On the Communication and Round Complexity of Secure Computation

Antigoni Polychroniadou

Χρόνια Πολλά Ivan!

Joint works with
Ivan Damgård, Sanjam Garg, Pratyay Mukherjee, Jesper Nielsen,
Omkant Pandey

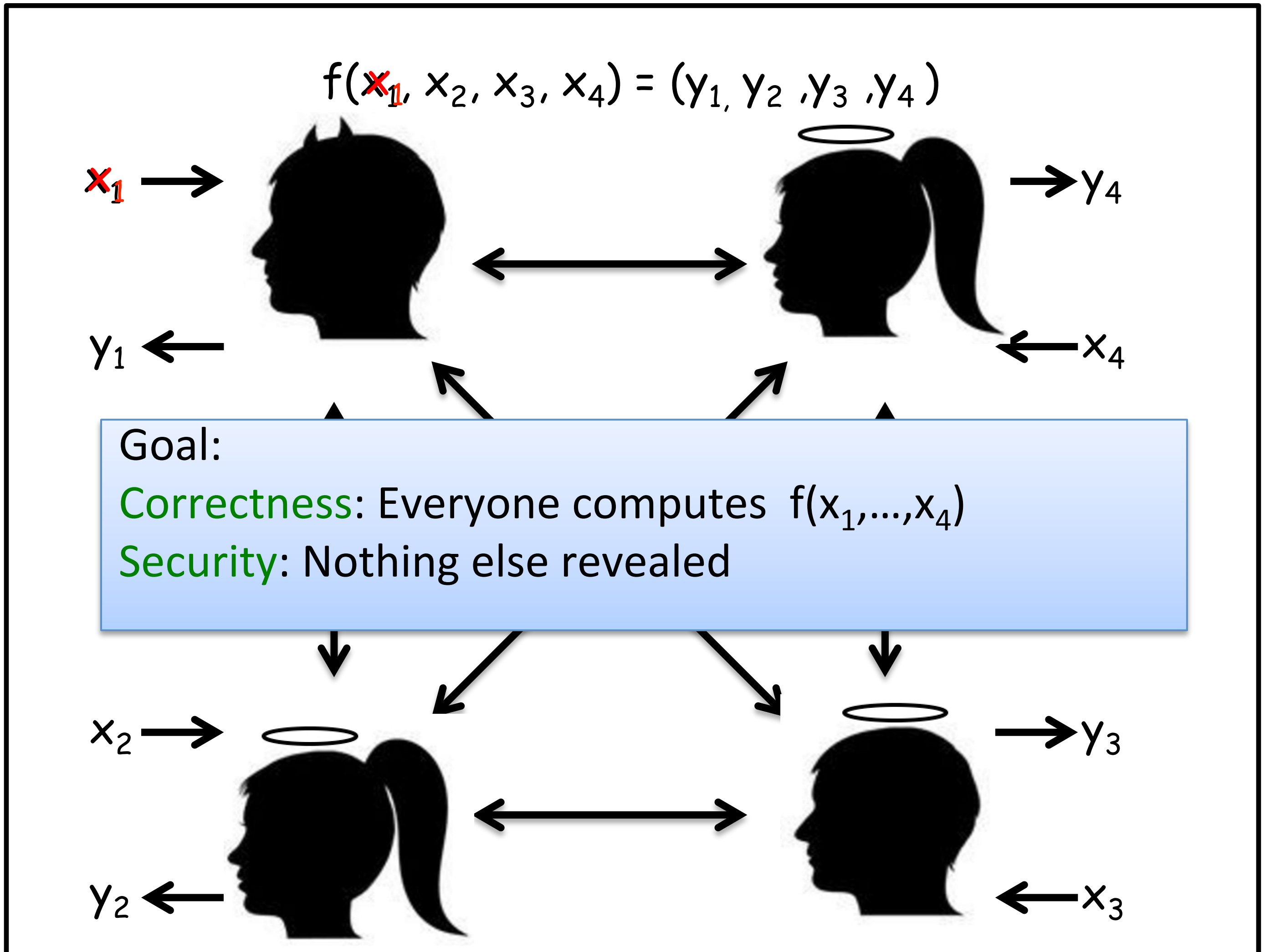

Bar-Ilan University
The Department of Computer Science
on Cryptography

Introduction of Secure MPC

[Yao82,GMW87,BGW88, CCD88]



