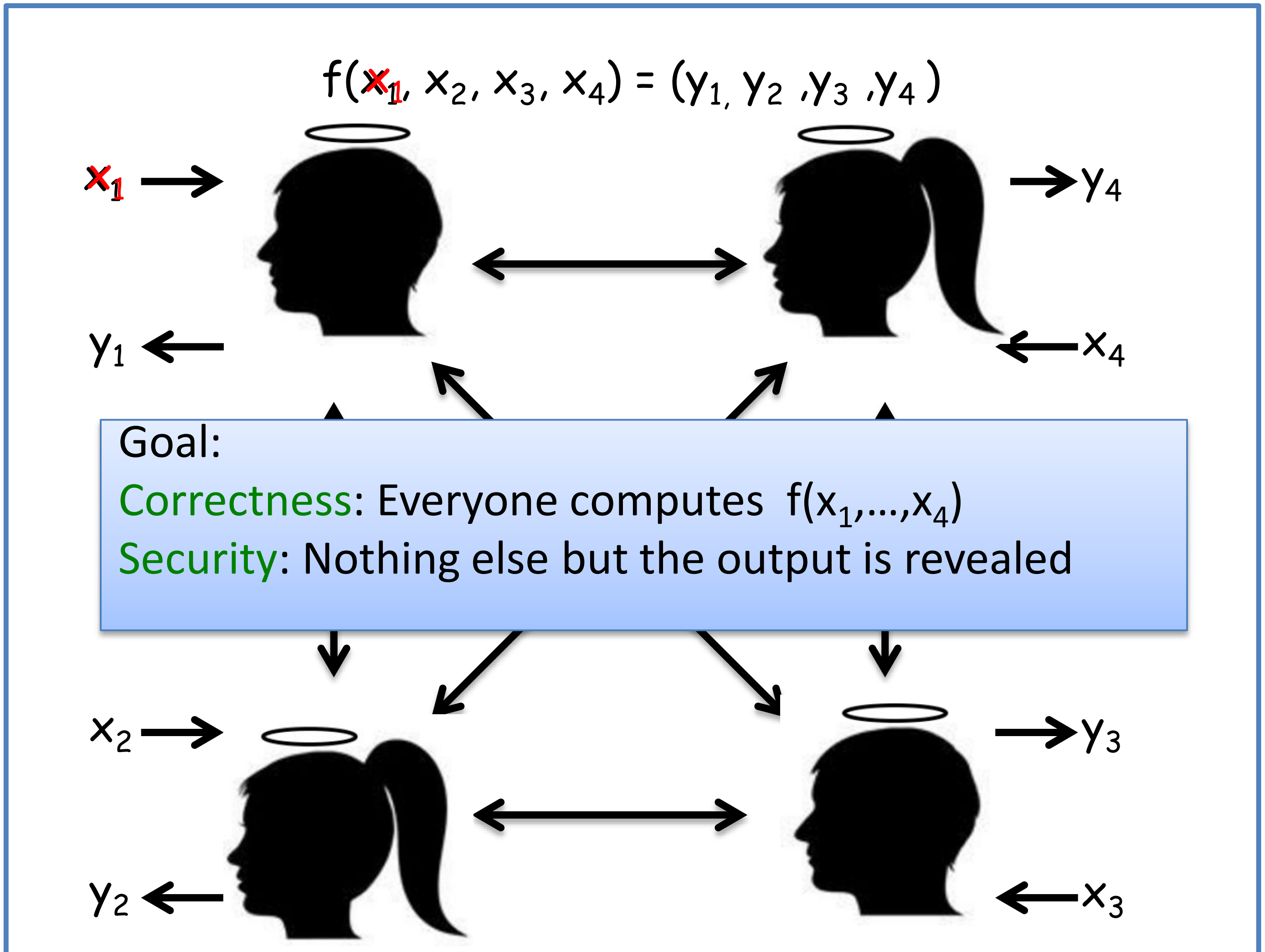
The Exact Round Complexity of Secure Computation

Antigoni Polychroniadou (Aarhus University)
joint work with
Sanjam Garg, Pratyay Mukherjee (UC Berkeley), Omkant Pandey (Drexel University)

Background: Secure Multi-Party Computation



Goal:

Correctness: Everyone computes $f(x_1,\ldots,x_4)$

Security: Nothing else but the output is revealed

Adversary:

PPT

Malicious

Static

Motivating Questions

Lower bounds on the round complexity of secure protocols.

Construct **optimal** round secure protocols.

State of the Art: Information-Theoretic Setting

Communication Complexity	Round Complexity
$O(n\|C\|)$	$O(depth_C)$

State of the Art: Information-Theoretic Setting

Communication Complexity	Round Complexity
$\Omega(n\|C\|)$ [DN**P**R16]	$\Omega(\text{depth}_C)$ [DN**P**R16]

Novel approach must be found to construct **O(1)** round protocols
(that beat the complexities of BGW, CCD, GMW, SPDZ etc.)

State of the Art: Computational Setting

Communication Complexity	Round Complexity	
<<|C|	2PC	MPC

FHE

State of the Art: Computational Setting

Round Complexity	
2PC	MPC
5 rounds [KO04,ORS15]	O(1)*

No CRS
No Preprocessing

*[BMR90,KOS03,Pas04,DI05,DI06,PPV08,IPS08,Wee10,Goy11,LP11,GLOV12]

State of the Art: Computational Setting

Round Complexity	
2PC	MPC
5 rounds [KO04,ORS15]	O(1)

What is the exact round complexity of secure MPC?

Standard Communication Model for MPC

Simultaneous Message Exchange Channel

Standard Communication Model for MPC

Standard Communication Model for MPC

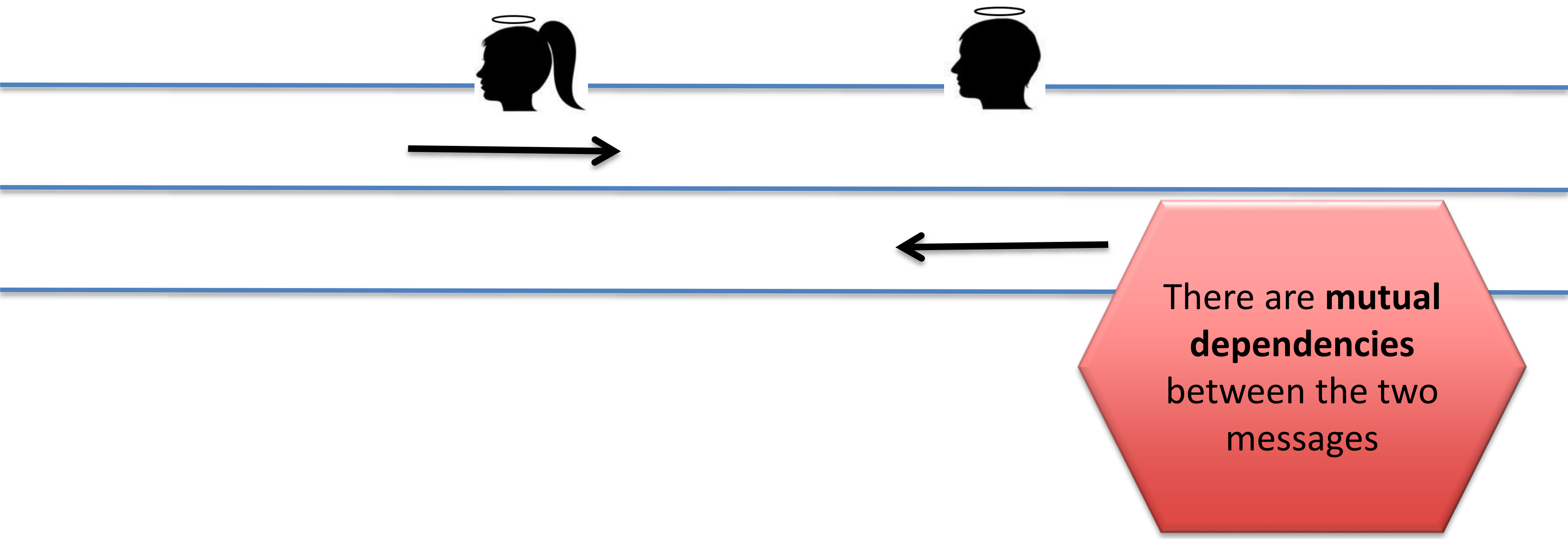
Simultaneous Message Exchange Channel

Standard Communication Model for MPC

Simultaneous Message Exchange Channel

Communication Model for 2PC

Non-Simultaneous Message Exchange Channel



State of the Art: Computational Setting

Round Complexity	
2PC	MPC
5 rounds [KO04]	O(1)

What is the exact round complexity of secure **MPC**?

How many simultaneous message exchange rounds are necessary for **2PC**?

Our Results

Round Complexity	
2PC	MPC
5 rounds [KO04]	O(1)

- **(3-round Impossibility)**:

There does **not** exist a **3-round protocol** for the **two-party coin-flipping** functionality.

Our Results

Round Complexity	
2PC	MPC
max(4,k+1)[1]	O(1)

[1] k-round NMCOM

Suppose that there exists a k-round NMCOM scheme; then

- **(2PC)**: there exists a **max(4, k + 1)-round** protocol for securely realizing every two-party functionality.

The use of NMCOM is not a coincidence [LPV09,Goy11,LP11,LPTV10,GLOV12]

Our Results

Round Complexity	
2PC	MCF*
max(4,k+1)[1]	max(4,k+1)

[1] k-round NMCOM

Suppose that there exists a k-round NMCOM scheme; then

- **(2PC)**: there exists a **max(4, k + 1)-round** protocol for securely realizing every two-party functionality;
- **(MPC)**: there exists a **max(4, k + 1)-round** protocol for securely realizing the multi-party coin-flipping functionality.

