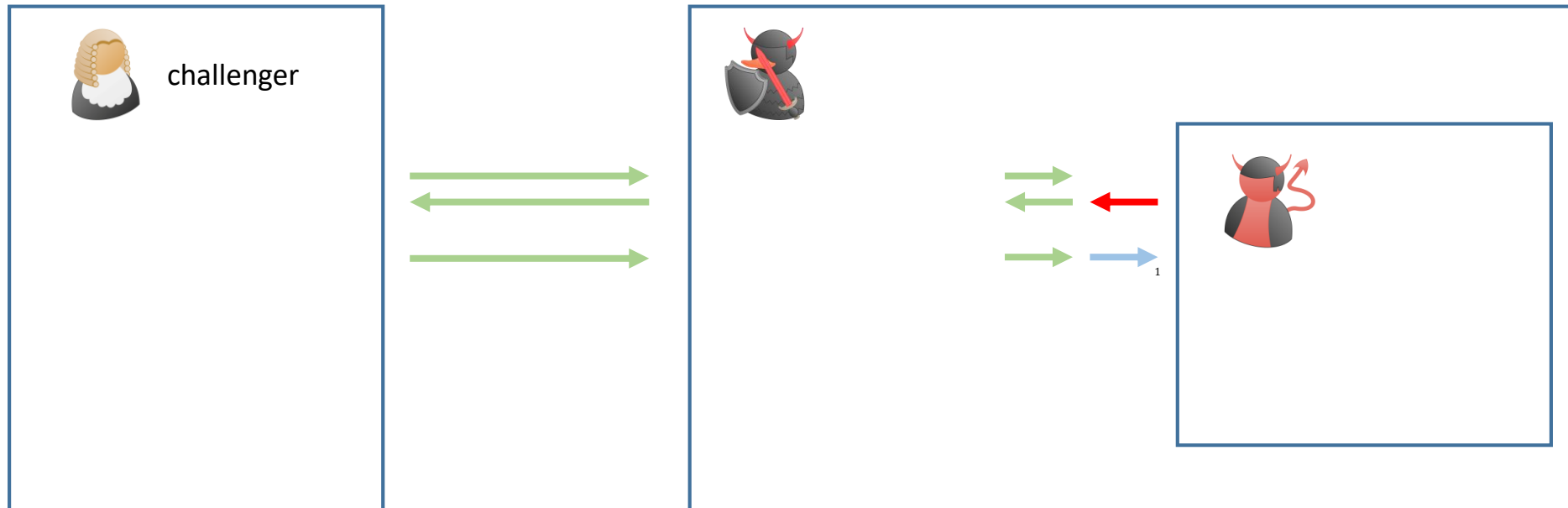


if  then 

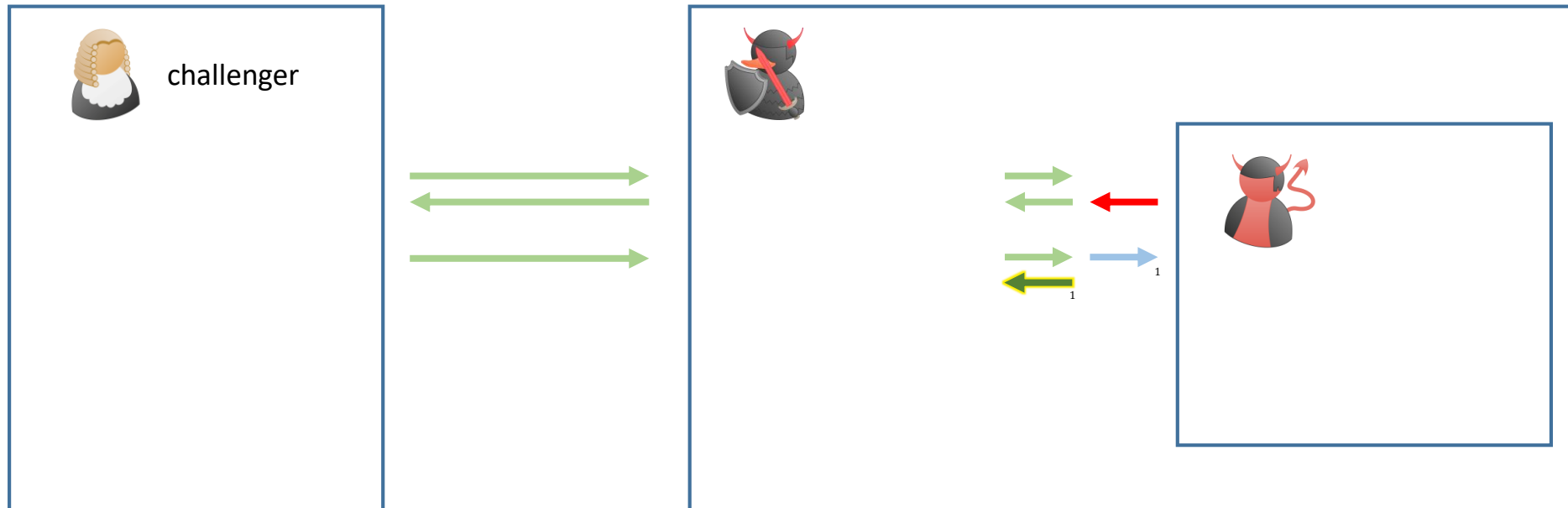




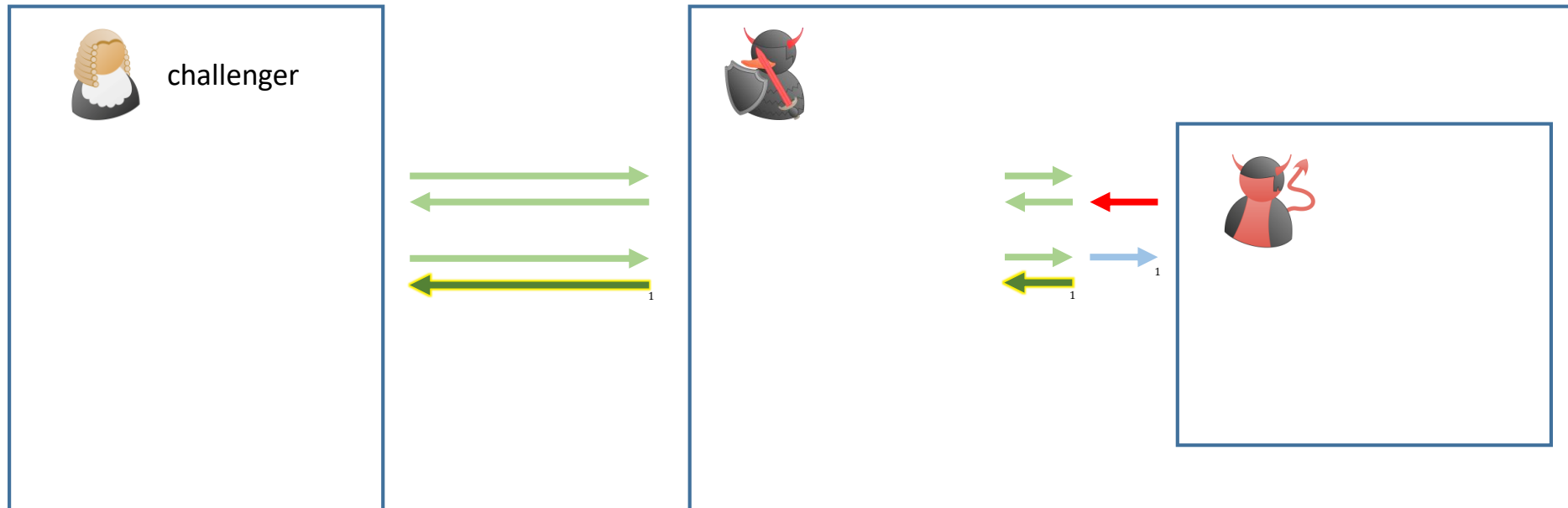
if  then 



