A New Approach to Round-Optimal Secure Multiparty Computation

Prabhanjan Ananth
University of California Los Angeles

Arka Rai Choudhuri
Johns Hopkins University

Abhishek Jain
Johns Hopkins University

Crypto 2017

What is the round complexity of MPC?

What is the round complexity of MPC?

What is the round complexity of MPC?

Computational security.

What is the round complexity of MPC?

Computational security.

Malicious adversaries with dishonest majority.

What is the round complexity of MPC?

Computational security.

Malicious adversaries with dishonest majority.

No trusted setup.

What is the round complexity of MPC?

Computational security.

Malicious adversaries with dishonest majority.

No trusted setup.

In the CRS model: 2 rounds [Garg-Gentry-Halevi-Raykova14, Mukherjee-Wichs16, Dodis-Halevi-Rothblum-Wichs16]

Brief history

Brief history

Polynomial round protocol:

[Goldreich-Micali-Wigderson87]

Brief history

Polynomial round protocol:

[Goldreich-Micali-Wigderson87]

Constant round protocols:

[Beaver-Micali-Rogaway90,

Brief history

Polynomial round protocol:

[Goldreich-Micali-Wigderson87]

Constant round protocols:

[Beaver-Micali-Rogaway90, Katz-Ostrovsky-Smith03, Pass04, Pass-Wee10, Wee10, Goyal11]

Exact round complexity

Exact round complexity

[Katz-Ostrovsky04]:

4 round impossible w.r.t black-box simulation for 2PC in the unidirectional message model.

Exact round complexity

[Katz-Ostrovsky04]:

4 round impossible w.r.t black-box simulation for 2PC in the unidirectional message model.

[Garg-Mukherjee-Pandey-Polychroniadou16]:

3 round impossible w.r.t black-box simulation in the simultaneous message model.

Exact round complexity

[Katz-Ostrovsky04]:

4 round impossible w.r.t black-box simulation for 2PC in the unidirectional message model.

[Garg-Mukherjee-Pandey-Polychroniadou16]:

3 round impossible w.r.t black-box simulation in the simultaneous message model.

5 round MPC protocol based on iO + other assumptions.

Exact round complexity

[Katz-Ostrovsky04]:

4 round impossible w.r.t black-box simulation for 2PC in the unidirectional message model.

[Garg-Mukherjee-Pandey-Polychroniadou16]:

3 round impossible w.r.t black-box simulation in the simultaneous message model.

5 round MPC protocol based on iO + other assumptions.

Exact round complexity

Does there exist a 5 round MPC protocol from standard assumptions?

[Garg-Mukherjee-Pandey-Polychroniadou16]:

3 round impossible w.r.t black-box simulation in the simultaneous message model.

5 round MPC protocol based on iO + other assumptions.

Exact round complexity

Does there exist a 5 round MPC protocol from standard assumptions?

Does there exist a 4 round MPC protocol?

[Garg-Mukherjee-Pandey-Polychroniadou16]:

3 round impossible w.r.t black-box simulation in the simultaneous message model.

5 round MPC protocol based on iO + other assumptions.

Our results

Result 1:

Assuming DDH, there exists a 5 round MPC protocol.

Result 2:

Assuming OWP + sub-exponentially secure DDH, there exists a 4 round MPC protocol.

Our results

Result 1:

Assuming DDH, there exists a 5 round MPC protocol.

Result 2:

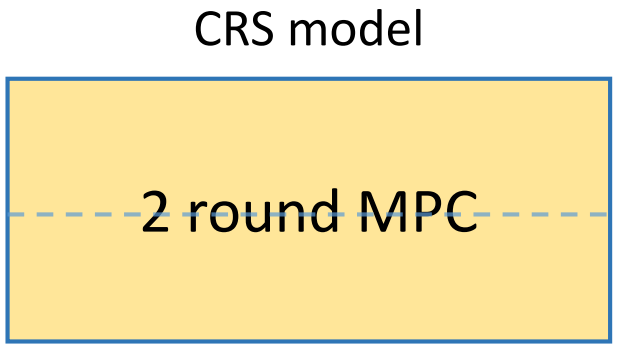
Assuming OWP + sub-exponentially secure DDH, there exists a 4 round MPC protocol.