Our Results

Round Complexity	
2PC	MCF*
max(4,k+1)[1]	max(4,k+1)

[1] k-round NMCOM

Suppose that there exists a k-round NMCOM scheme; then

- **(2PC)**: there exists a **max(4, k + 1)-round** protoc -
  party functionality;
- **(MPC)**: there exists a **max(4, k + 1)-round** proto -
  party coin-flipping functionality.

Four rounds are both **necessary and sufficient** for both the results based on 3-round NMCOMs [PPV08,GPR16,COSV16].

Outline

1. Lower bound on the two-party coin-flipping.
2. 4-round 2PC protocol.

Our Results

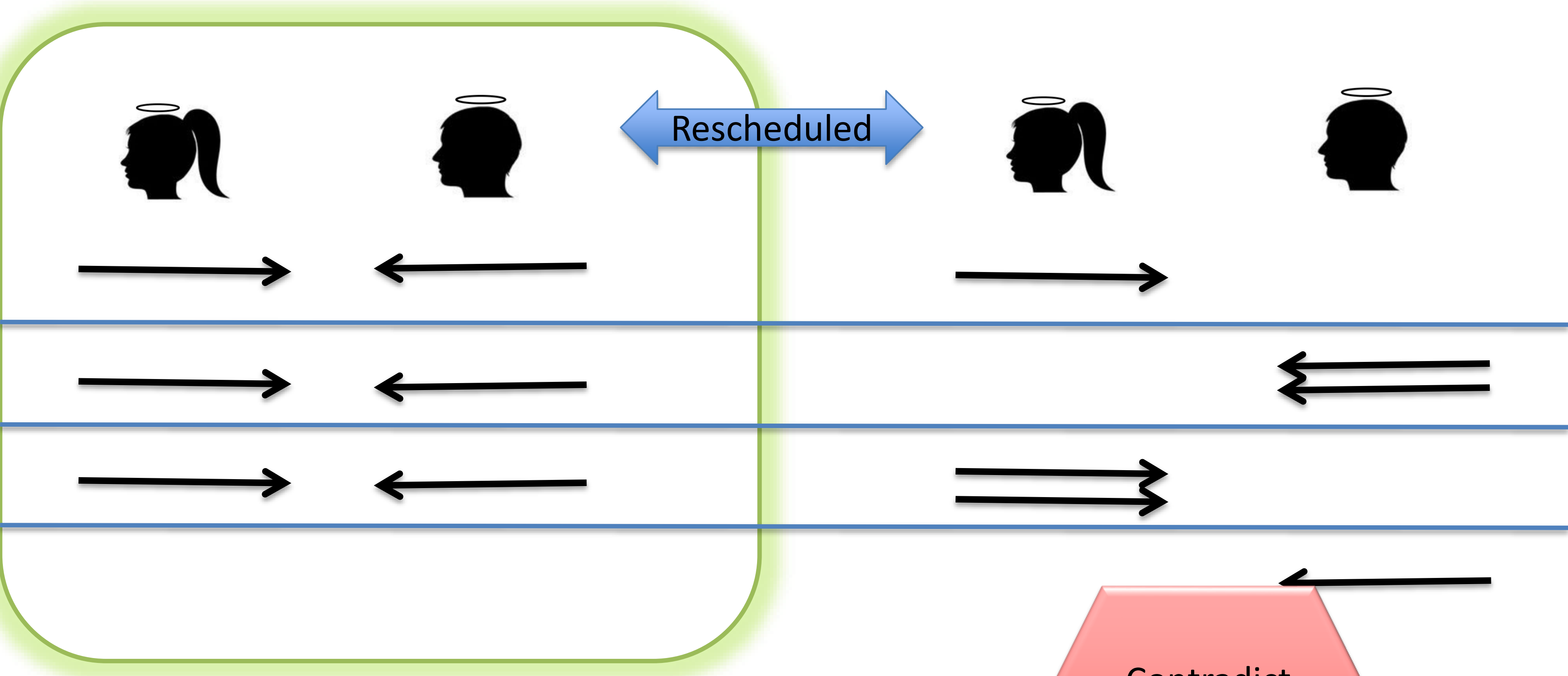
Theorem 1. There does **not** exist a **3-round protocol** for the **two-party coin-flipping** functionality

- for tossing $\omega(\log \lambda)$ coins,
- with a black-box simulation,
- in the simultaneous message exchange model.

where λ is the security parameter

Proof (sketch)

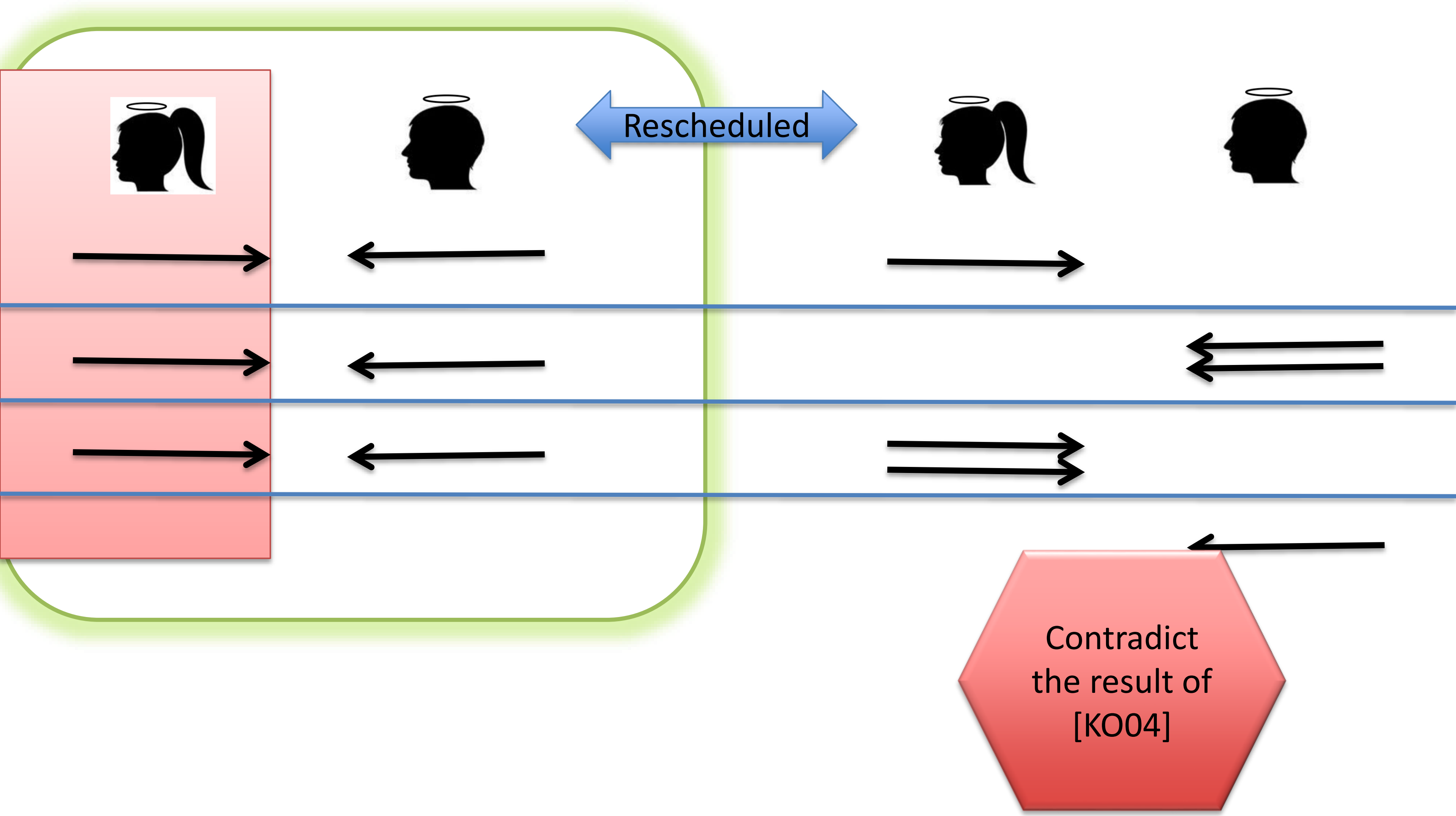
Suppose that there exists a protocol which realizes simulatable coin-flipping in 3 rounds.



Contradict the result of [KO04]