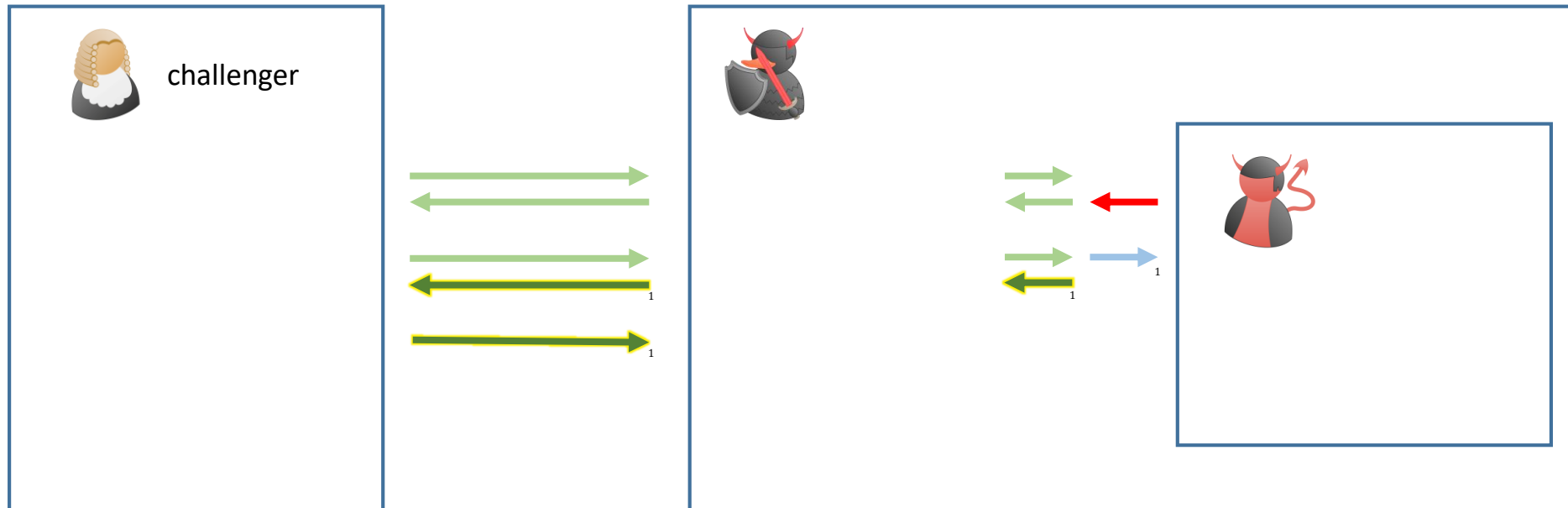
if  then 



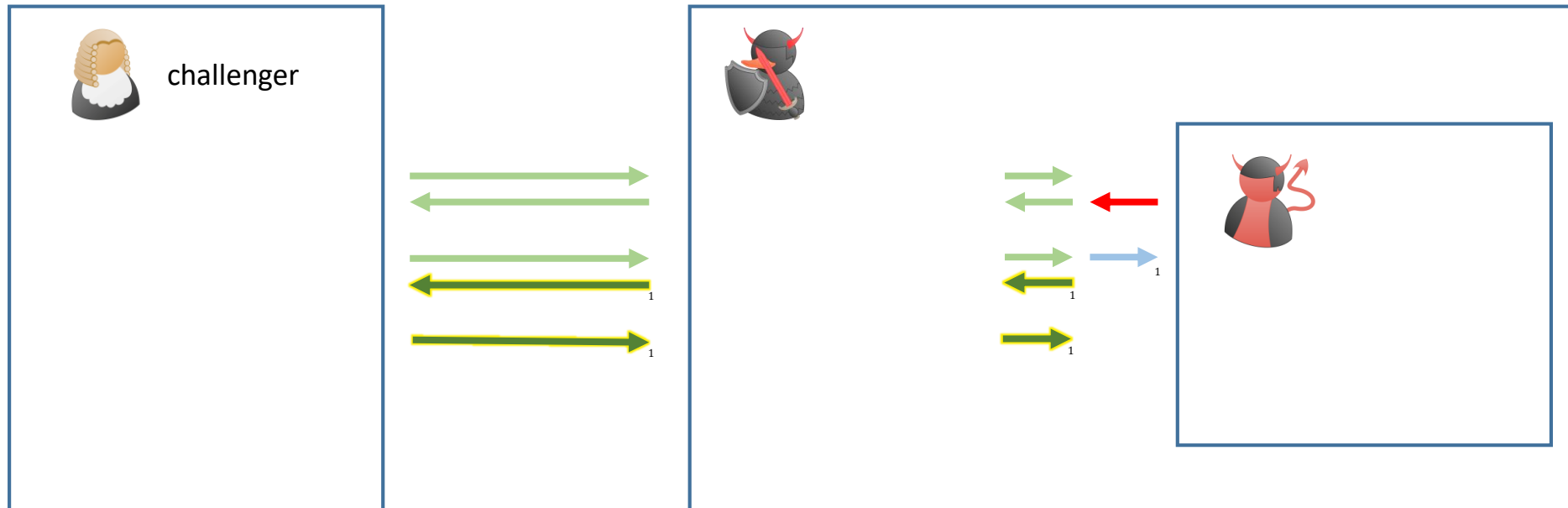
if  then 



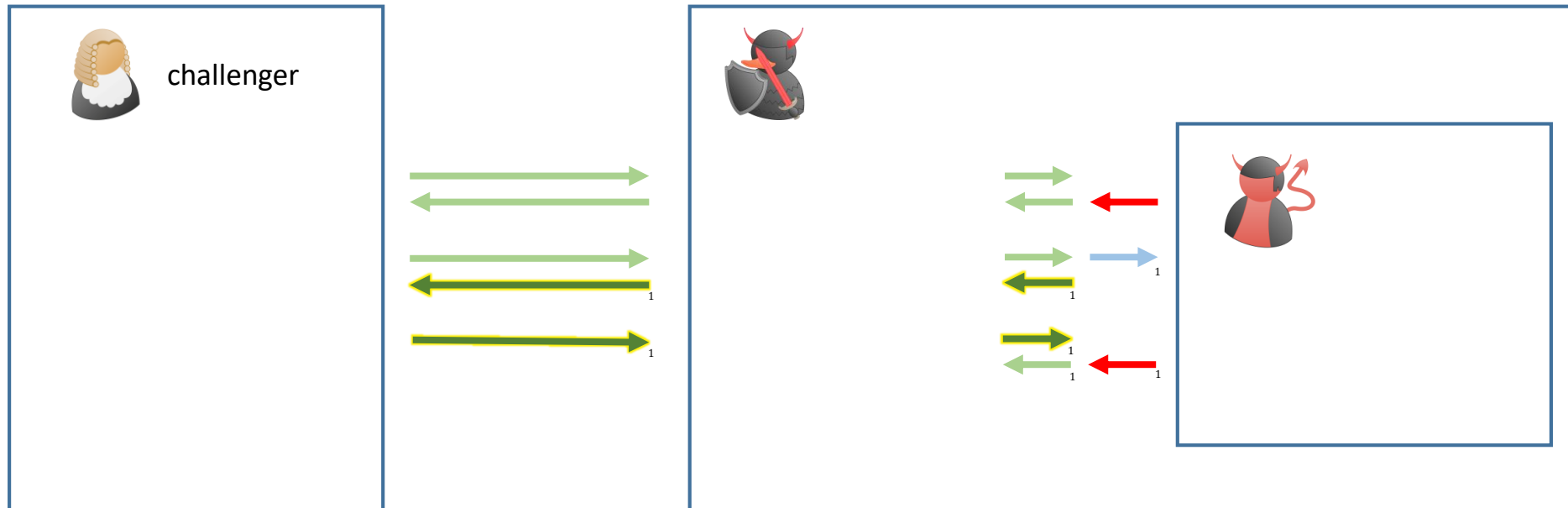