Multi-Party Computation (MPC)

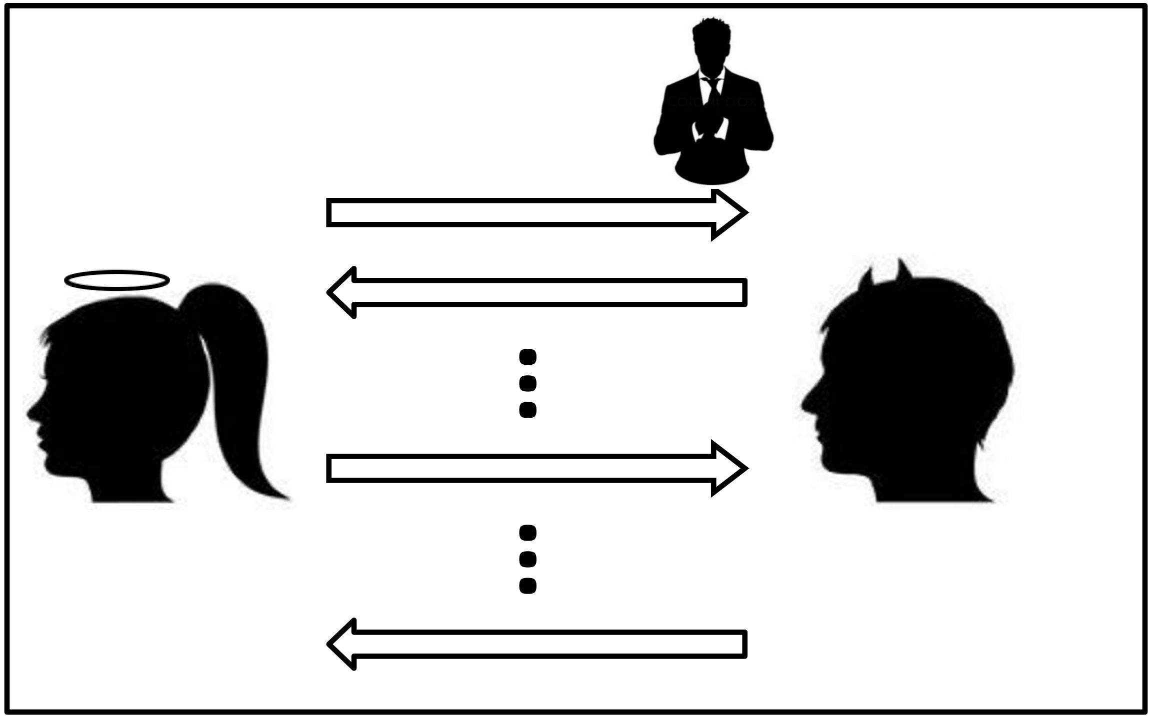


Adversary:

Unbounded or PPT

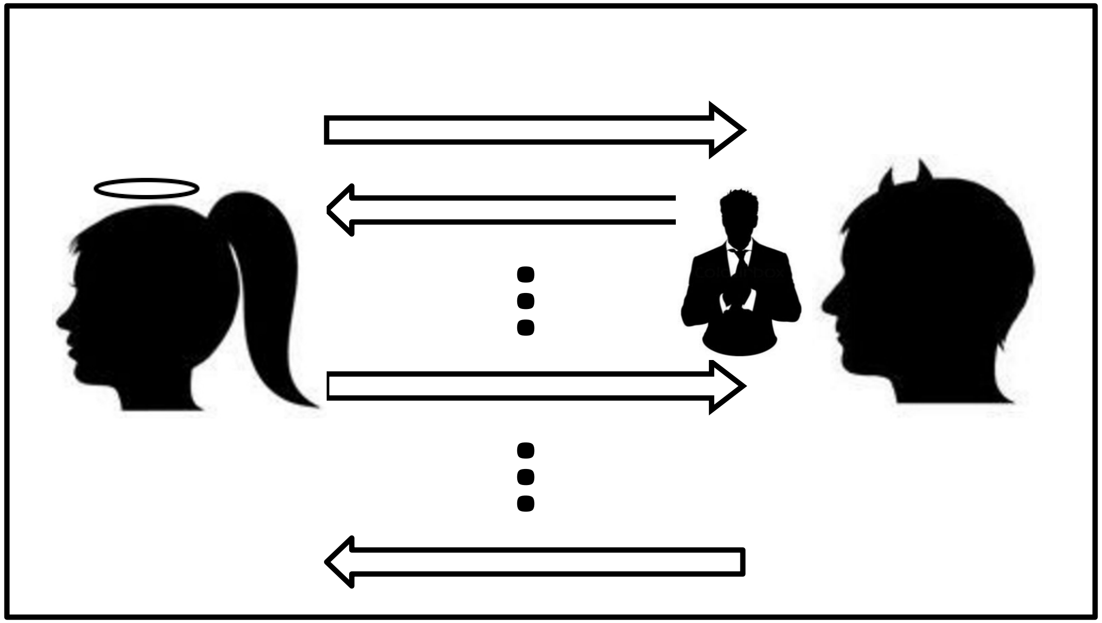
Passive or Active

Static or Adaptive



Static Corruption

Corrupt only on the onset of π



Adaptive Corruption

Corrupt *adaptively* during the execution of π

Modelling Communication

Important: Round/Communication complexity

Simultaneous Message Exchange Channel: in each round, all parties can simultaneously exchange messages (rushing-adversary).

State of the Art: Communication Complexity

Information-Theoretic Setting	Computational Setting
O(n|C|)	<< |C|

FHE

State of the Art: Round Complexity

Information-Theoretic Setting*	Computational Setting	
	2PC	MPC
O($depth_C$)	5 rounds [KO04]	O(1)

Motivating Questions

Lower bounds on the communication and round complexity of (adaptive) protocols.

Both for Information-Theoretic
&
Computationally secure protocols

Our results: Communication Complexity

Information-Theoretic Setting*	Computational Setting
Ω(n|C|)	<< |C|

FHE

Information-Theoretic Setting:

[DNP16]: **any protocol** that follows the typical gate-by-gate design pattern* of secure computation must have **Ω(n|C|)** communication (even with preprocessing).

Our Results: Round Complexity

Information-Theoretic Setting	Computational Setting	
	2PC	MPC
$\Omega(\text{depth}_C)$	5 rounds [KO04]	O(1)

Information-Theoretic Setting:
[DNP16]: **any protocol** that follows the typical gate-by-gate design pattern of secure computation must have $\mathbf{\Omega(depth_C)}$ **rounds** (even with preprocessing).

Computational Setting:
[GMPP16]: Suppose that there exists a k-round NMCOM scheme; then there exists a **max(4, k + 1)-round** protocol for securely realizing every functionality in **the simultaneous message exchange model**.

Our Results: Round Complexity

Information-Theoretic Setting	Computational Setting	
	2PC	MCF*
$\Omega(\text{depth}_C)$	max(4,k+1)[1]	max(4,k+1)

[1] k-round NMCOM

Information-Theoretic Setting:

[DNP16]: **any protocol** that follows the typical gate-by-gate design pattern of secure computation must have **$\Omega(\text{depth}_C)$ rounds** (even with preprocessing).