Concurrent work [Brakerski-Halevi-Polychroniadou17]:

4 round MPC protocol assuming adaptive commitments + sub-exponential LWE.

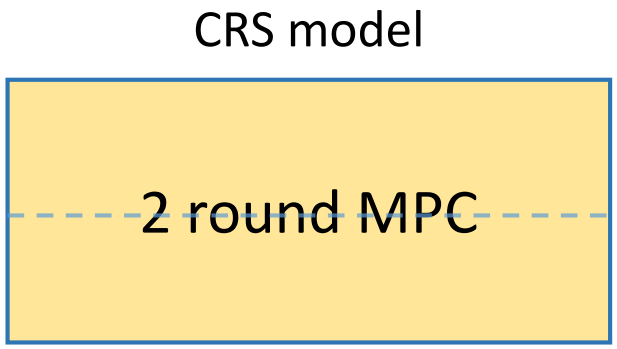
[Garg-Mukherjee-Pandey-Polychroniadou 16] template

[Garg-Mukherjee-Pandey-Polychroniadou 16] template



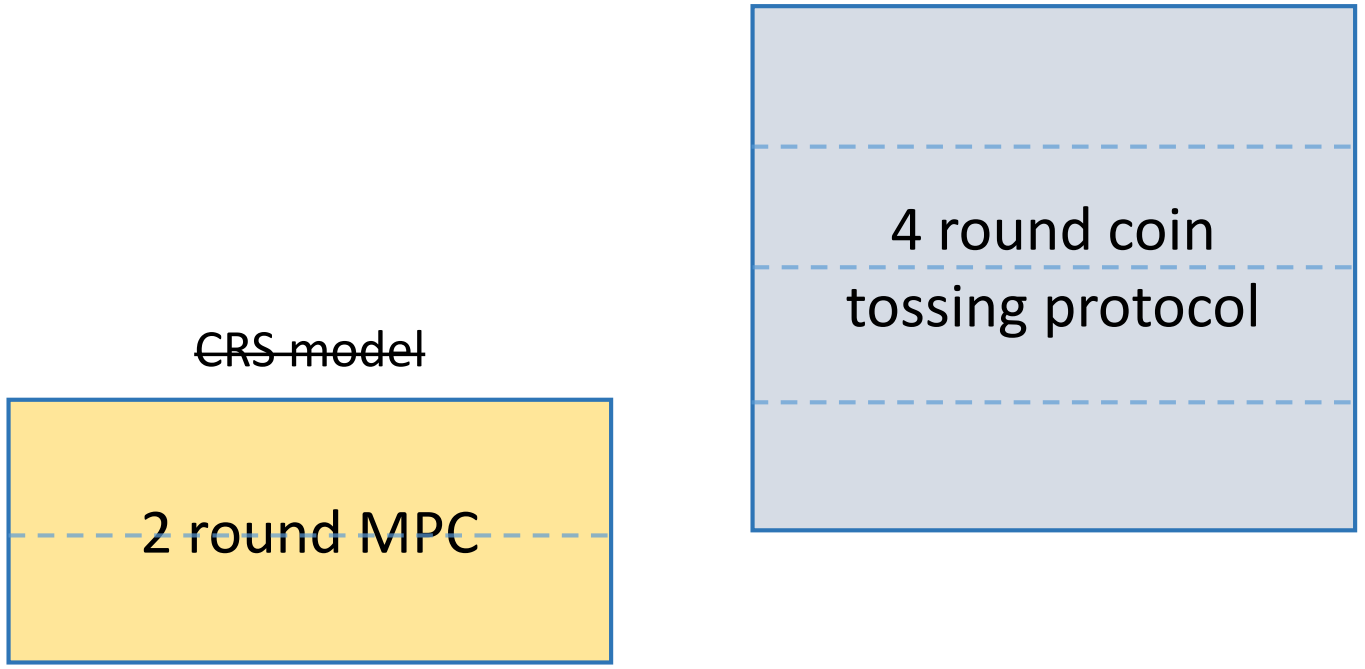
- from iO [GGHR14]
- from LWE [MW16]