if  then 



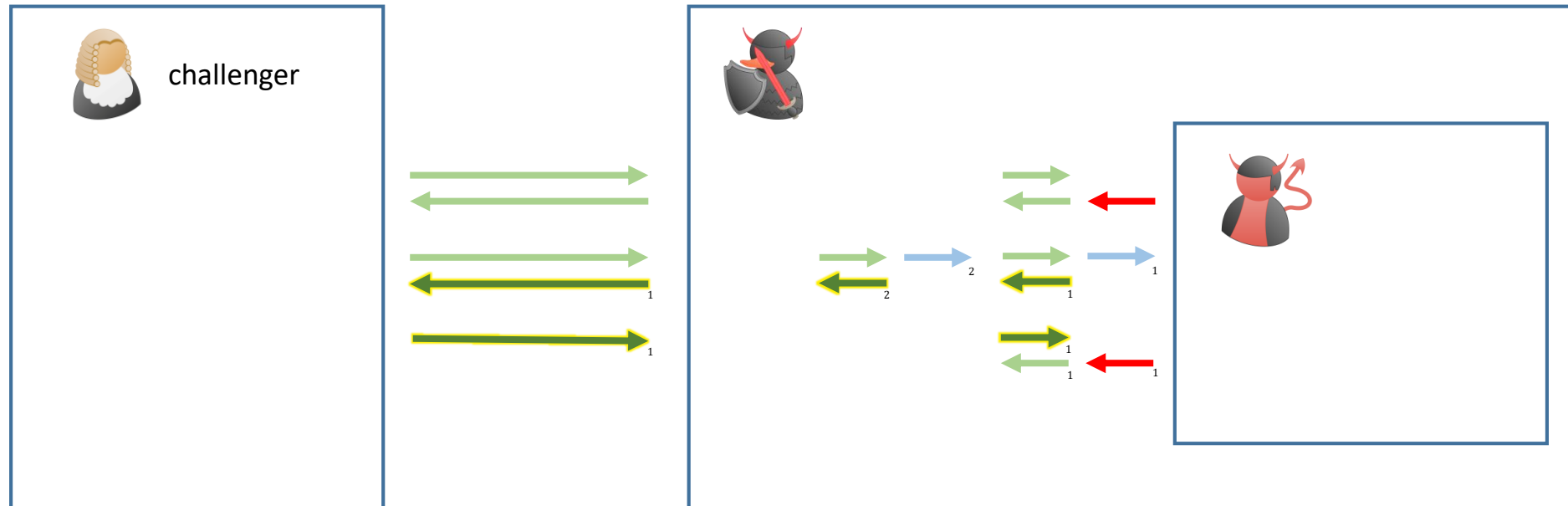
if  then 



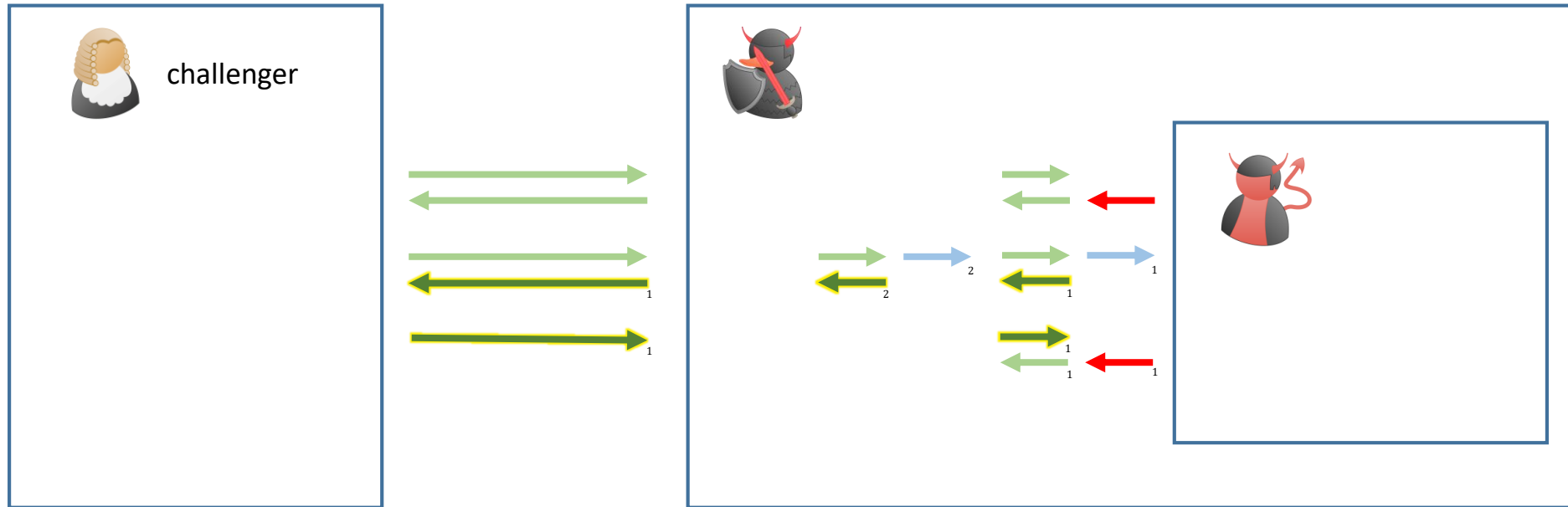
if  then 



if  then 