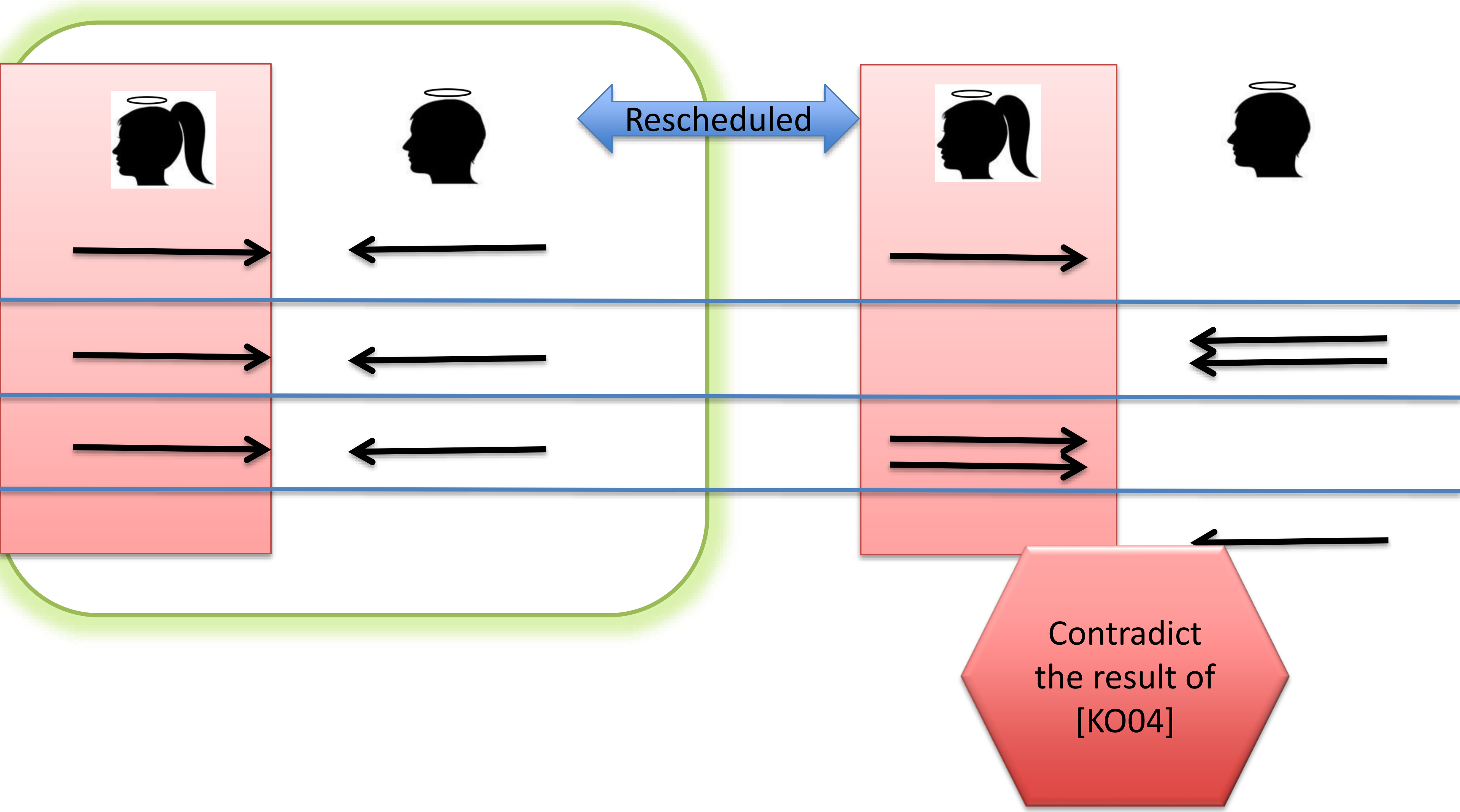
Proof (sketch)

Suppose that there exists a protocol which realizes simulatable coin-flipping in 3 rounds.



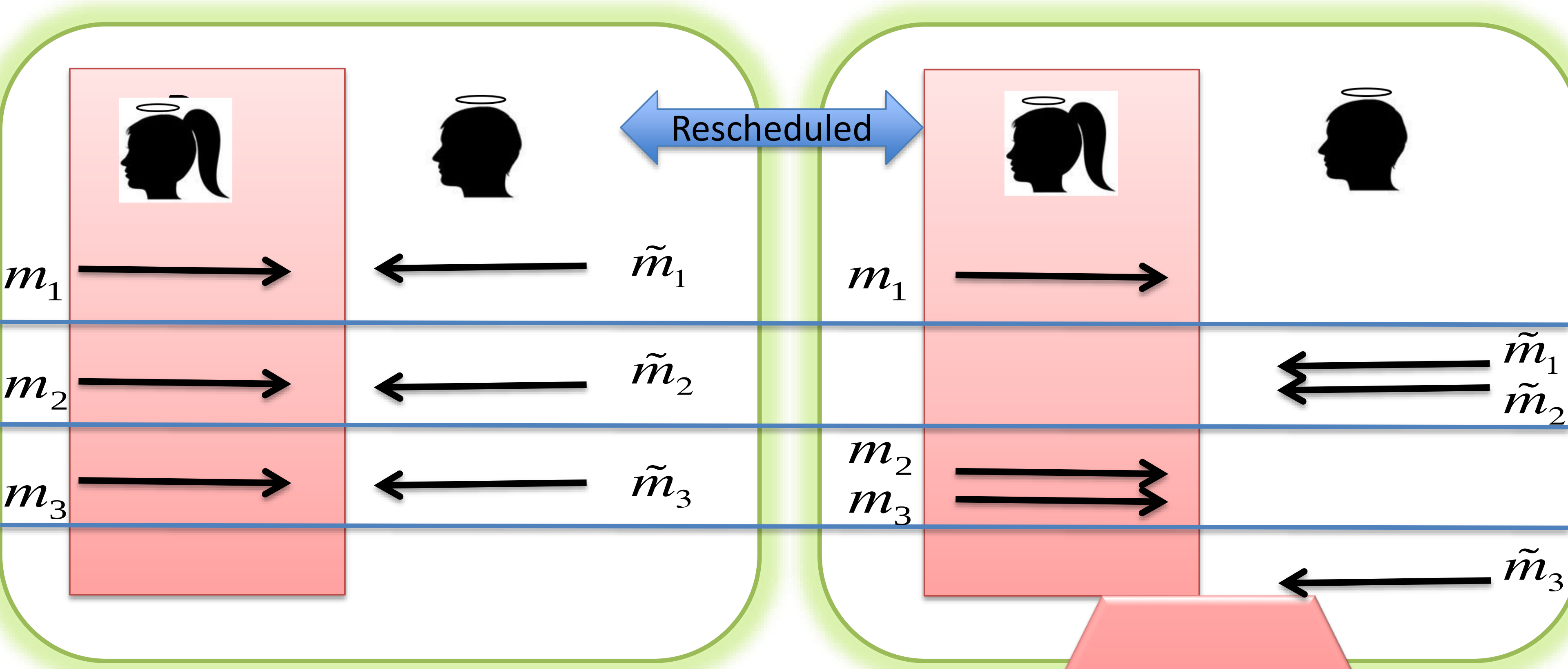
Proof (sketch)

Suppose that there exists a protocol which realizes simulatable coin-flipping in 3 rounds.



Proof (sketch)

Suppose that there exists a protocol which realizes simulatable coin-flipping in 3 rounds.

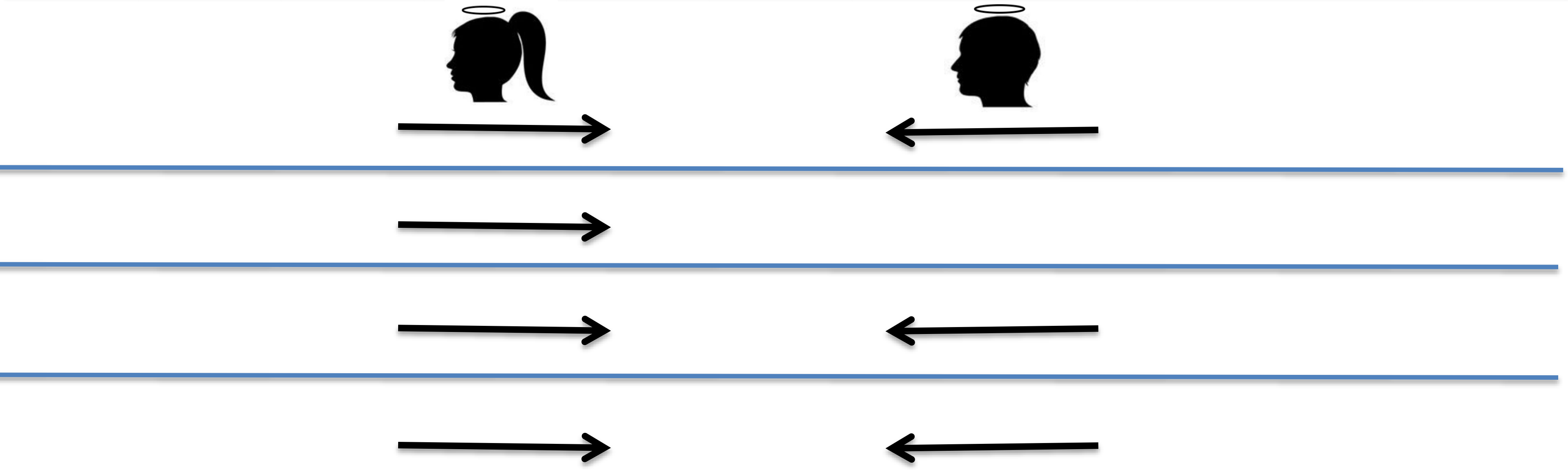


Contradict the result of [KO04]

Our Results

Theorem 2. There does **not** exist a **4-round protocol** for the **two-party coin-flipping** functionality

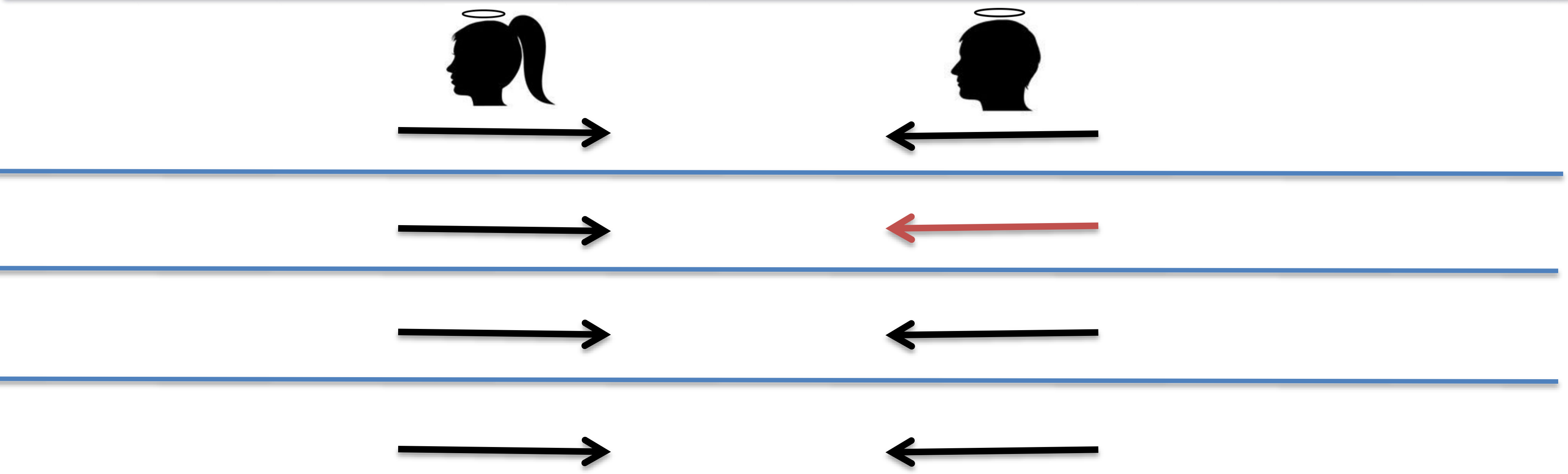
- for tossing ω(log λ) coins,
- with a black-box simulation,
- in the simultaneous message exchange model,
- with **at least one unidirectional round.**