[Garg-Mukherjee-Pandey-Polychroniadou 16] template

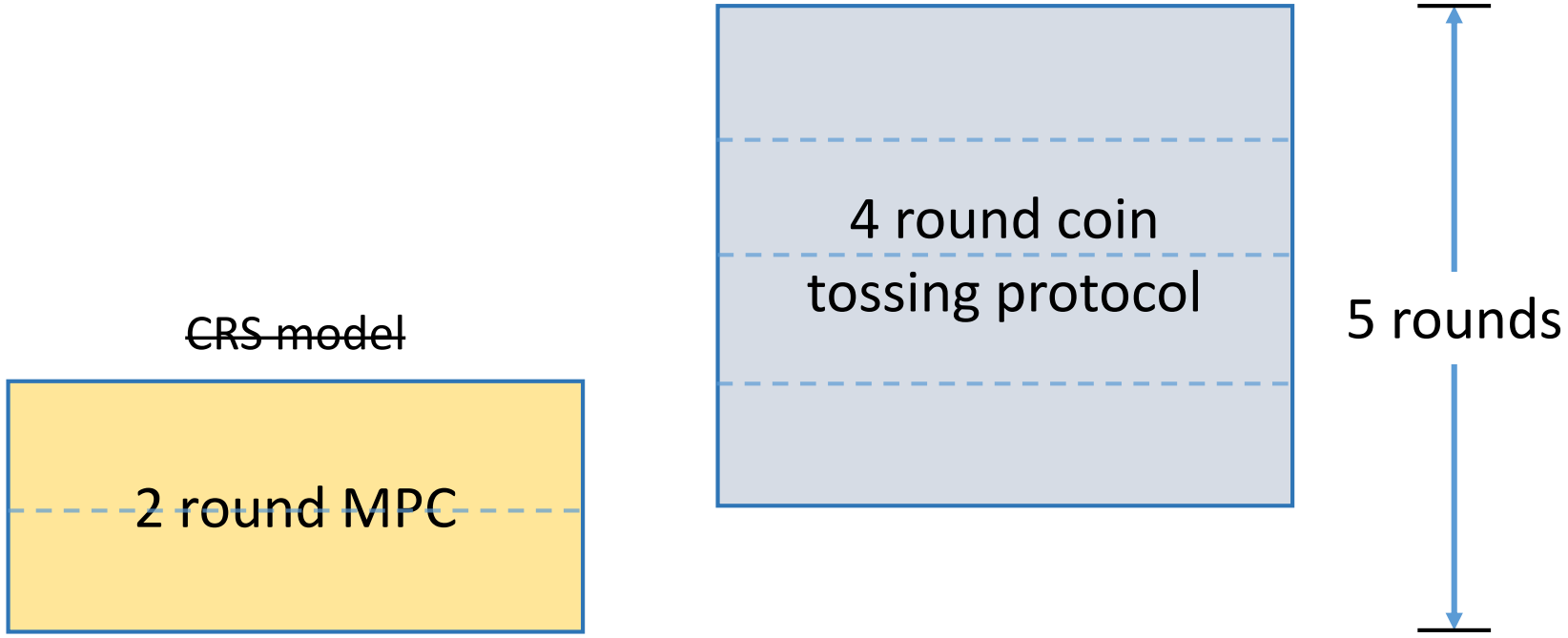


- from iO [GGHR14]