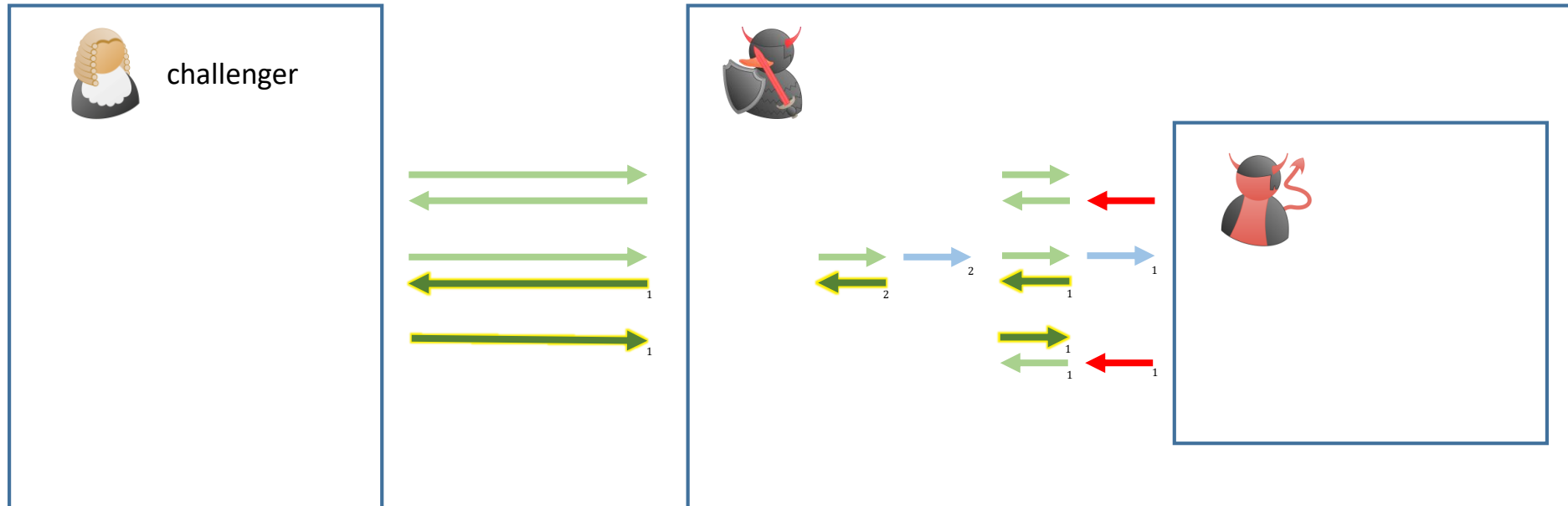
if  then 



How do we respond to  ?



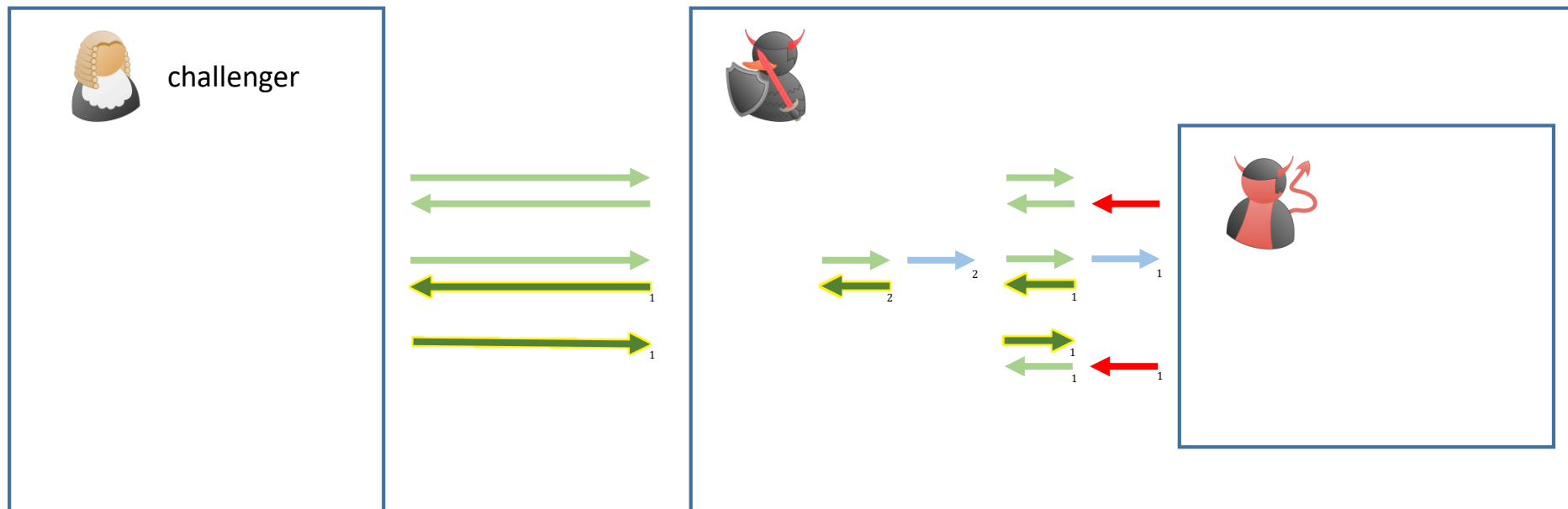
if  then 



How do we respond to  ?