Our Results

Theorem 2. There does **not** exist a **4-round protocol** for the **two-party coin-flipping** functionality

- for tossing ω(log λ) coins,
- with a black-box simulation,
- in the simultaneous message exchange model,
- with **at least one unidirectional round.**

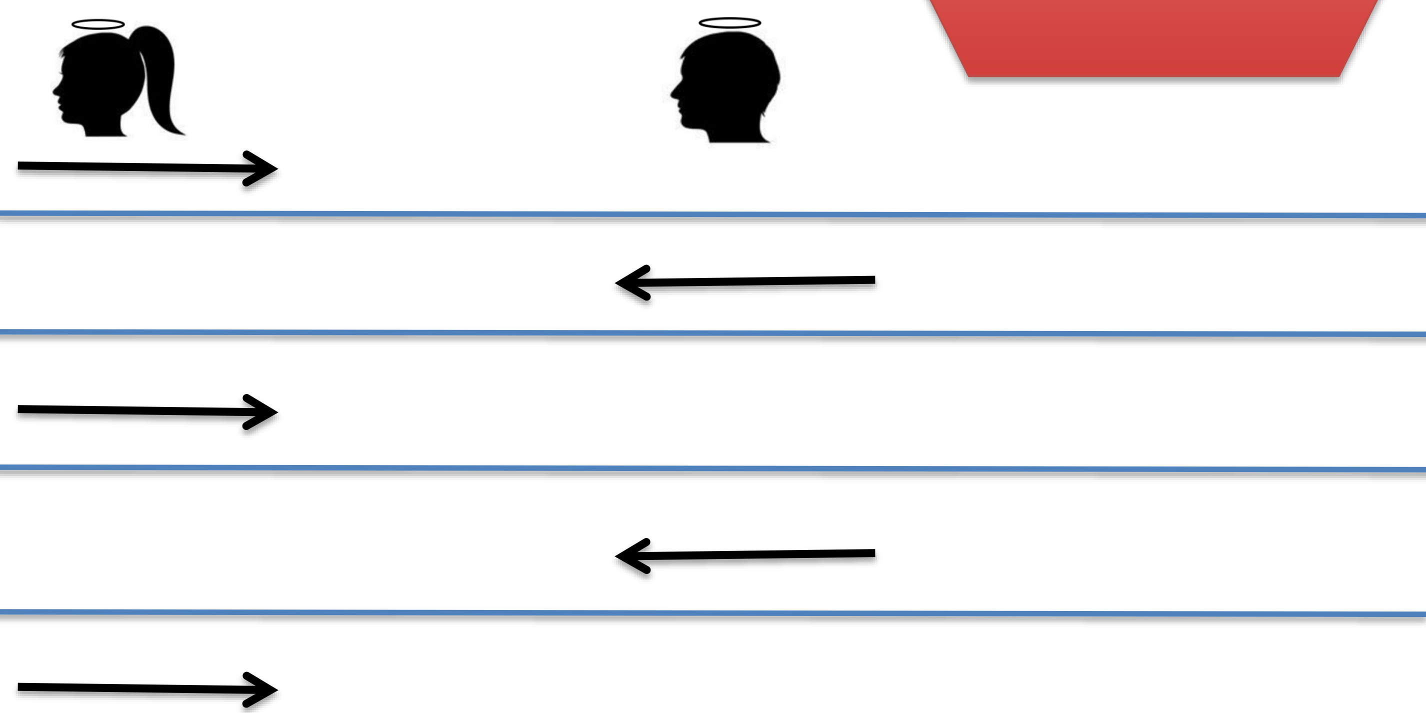


Our Approach for 2PC

Starting point: Katz-Ostrovsky (KO) protocol [KO04] which is a 4-round protocol for **only** one-sided functionalities and 5-rou… …d functionalities.

Is it still **5** rounds with simultaneous transmission?

5-round [KO04]:

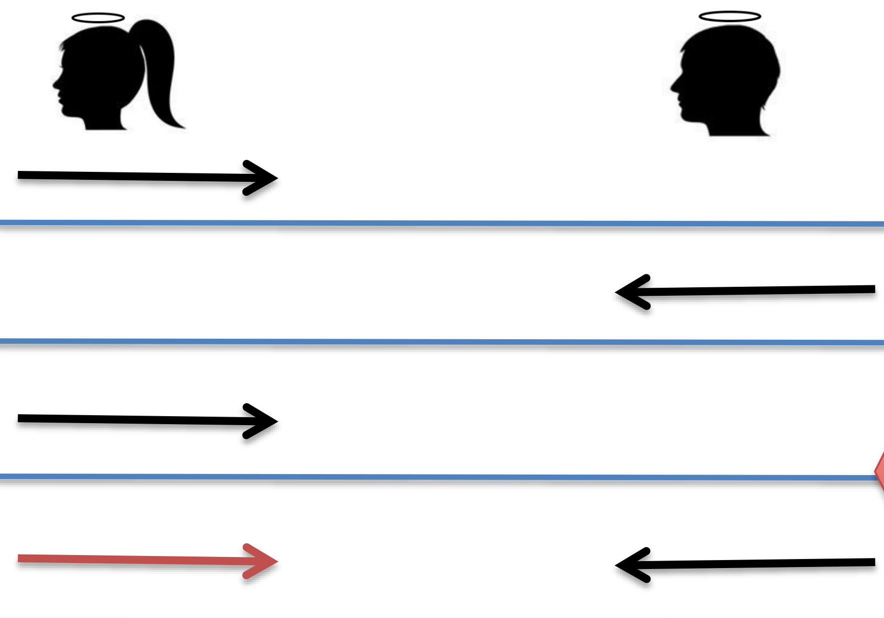


Our Approach for 2PC

Starting point: Katz-Ostrovsky (KO) protocol [KO04] which is a 4-round protocol for **only** one-sided functionalities and 5-rou d functionalities.

Is it still **5** rounds with simultaneous transmission?

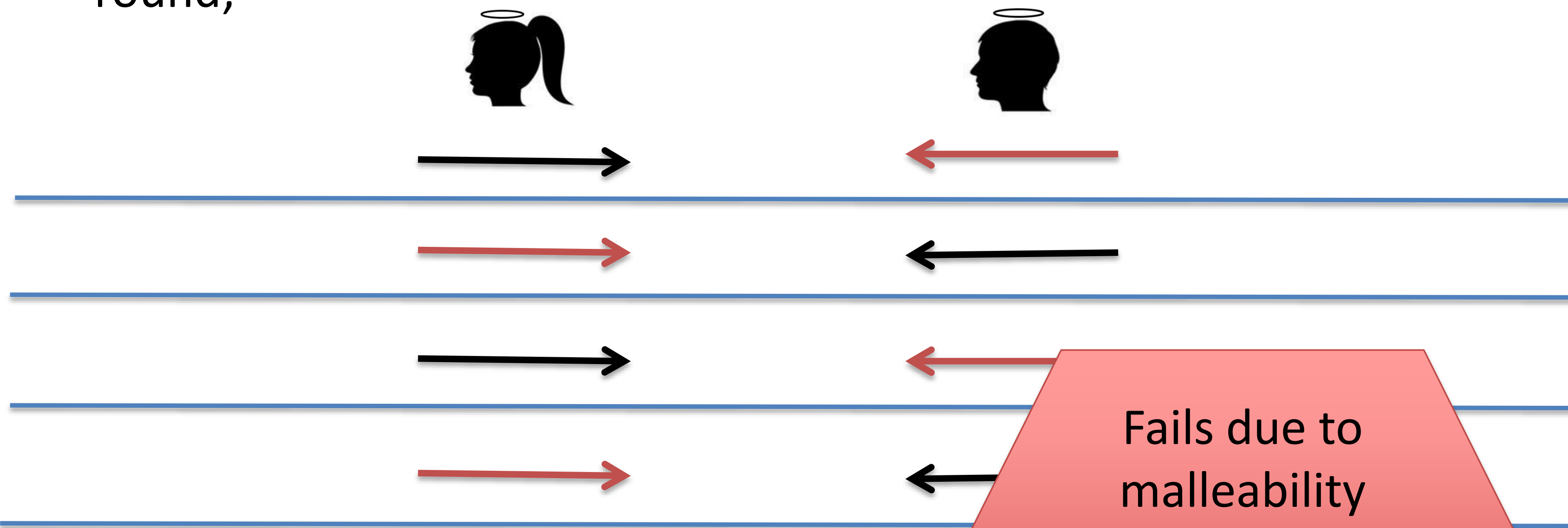
4-round attempt:



Such a 4-round protocol fails due to Theorem 2.

Our Approach for 2PC

Must use the simultaneous message exchange channel in each round;



Fails due to malleability and input consistency issues.

Run two executions of a 4-round protocol (party learns the output) in “opposite” directi

Our Approach for 2PC

Simultaneous Executions

+

3-round NMCOM

+

...