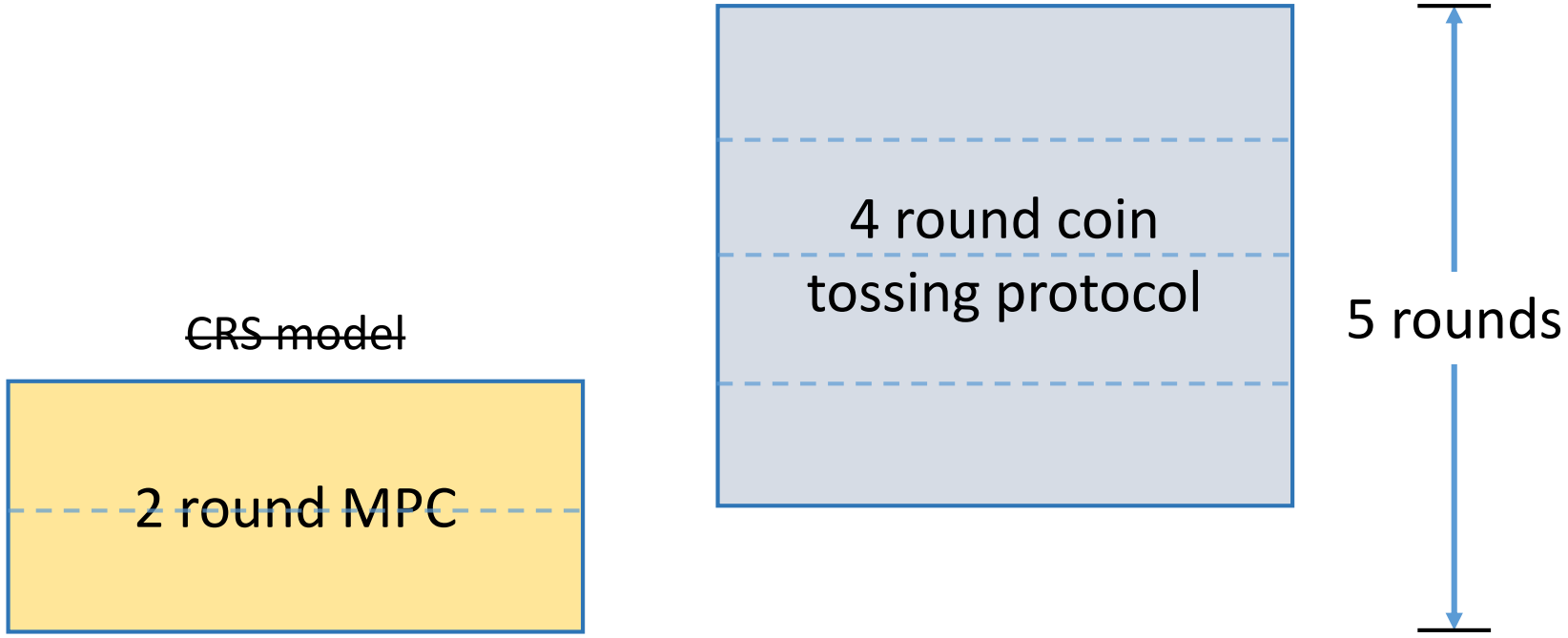
[Garg-Mukherjee-Pandey-Polychroniadou 16] template