How many responses do we need to extract?

if  then 

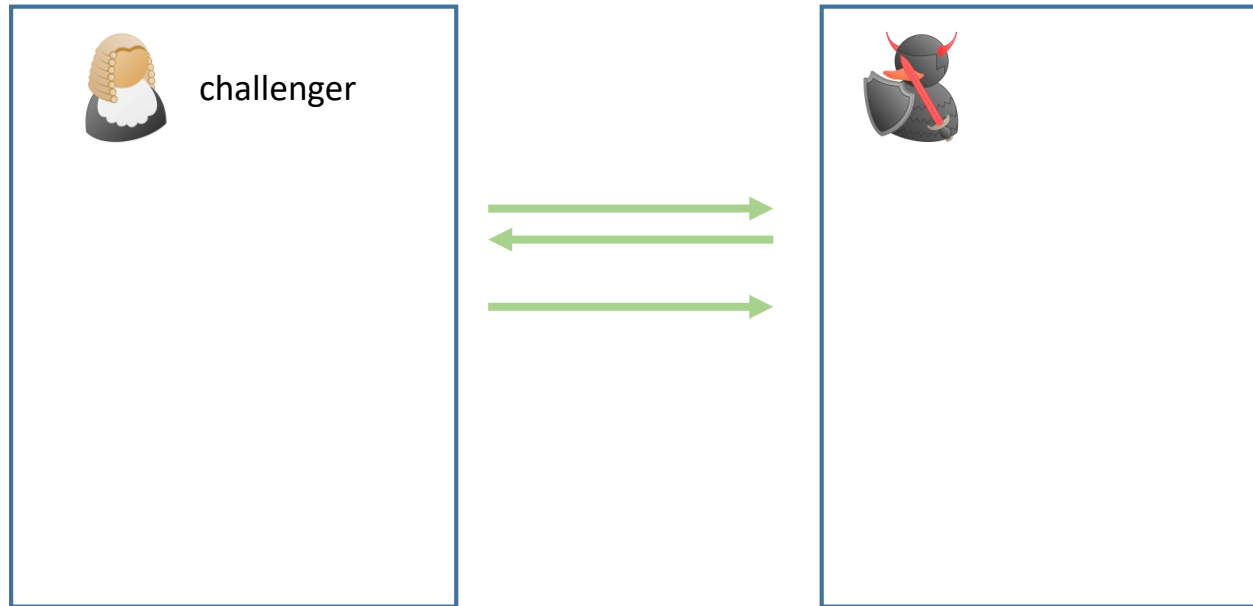


How do we respond to  ?

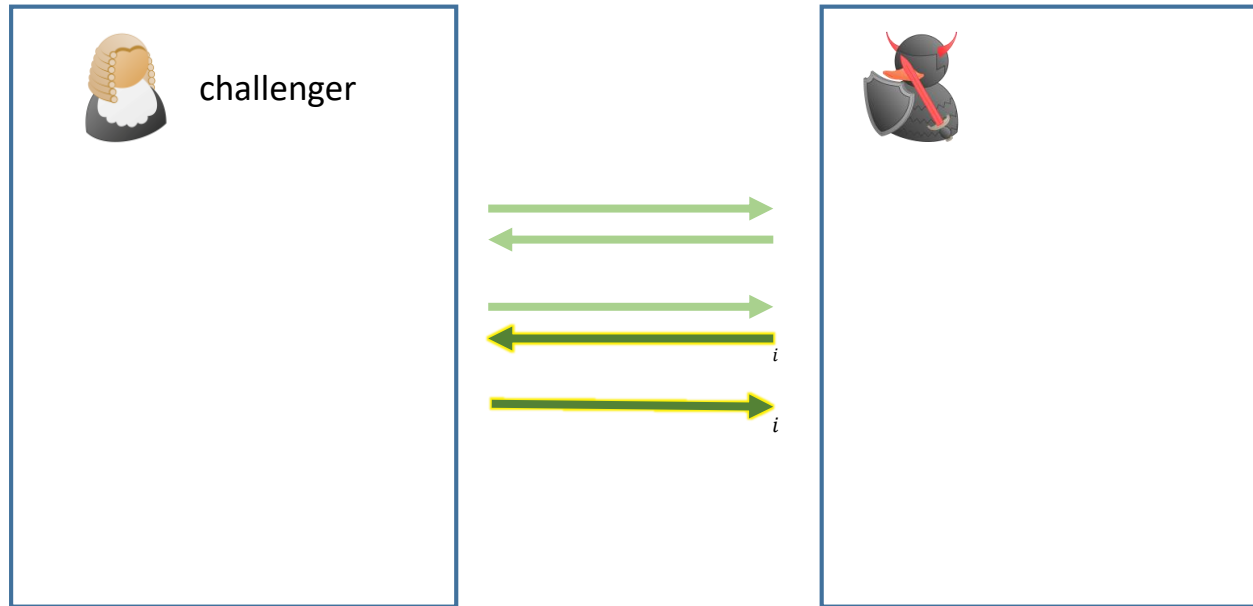
How many responses do we need to extract?