↓

4-round 2PC

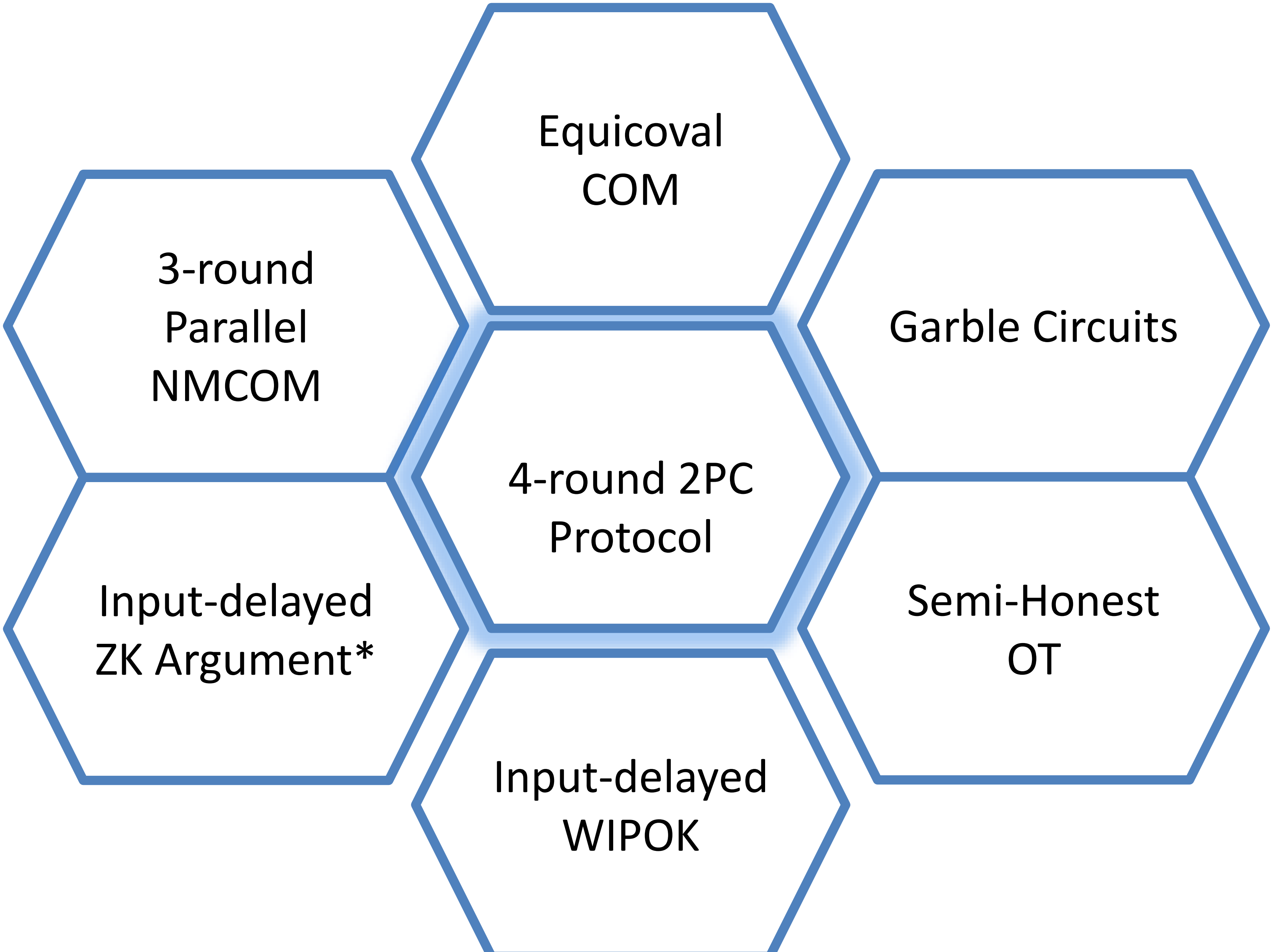
max(4, k + 1)-round 2PC protocols

Theorem 3.

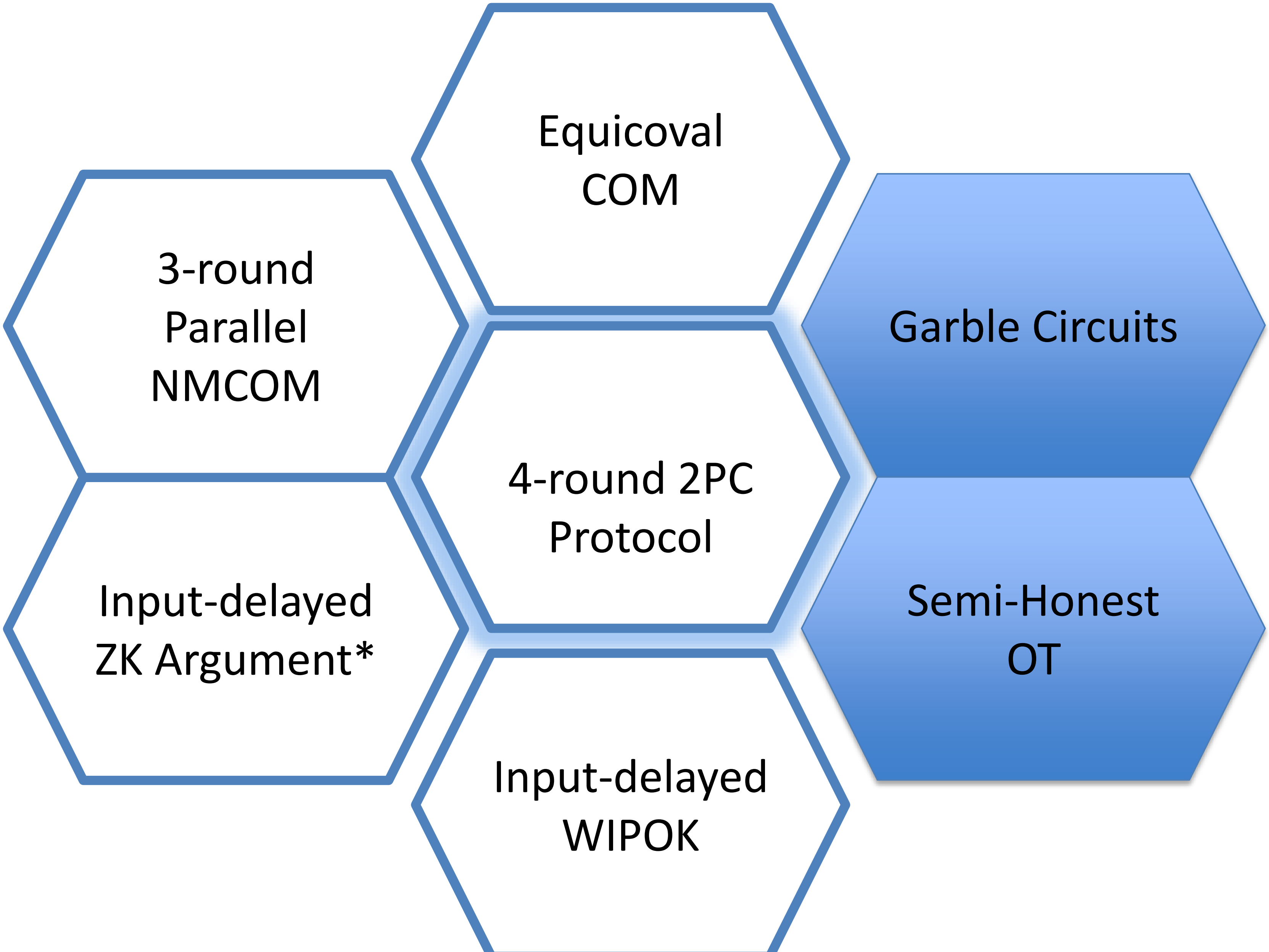
TDP + k-round (parallel) **NMCOM → max(4, k + 1)**-round **2PC** protocol

- with black-box simulation,
- in the presence of a malicious adversary,
- in the simultaneous message exchange model.

Tools for our 2PC Protocol

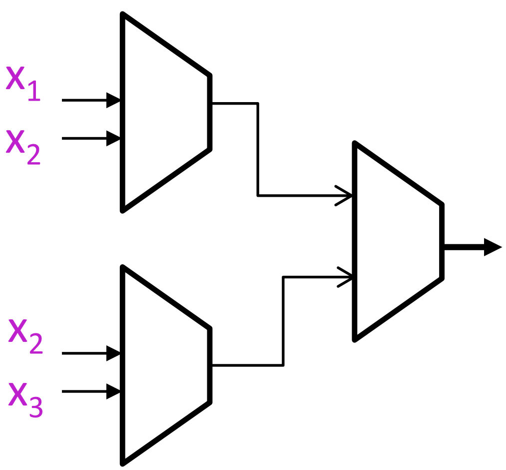


Tools for our 2PC Protocol

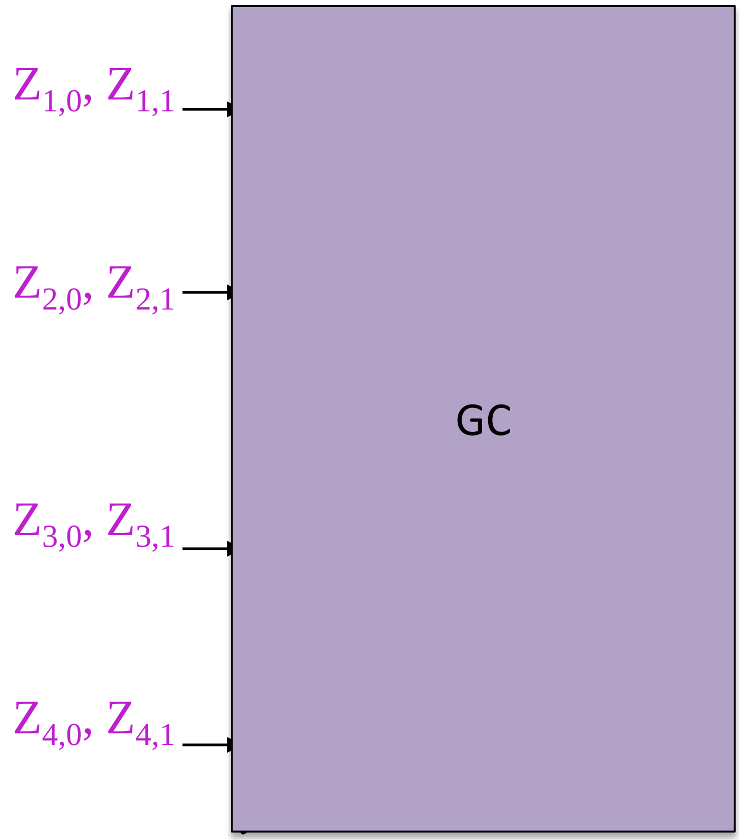


Garble Circuit Construction [Yao80]