[Garg-Mukherjee-Pandey-Polychroniadou 16] template

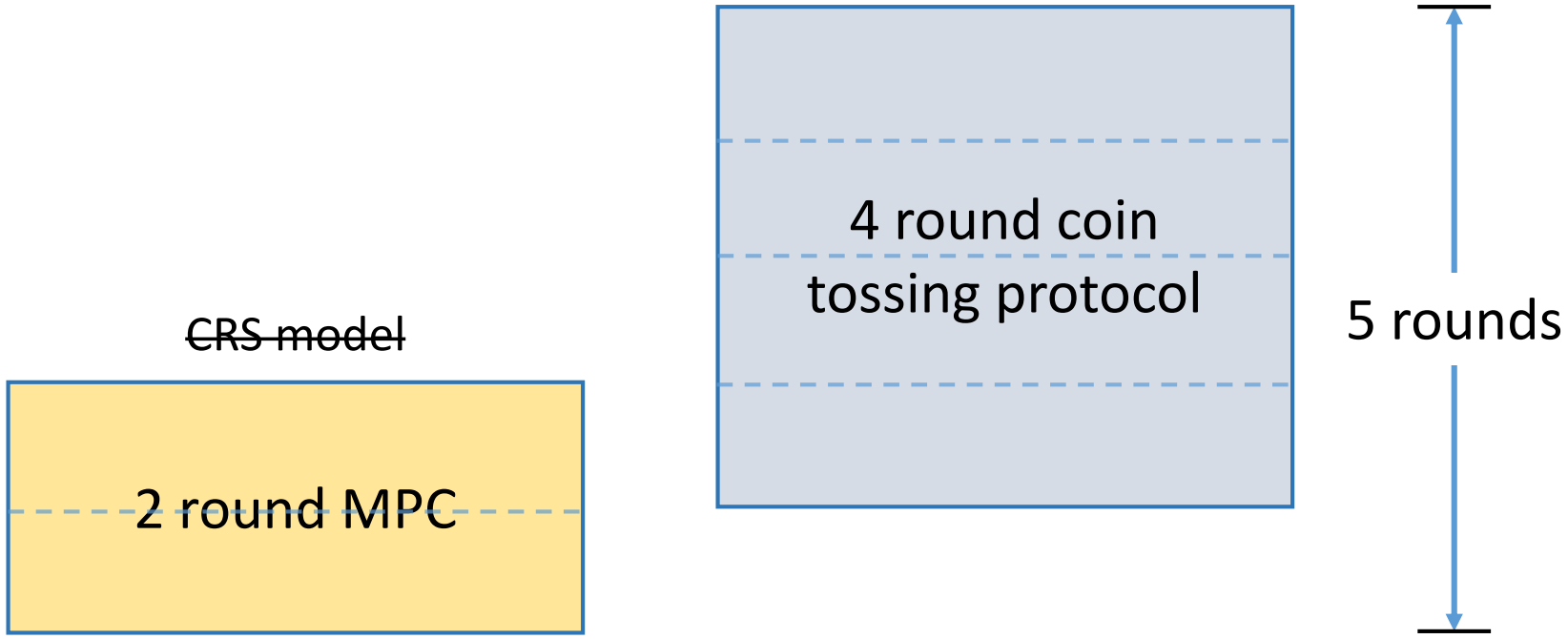


[Garg-Mukherjee-Pandey-Polychroniadou 16] template



Limitations of this approach:

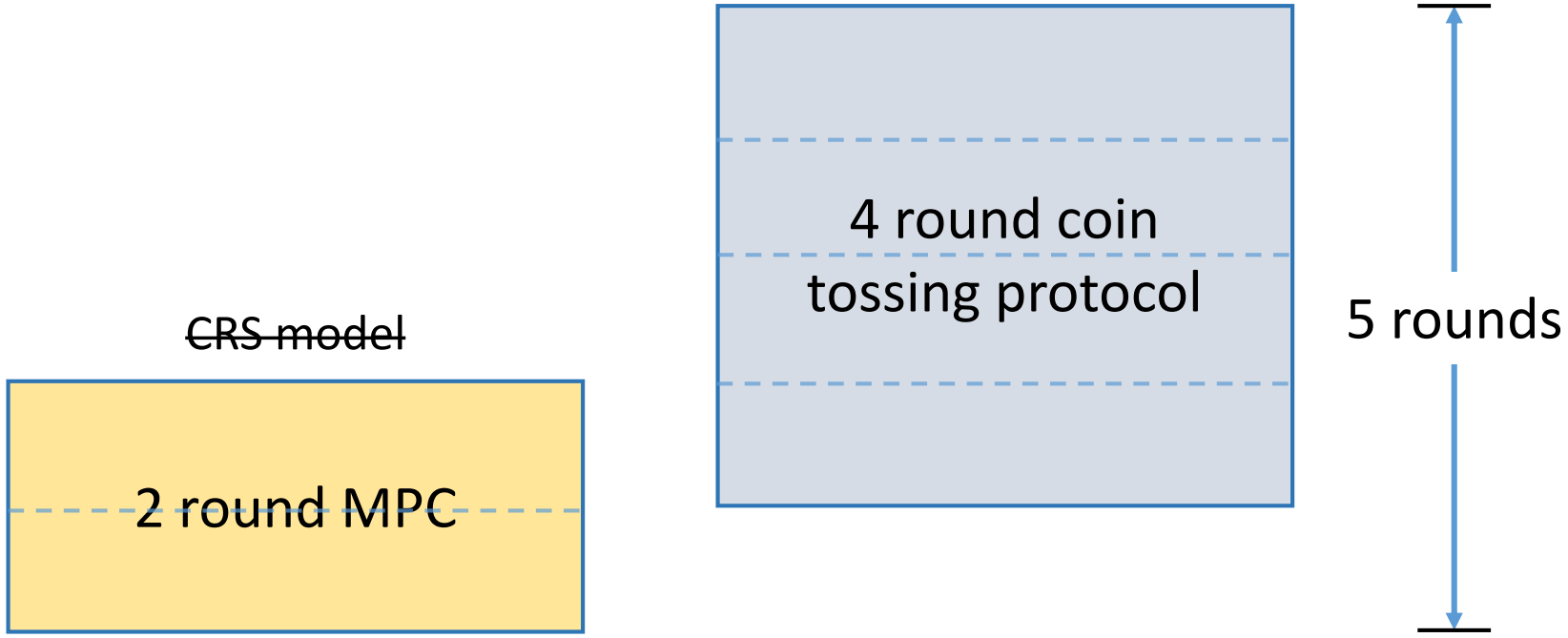
[Garg-Mukherjee-Pandey-Polychroniadou 16] template