Computational Setting:

[GMPP16]: Suppose that there exists a k-round NMCOM scheme; then there exists a **max(4, k + 1)-round** protocol for securely realizing every functionality in **the simultaneous message exchange model**.

Computational Setting

Round Complexity of MPC Protocols in the computational setting

Plain model: max(4, k+1) rounds given a k-round non-malleable commitment [GMPP16]
CRS Model: 2 rounds [HLP11]

Without privacy: one round is enough
Everyone broadcast their inputs

With privacy: need AT LEAST TWO ROUNDS
Corrupted parties can evaluate residual function on many inputs

$$f_h(x)=f(h,x)$$

where h=fixed inputs of honest parties

Round Complexity and Assumptions

Crypto Assumption	Plain Model	CRS Model
Static MPC protocols		
Semi-Honest OT	O(1) rounds [BMR90…]	4 rounds [GMW87+AIK05]
LWE	6 rounds [GMP**P**16]	2 rounds [MW15]
iO	4 rounds [H**P**W16]	2 rounds [GGHR14]
Adaptive MPC protocols		
Semi-Honest OT	O(1)[1] [IPS08]; O($depth_C$)[2] [CLOS02, GS12, DMRV13, V14]	
LWE	O(1) [1] rounds [D**P**R16]	3 rounds [1] [D**P**R16]
iO	O($depth_C$)[G**P**15+CLOS02]	2 rounds [2] [G**P**15]

[1] n-1 adaptive corruptions.

[2] n adaptive corruptions.

[GMPP16]

Suppose that there exists a k-round NMCOM; 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.

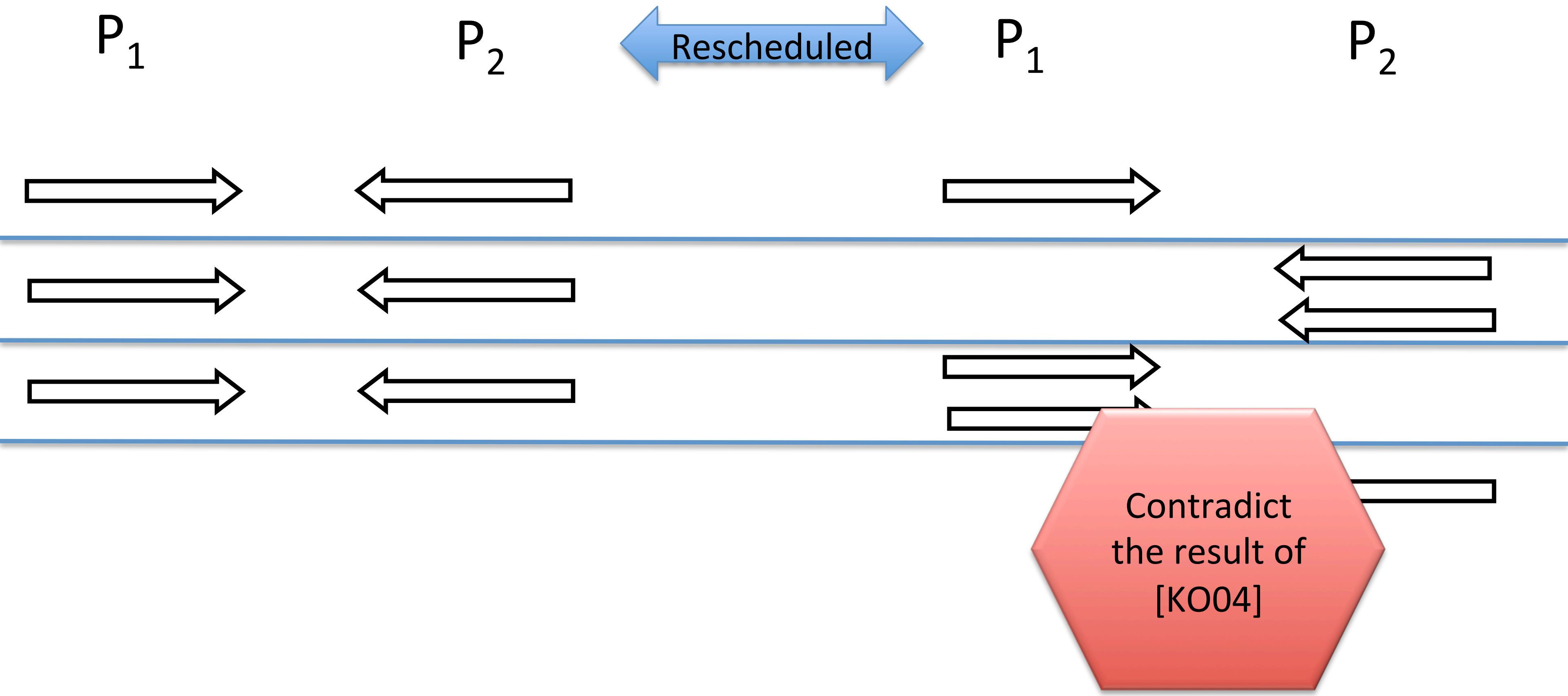
We establish that **four rounds** are both **necessary and sufficient** for both the results above based on the 3-round NMCOM of [GPR16].