$$\Pr[\text{ wins}] \geq \text{noticeable}$$

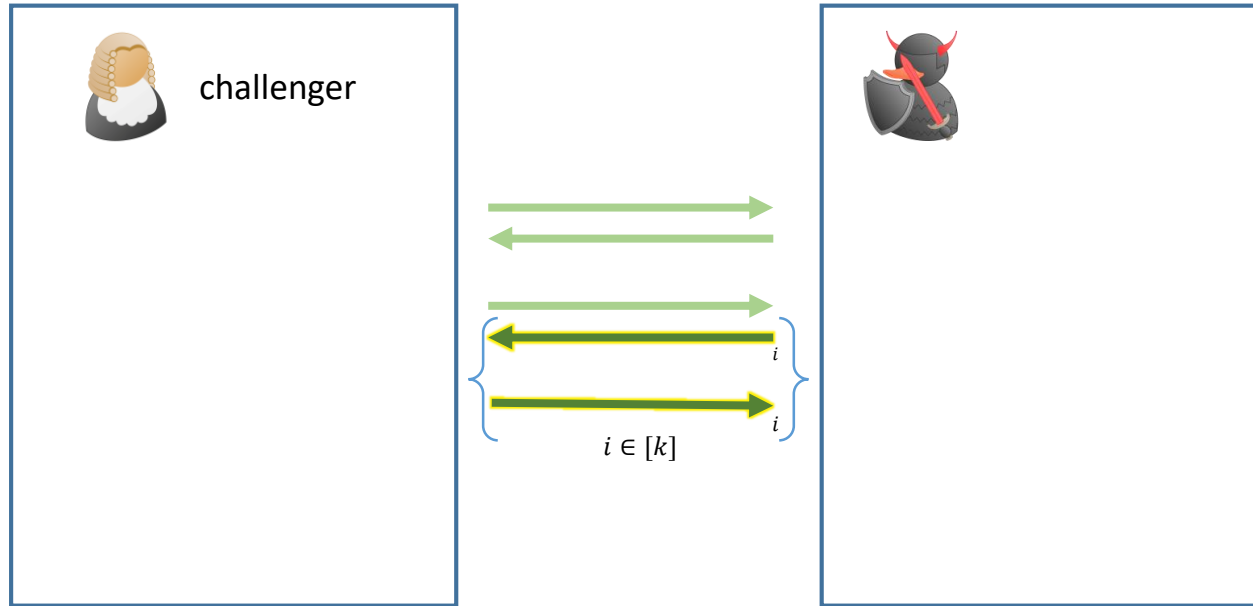
# $k$ -Bounded Rewind Security



# $k$ -Bounded Rewind Security



# $k$ -Bounded Rewind Security



# Bounded Rewind Secure Primitives

# Bounded Rewind Secure Primitives

require **multiple primitives** to be **bounded rewind secure**

# Bounded Rewind Secure Primitives

require **multiple primitives** to be **bounded rewind secure**

**bounds** (levels) stack up



# Bounded Rewind Secure Primitives

require **multiple primitives** to be **bounded rewind secure**

**bounds** (levels) stack up

4 bounded rewind secure round semi-malicious MPC?

# Bounded Rewind Secure Primitives

require **multiple primitives** to be **bounded rewind secure**

**bounds** (levels) stack up

4 bounded rewind secure round semi-malicious MPC OT?

# Bounded Rewind Secure Primitives

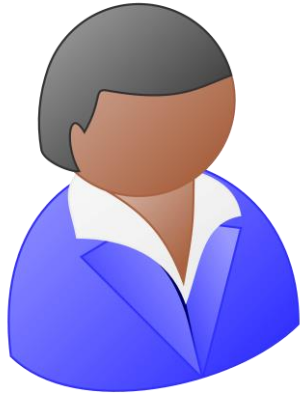
require **multiple primitives** to be **bounded rewind secure**

**bounds** (levels) stack up

4 bounded rewind secure round semi-malicious ~~MPC~~ OT?

Assuming **4 round OT**, there exists a **4 round rewind secure OT**.