Boolean Circuit C



Garbled Circuit GC

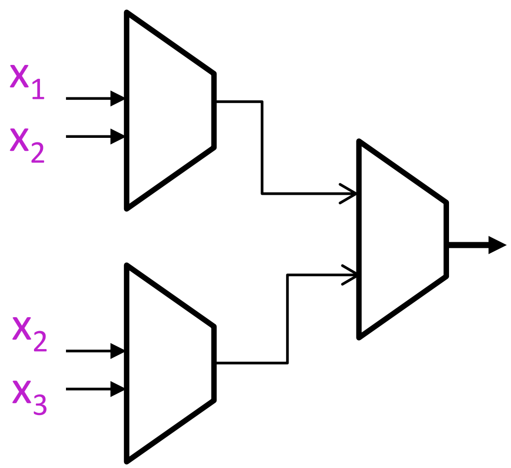


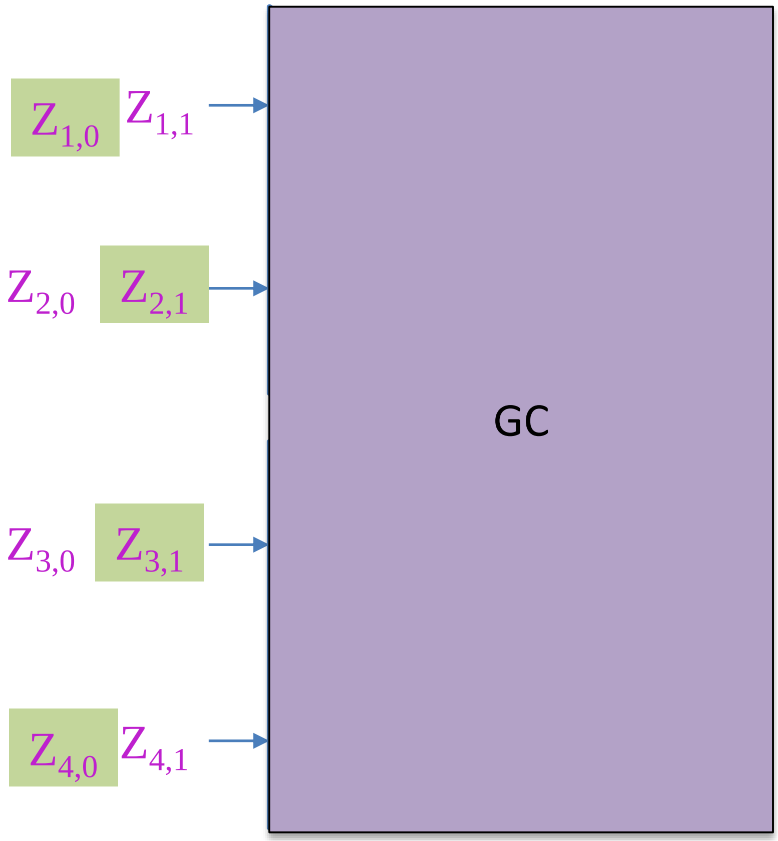
Pairs of λ-bit keys

Garble Circuit Construction [Yao80]

Boolean Circuit C

Garbled Circuit GC





Pairs of λ-bit keys

$$C(x) \xleftarrow{\text{Decoder}} GC, Z_x$$

Semi-Honest Secure 2PC

 (x)

$C(x, y)$

(y) 

$\xleftarrow{(GC_y, f_{i,b})}$

$Z_{i,b}, GC_y, f_{i,b}, f_{i,b}^{-1}$

$z'_{i,b} \leftarrow \{0,1\}^\lambda, z_{i,b} = f_{i,b}(z'_{i,b}),$
$z_{i,1-b} = z'_{i,1-b}$

$\xrightarrow{z_{i,b}}$

$\xleftarrow{W_{i,b}}$

$W_{i,b} = Z_{i,b} \oplus H(f_{i,b}^{-1}(z_{i,b}))$

$Z_{i,x_i} = W_{i,x_i} \oplus H(z_{i,x_i})$

$v = EvalGC(GC_y, Z_{i,x_i})$
$where\ v = C(x, y)$

$i \in \{0,1\}^\lambda, b \in \{0,1\}$

Semi-Honest Secure 2PC

 (x) $C(x, y)$ (y) 

$s_1 = (GC_y, f_{i,b})$ $\longleftarrow$

$Z_{i,b}, GC_y, f_{i,b}, f_{i,b}^{-1}$

$z'_{i,b} \leftarrow \{0,1\}^\lambda, z_{i,b} = f_{i,b}(z'_{i,b}),$
$z_{i,1-b} = z'_{i,1-b}$

$s_2 = (z_{i,b})$ $\longrightarrow$

$s_3 = (W_{i,b})$ $\longleftarrow$

$W_{i,b} = Z_{i,b} \oplus H(f_{i,b}^{-1}(z_{i,b}))$

$Z_{i,x_i} = W_{i,x_i} \oplus H(z_{i,x_i})$

$v = EvalGC(GC_y, Z_{i,x_i})$
$where\ v = C(x, y)$

$i \in \{0,1\}^\lambda, b \in \{0,1\}$

3-round SH 2PC: (S_1 , S_2 , S_3)

 (x)

$C(x, y)$

(y) 

S_1 $\longleftarrow$

$Z_{i,b}, GC_y, f_{i,b}, f^{-1}_{i,b}$

$$z'_{i,b} \leftarrow \{0,1\}^\lambda, z_{i,b} = f_{i,b}(z'_{i,b}), \quad z_{i,1-b} = z'_{i,1-b}$$

S_2 $\longrightarrow$

S_3 $\longleftarrow$

$$W_{i,b} = Z_{i,b} \oplus H(f^{-1}_{i,b}(z_{i,b}))$$

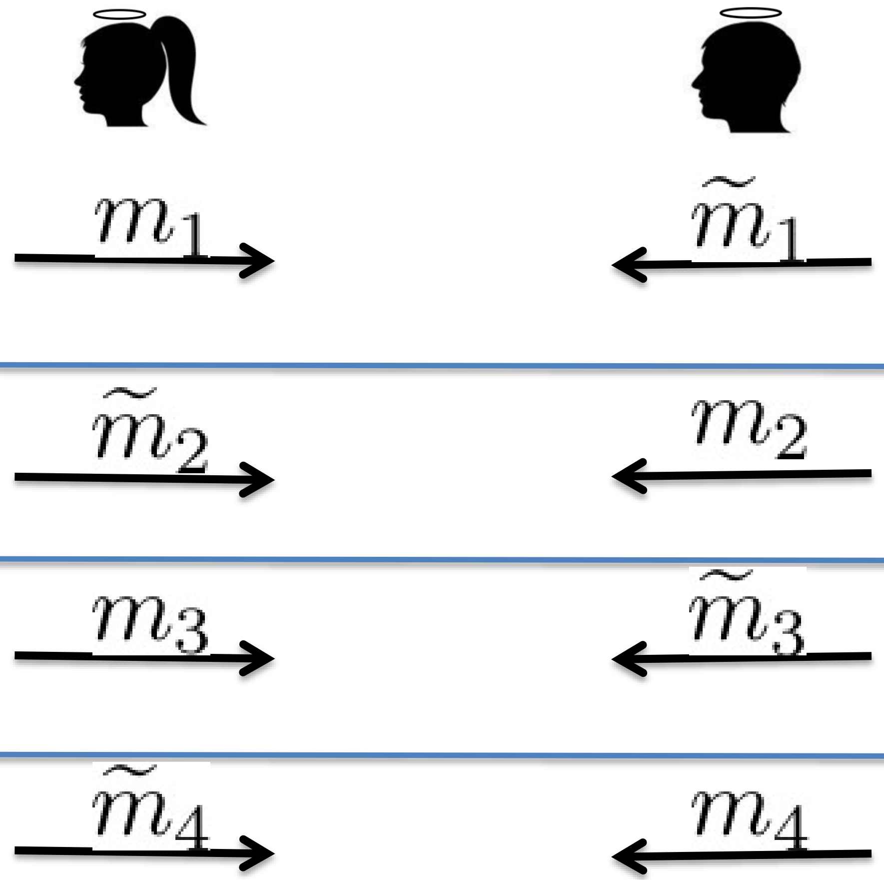
$$Z_{i,x_i} = W_{i,x_i} \oplus H(z_{i,x_i})$$