[GMPP16]

Let $p(\lambda) = \omega(\log\lambda)$, where λ is the security parameter. Then there **does not exist a 3-round protocol** with **simultaneous message transmission for tossing $p(\lambda)$ coins** which can be proven secure via black- box simulation.

Proof (sketch)

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



Remark

Information-Theoretic Setting

[DNP16]

Is it really inherent that the typical gate-by-gate approach to secure computation requires communication for each multiplication operation?

(both for honest majority and dishonest majority with preprocessing)

Our Model

Gate-by-gate protocols:

synchronous

point-to-point secure channels

n-party

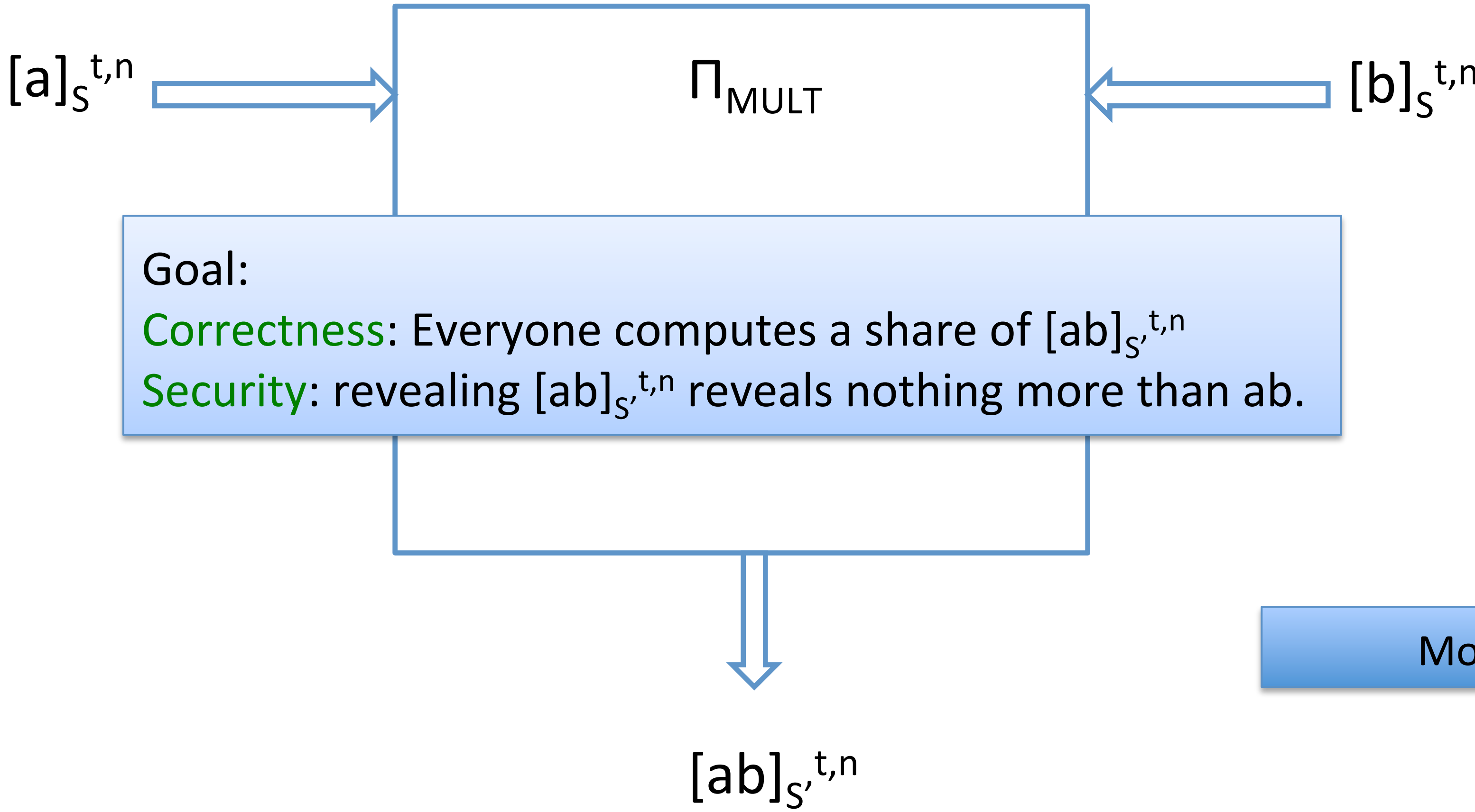
t-out-of-n static corruptions

semi-honest security

statistical security

Protocols call an MGP protocol per Mult. gate

Multiplication Gate Protocol Π_{MULT}



Goal:

Correctness: Everyone computes a share of $[ab]_{S'}^{t,n}$

Security: revealing $[ab]_{S'}^{t,n}$ reveals nothing more than ab.