# 4 round 1-Rewind Secure OT



receiver  
 *$b$*

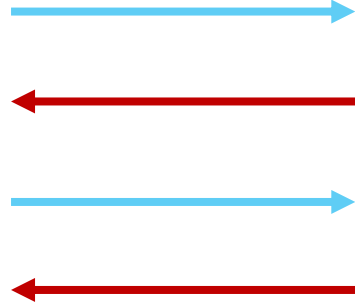


sender  
 *$x_0, x_1$*

# 4 round 1-Rewind Secure OT



receiver  
 $b$

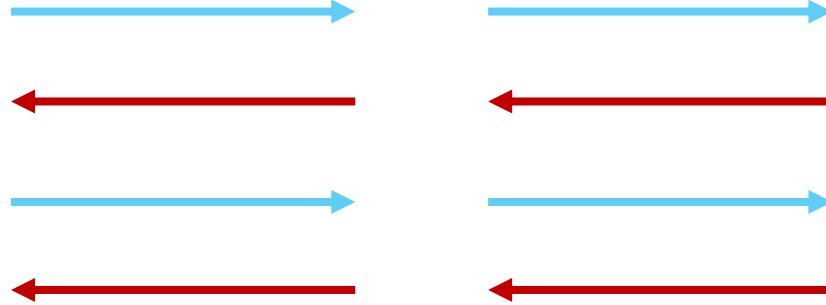


sender  
 $x_0, x_1$

# 4 round 1-Rewind Secure OT



receiver  
 $b$



sender  
 $x_0, x_1$

# 4 round 1-Rewind Secure OT

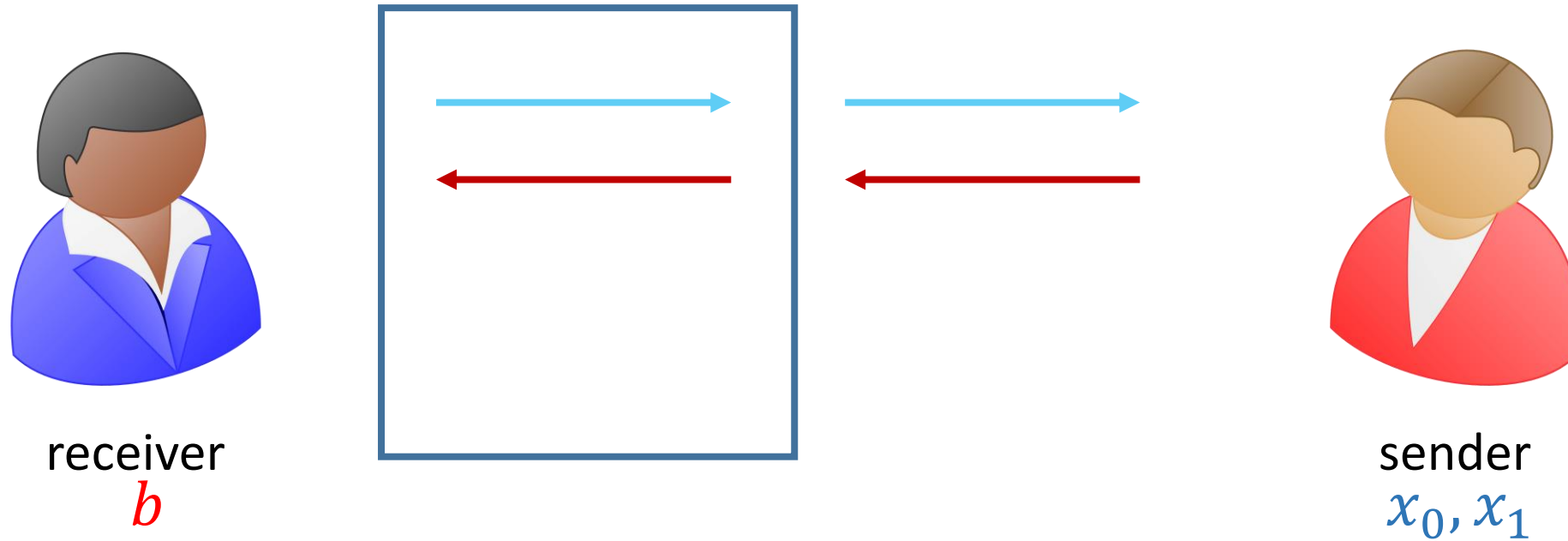


receiver  
 $b$



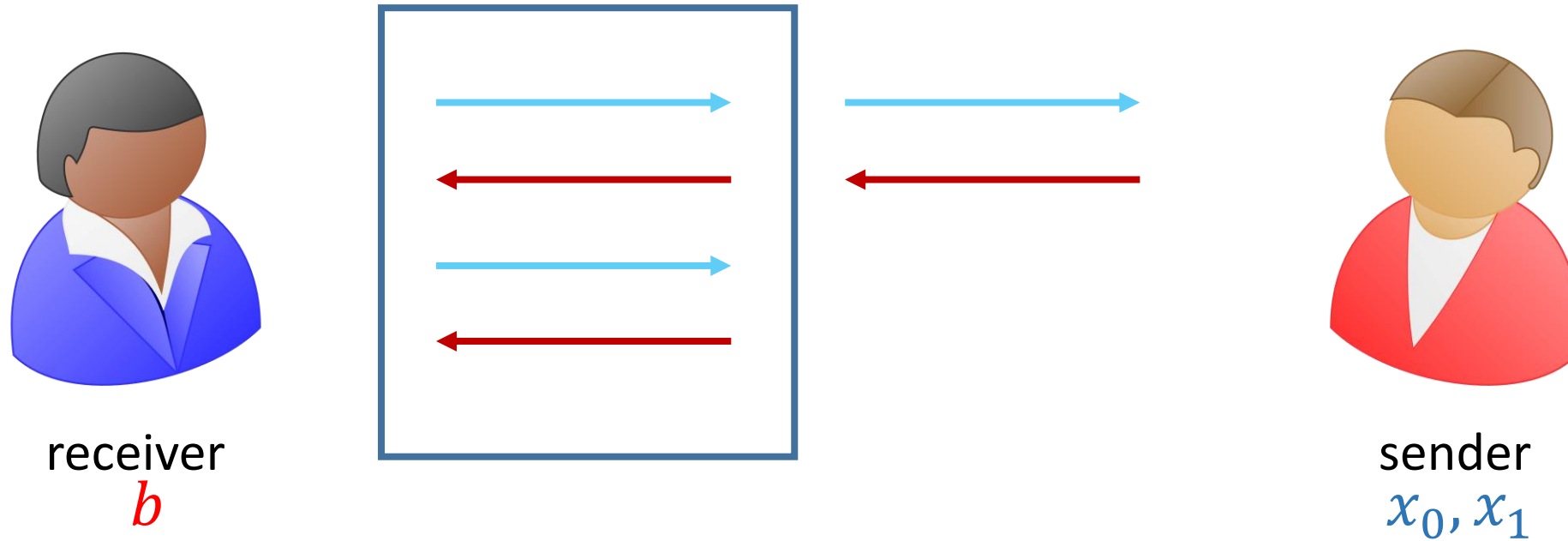
sender  
 $x_0, x_1$

# 4 round 1-Rewind Secure OT

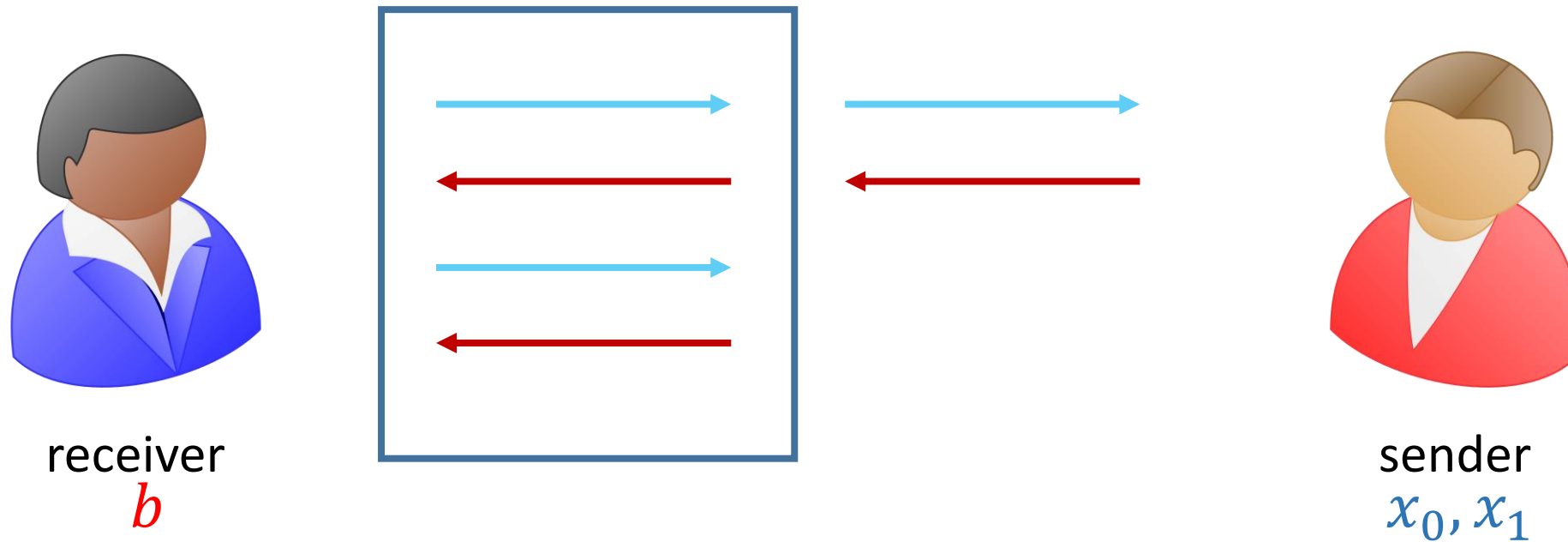




# 4 round 1-Rewind Secure OT

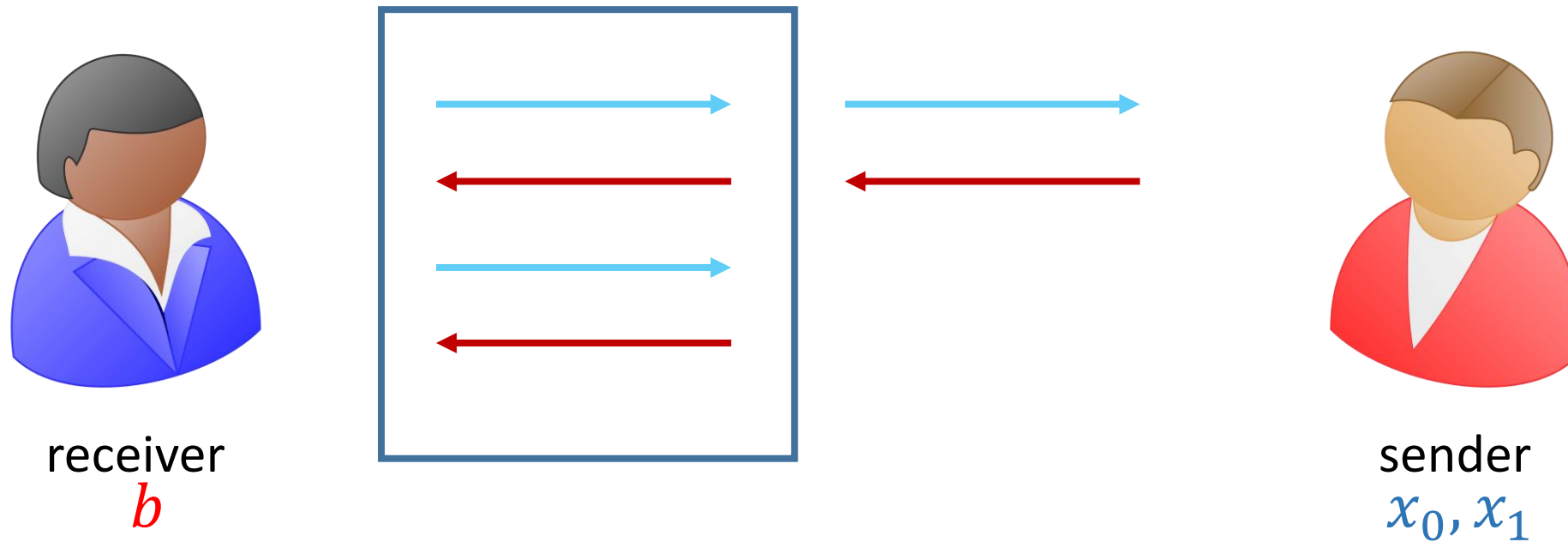


# 4 round 1-Rewind Secure OT



When rewinding, use each in a separate rewind.

# 4 round 1-Rewind Secure OT



When rewinding, use each in a separate rewind.

**Biased transcript!**

# 4 round 1-Rewind Secure OT



receiver

$$b = b_1 \oplus b_2$$



sender

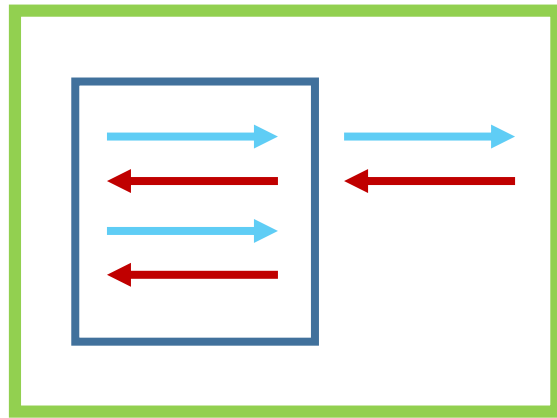