$$v = EvalGC(GC_y, Z_{i,x_i})$$

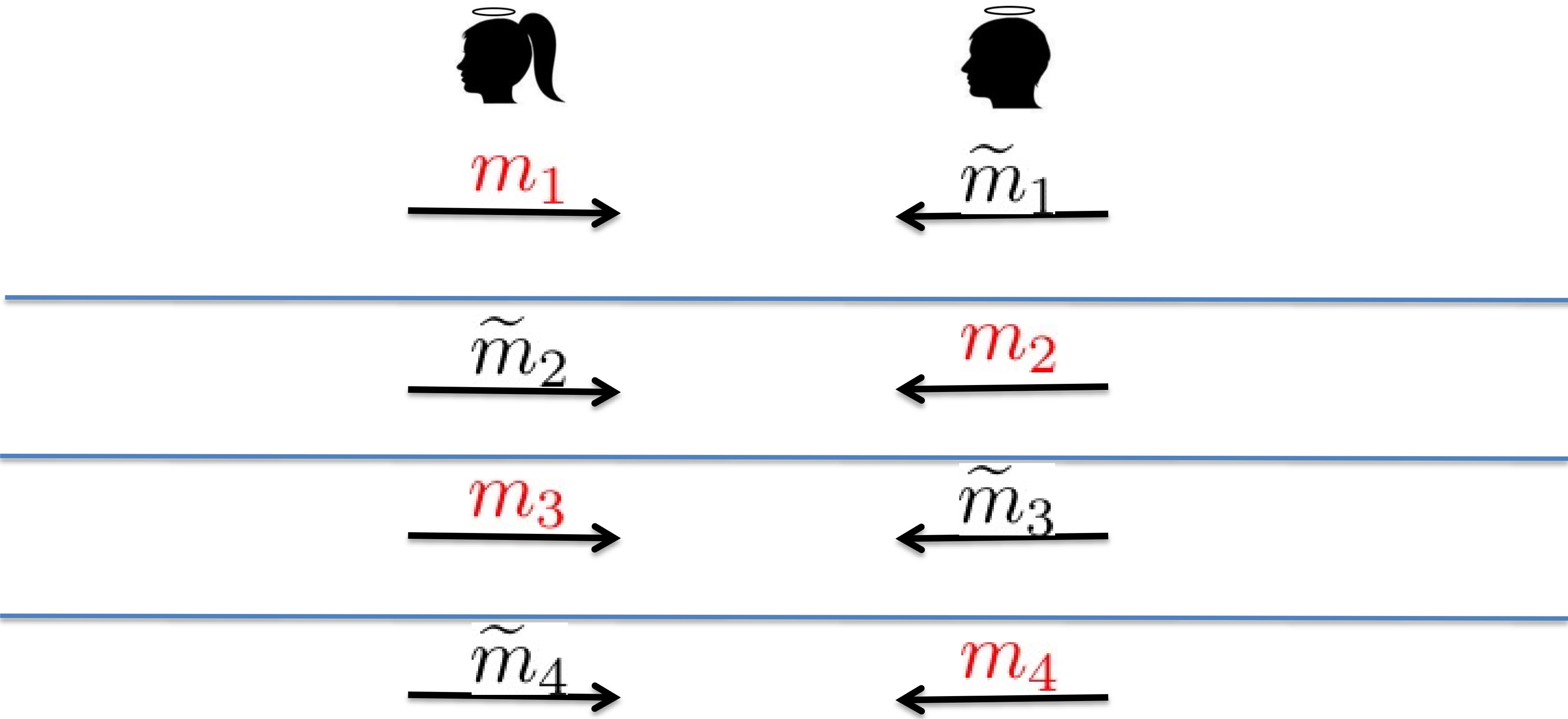
$$where\ v = C(x, y)$$

$i \in \{0,1\}^\lambda, b \in \{0,1\}$

Our 2PC Protocol



Our 2PC Protocol



Our 2PC Protocol

3-round SH 2PC: (s_1 , s_2 , s_3)

3-round NMCOM: (nm_1 , nm_2 , nm_3)

3-round Π_{WIPOK}: (p_1 , p_2 , p_3)

4-round Π_{FS}: (fs_1 , fs_2 , fs_3 , fs_4)

Our 2PC Protocol

 (x)

(y) 

fs_1 p_1 nm_1

$$r_{i,b} \leftarrow \{0,1\}^{\lambda}, nmcom(id_1, r_{i,b})$$

fs_2 p_2 nm_2 S_1 C_{GC} C_Z **r’**

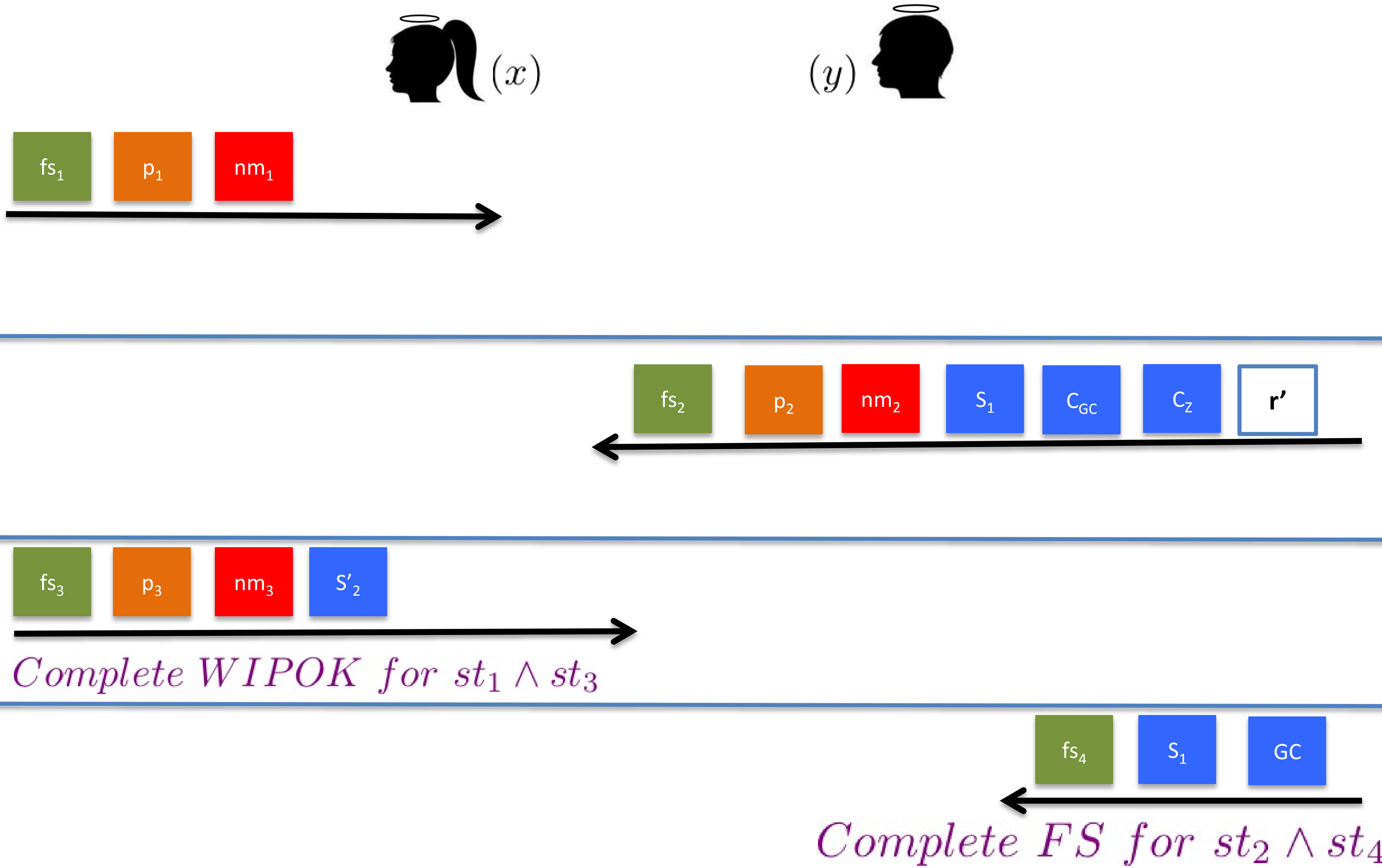
$$r'_{i,b} \leftarrow \{0,1\}^{\lambda}$$

fs_3 p_3 nm_3 S'_2

$$If\ x_i = 1,\ z'_{i,1} \leftarrow \{0,1\}^{\lambda}, z_{i,1} = f^{\lambda}_{i,1}(z'_{i,1}),$$
$$z_{i,0} = r_{i,0} \oplus r'_{i,0}.$$
$$If\ x_i = 0,\ z'_{i,0} \leftarrow \{0,1\}^{\lambda}, z_{i,0} = f^{\lambda}_{i,0}(z'_{i,0}),$$
$$z_{i,1} = r_{i,1} \oplus r'_{i,1}.$$

fs_4 S_1 GC

Our 2PC Protocol



Proof Systems

- 3-round Π_{WIPOK} public-coin, witness-indistinguishable proof-of-knowledge [FLS99] for NP $(st_1 \wedge st_2)$

- 4-round Π_{FS} zero-knowledge argument-of knowledge protocol [FS90] for NP (*thm*) based on NMCOM and Π_{WIPOK}.

1st Π_{WIPOK}: V sets $t_1=f(w_1)$, $t_2=f(w_2)$

and proves knowledge of a w for $t_1 \vee t_2$

2nd Π_{WIPOK}: P proves knowledge of a witness to

$thm \vee (t_1 \vee t_2)$

Proof Systems

- 3-round Π_{WIPOK} public-coin, witness-indistinguishable proof-of-knowledge [FLS99] for NP *($st_1 \wedge st_2$)*

- 4-round Π_{FS} zero-knowledge argument-of knowledge protocol [FS90] for NP (*thm*) based on NMCOM and Π_{WIPOK}.

Crucial Change

1st Π_{WIPOK}: V sets $t_1=nm^{\sigma 1}$, $t_2=nm^{\sigma 2}$

and proves knowledge of a w for $t_1 \vee t_2$

2nd Π_{WIPOK}: P proves knowledge of a witness to

$thm \vee (t_1 \vee t_2)$

Proof Systems

- 3-round Π_{WIPOK} public-coin, witness-indistinguishable proof-of-knowledge [FLS99] for NP $(st_1 \wedge st_2)$

- 4-round Π_{FS} zero-knowledge argument-of knowledge protocol [FS90] for NP ($thm \wedge thm'$) based on NMCOM and Π_{WIPOK}.