Limitations of this approach:

Unclear how to parallelize both rounds.

[Garg-Mukherjee-Pandey-Polychroniadou 16] template



Limitations of this approach:

Unclear how to parallelize both rounds.

Limits to the 2 round MPC assumptions.

[Goldreich-Micali-Wigderson 87]

GMW compiler.

[Goldreich-Micali-Wigderson 87]

GMW compiler.

Semi-honest to malicious security.

[Goldreich-Micali-Wigderson 87]

Coin tossing

GMW compiler.

Semi-honest to malicious security.

[Goldreich-Micali-Wigderson 87]

Coin tossing

GMW compiler.

Semi-honest to malicious security.

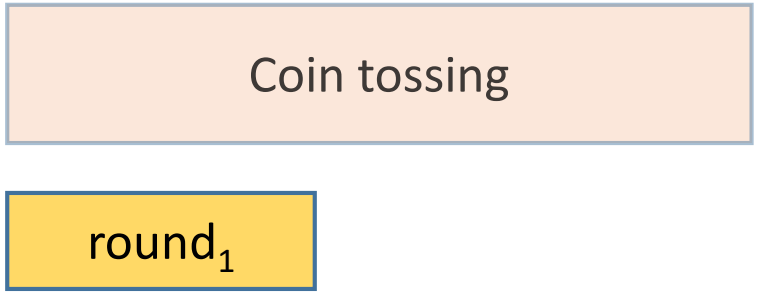
Proof of honest behavior with each round.

[Goldreich-Micali-Wigderson 87]

GMW compiler.

Semi-honest to malicious security.

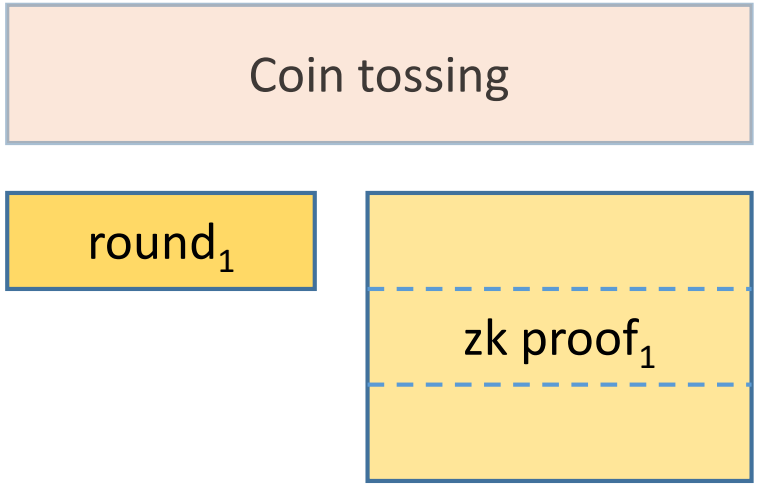
Proof of honest behavior with each round.