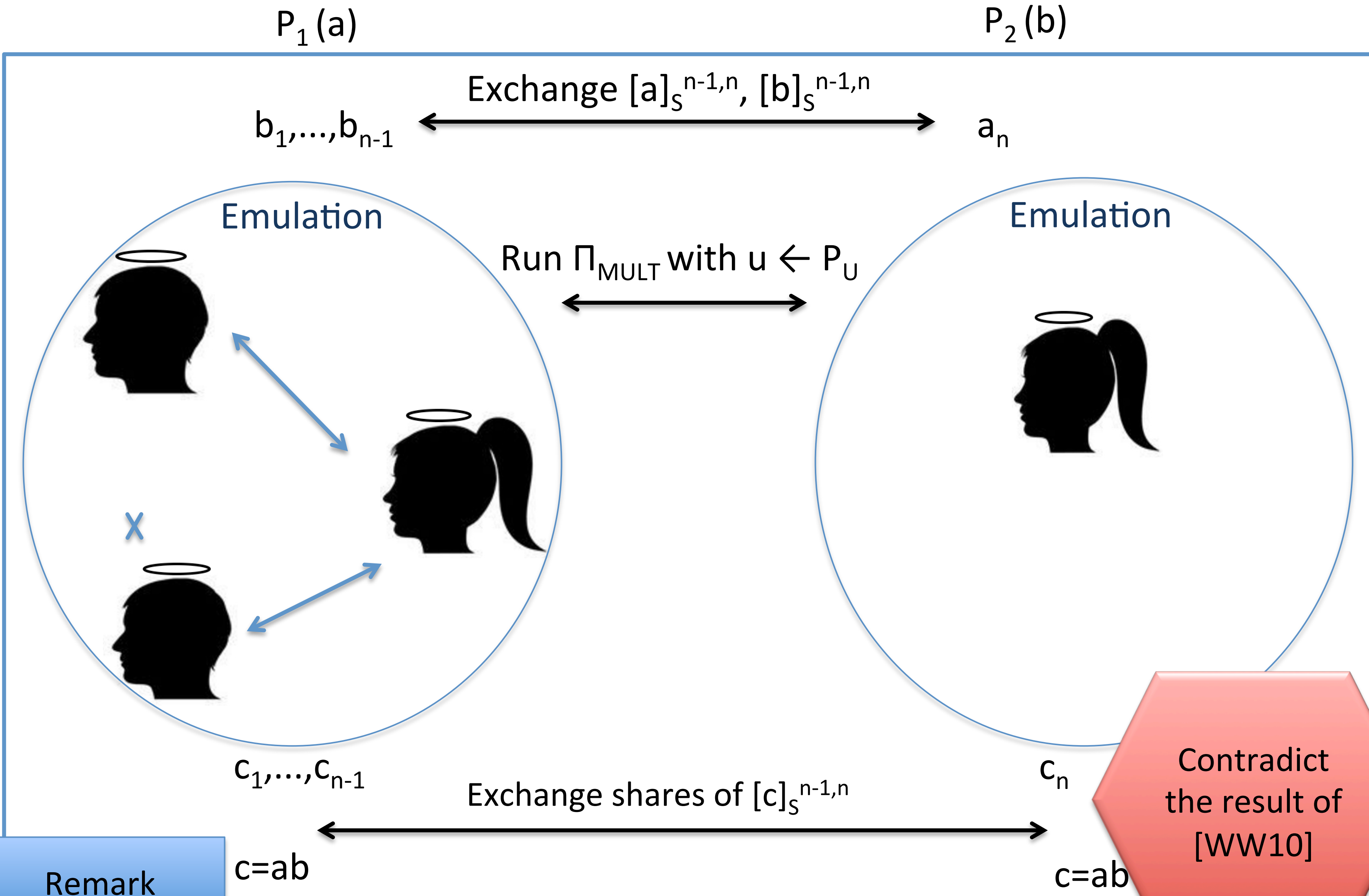
Model

[DNP16]

In the preprocessing model, there exists **no MGP Π_{MULT}** with expected anticipated communication complexity **≤ n – 1** and with **additive secret-sharing** $S^{n-1,n}$ as output sharing scheme.

Proof (sketch)

Suppose that there exists Π_{MULT} with expected CC $\leq n - 1$



Contradict the result of [WW10]

Remark

Conclusion

Lower bounds on the communication and round complexity of **information-theoretic** (adaptive) protocols that follow the gate-by-gate design pattern.

Lower bounds on the round complexity of **computationally secure** (adaptive) protocols.

Open problems in the IT Setting

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

Open problems in the Computational Setting

Bounds on the round complexity of secure MPC:
CRS Model: 2 rounds [HLP11]
Plain model: max(4, k+1) rounds given a k-round non-malleable commitment [GMP**P**16]

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

Round Complexity and Assumptions

Crypto Assumption	Plain Model	CRS Model
Static MPC protocols		
Semi-Honest OT	O(1) rounds [BMR90…]	4 rounds [GMW87+AIK05]
LWE	6 rounds [GMP**P**16]	2 rounds [MW15]
iO	4 rounds [H**P**W16]	2 rounds [GGHR14]
Adaptive MPC protocols		
Semi-Honest OT	O(1)[1] [IPS08]; O($depth_C$)[2] [CLOS02, GS12, DMRV13, V14]	
LWE	O(1)[1] rounds [D**P**R16]	3 rounds[1] [D**P**R16]
iO	O($depth_C$)[G**P**15+CLOS02]	2 rounds[2] [G**P**15]

[1] n-1 adaptive corruptions.

[2] n adaptive corruptions.

Tak!