1st Π_{WIPOK}: V sets $t_1=nm^{\sigma 1}$, $t_2=nm^{\sigma 2}$

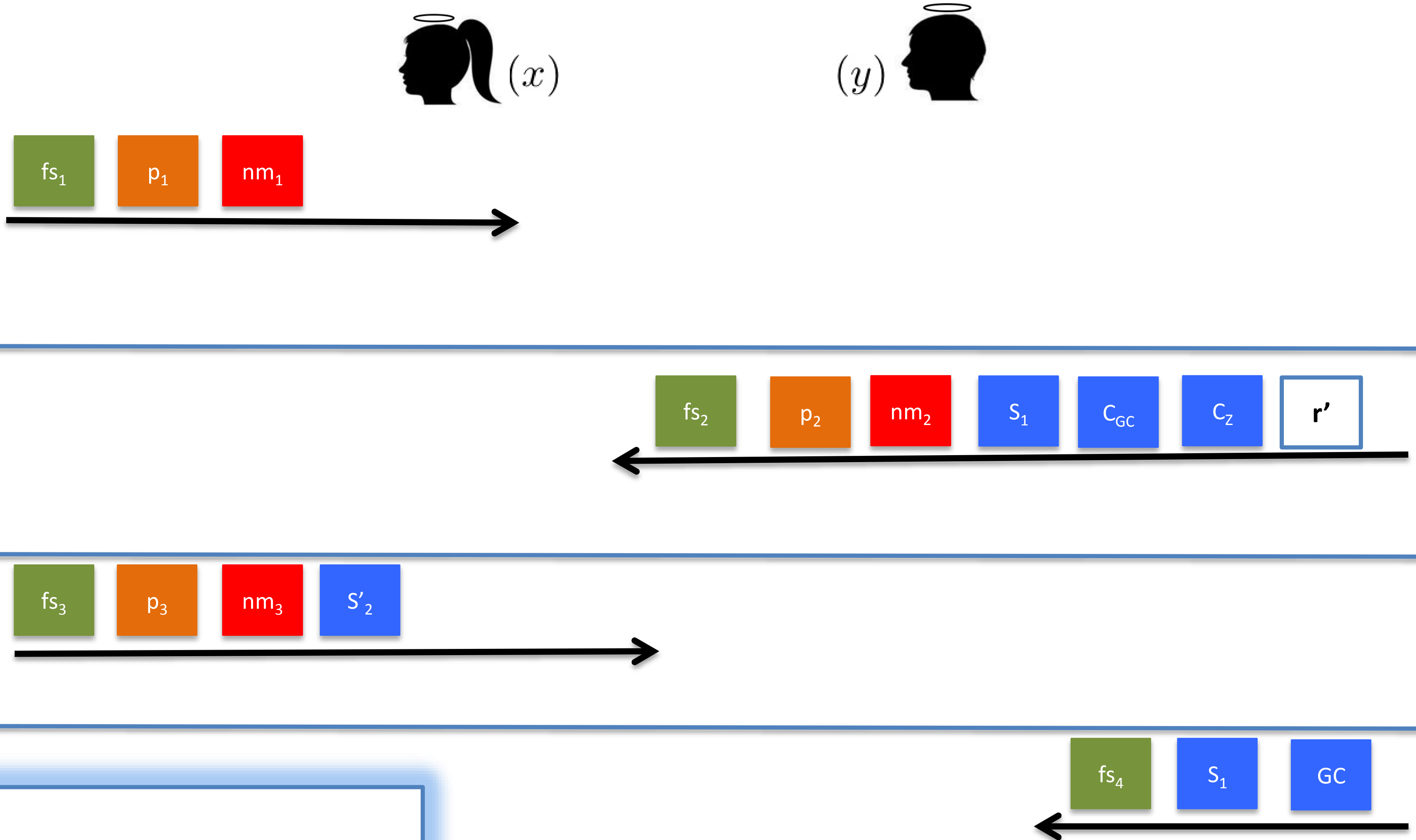
and proves knowledge of a w for $t_1 \vee t_2$

2nd Π_{WIPOK}: P proves knowledge of a witness to

$thm \vee (t_1 \vee t_2)$

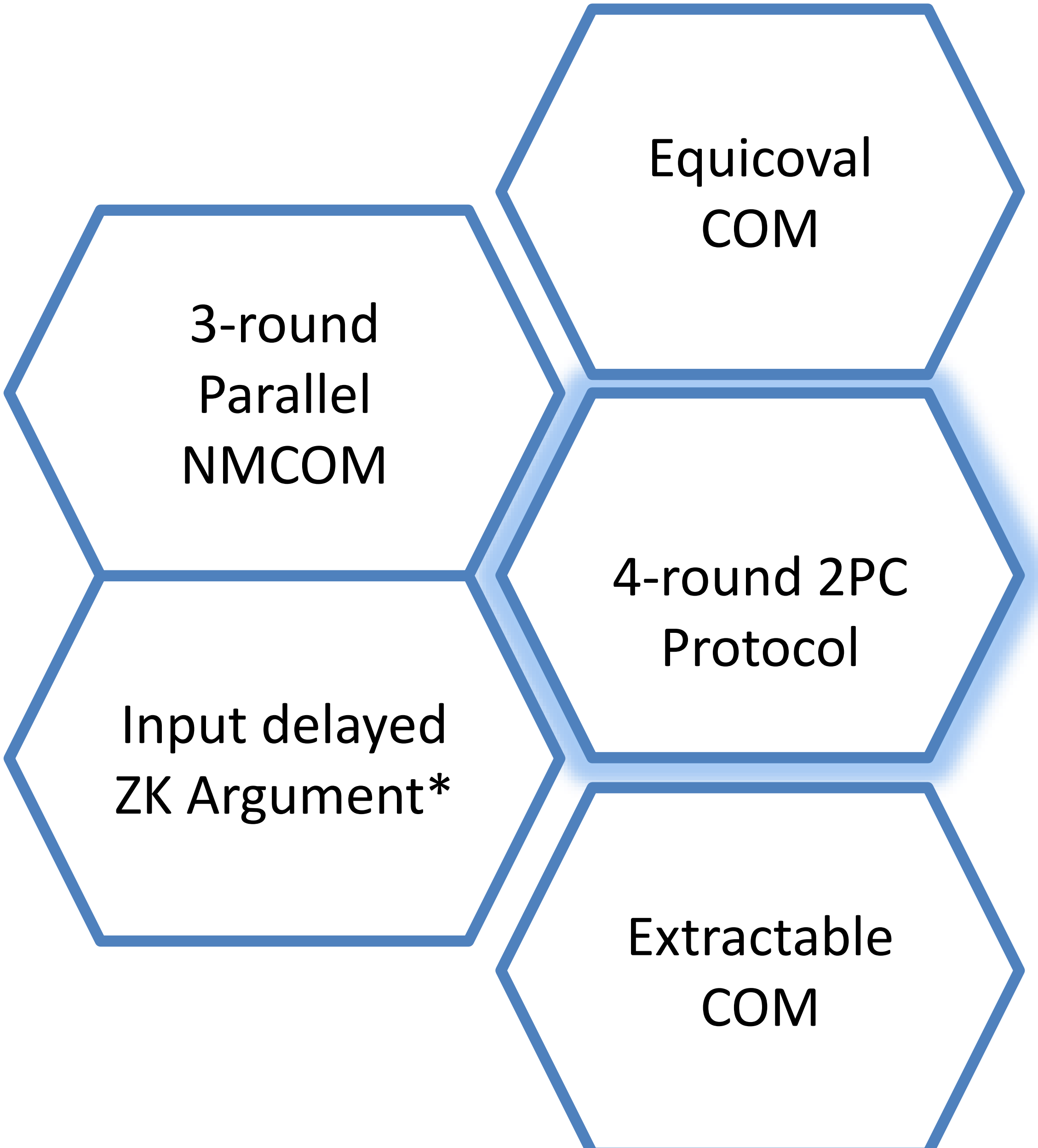
Input-Delayed Proof Systems

Our 2PC Protocol



Simulation Soundness

Tools for our Coin-Flipping Protocol



Conclusion

Round Complexity	
2PC	MPC
5 rounds [KO04]	O(1)

- **(3-round Impossibility)**:

There does **not** exist a **3-round protocol** for the **two-party coin-flipping** functionality.

Conclusion

Round Complexity	
2PC	MCF*
max(4,k+1)[1]	max(4,k+1)

[1] k-round NMCOM

Suppose that there exists a k-round NMCOM scheme; then

- **(2PC)**: there exists a **max(4, k + 1)-round** protoc -
  party functionality;
- **(MPC)**: there exists a **max(4, k + 1)-round** proto -
  party coin-flipping functionality.

Four rounds are both **necessary and sufficient** for both the results based on the 3-round NMCOM of [GPR16].

4-round 2PC protocols

Theorem [GMP**P**16]

TDP + k-round (parallel) **NMCOM → max(4, k + 1)**-round **2PC** protocol

[GMP**P**16]: **TDP +** **3-round NMCOM** [PPV08] → **4**-round **2PC** protocol

[H**P**V16]: **TDP +** **OWF** → **4**-round **2PC** protocol

4-round MPC protocols

[GMP**P**16]:	**TDP +**	LWE	➔ **6**-round **MPC** protocol
[GMP**P**16]:	**TDP +**	iO	➔ **5**-round **MPC** protocol
[H**P**V16]:	**TDP +**	iO	➔ **4**-round **MPC** protocol*

Open Problems

Crypto Assumption	Plain Model	CRS Model
MPC protocols		
Semi-Honest OT	O(1) rounds [BMR90…]	4 rounds [GMW87+AIK05]
LWE	6 rounds [this work]	2 rounds [MW15]
iO	4 rounds [H**P**V16]	2 rounds [GGHR14]

Can we get optimal-round static MPC protocols from different/weaker assumptions?

Thank you!