$x_0, x_1$

# 4 round 1-Rewind Secure OT



receiver

$$b = b_1 \oplus b_2$$



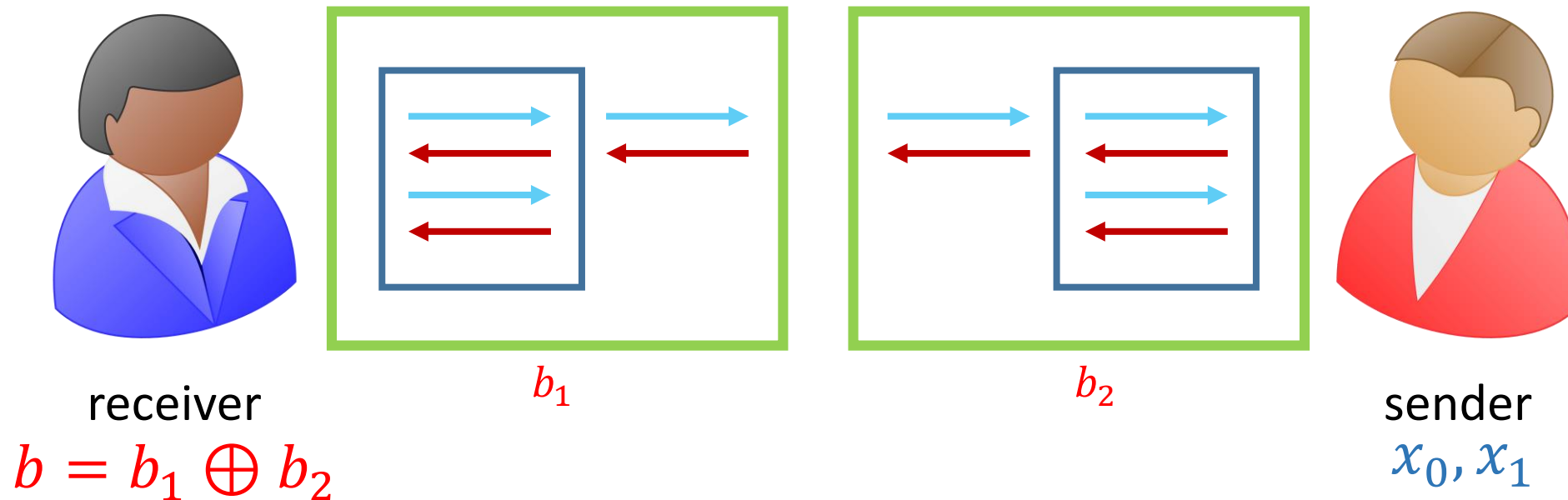
$b_1$



sender

$x_0, x_1$

# 4 round 1-Rewind Secure OT



Are we there yet?



Are we there yet?



Other challenges



Are we there yet?



Other challenges

non-malleability

Are we there yet?



## Other challenges

non-malleability



Are we there yet?



## Other challenges

non-malleability



Are we there yet?



## Other challenges

non-malleability



Are we there yet?



## Other challenges

non-malleability



Are we there yet?



## Other challenges

non-malleability



simulation-soundness [DDN91,Sah99]

Are we there yet?



## Other challenges

non-malleability

more components in the final protocol

# Thank you. Questions?

Arka Rai Choudhuri

[achoud@cs.jhu.edu](mailto:achoud@cs.jhu.edu)

[ia.cr/2019/216](https://ia.cr/2019/216)