[Goldreich-Micali-Wigderson 87]

GMW compiler.

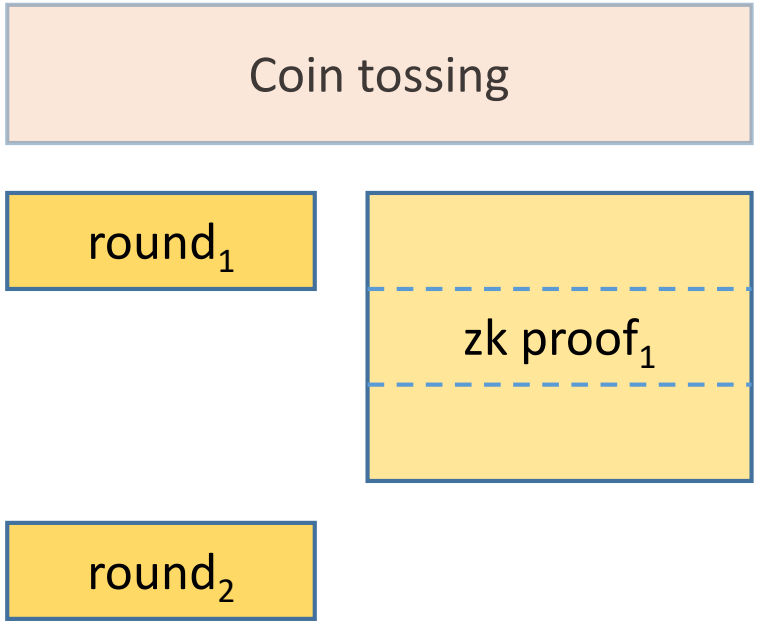
- Semi-honest to malicious security.
- Proof of honest behavior with each round.



[Goldreich-Micali-Wigderson 87]

GMW compiler.

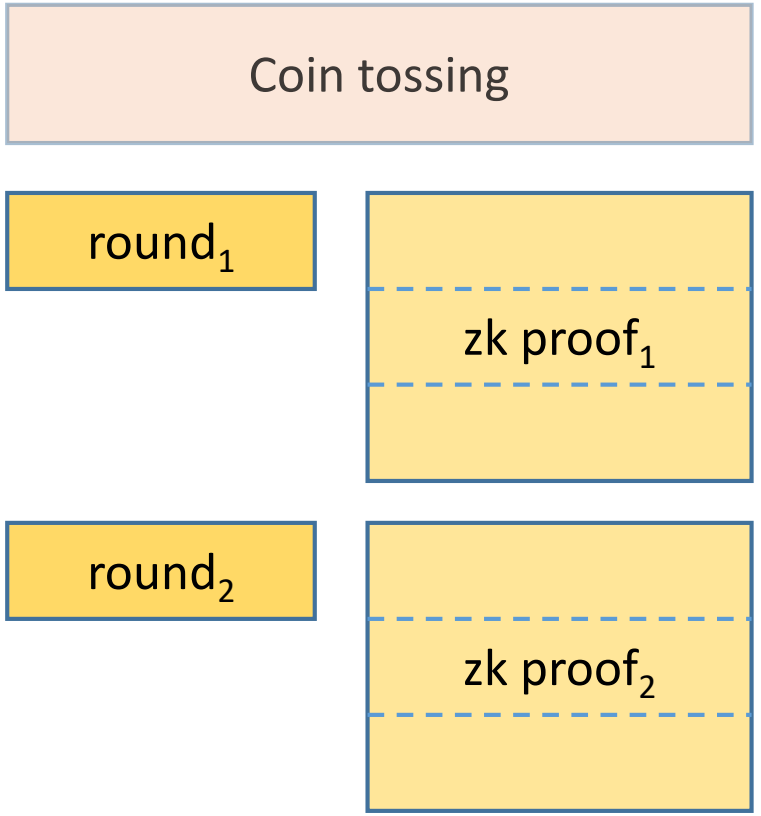
- Semi-honest to malicious security.
- Proof of honest behavior with each round.



[Goldreich-Micali-Wigderson 87]

GMW compiler.

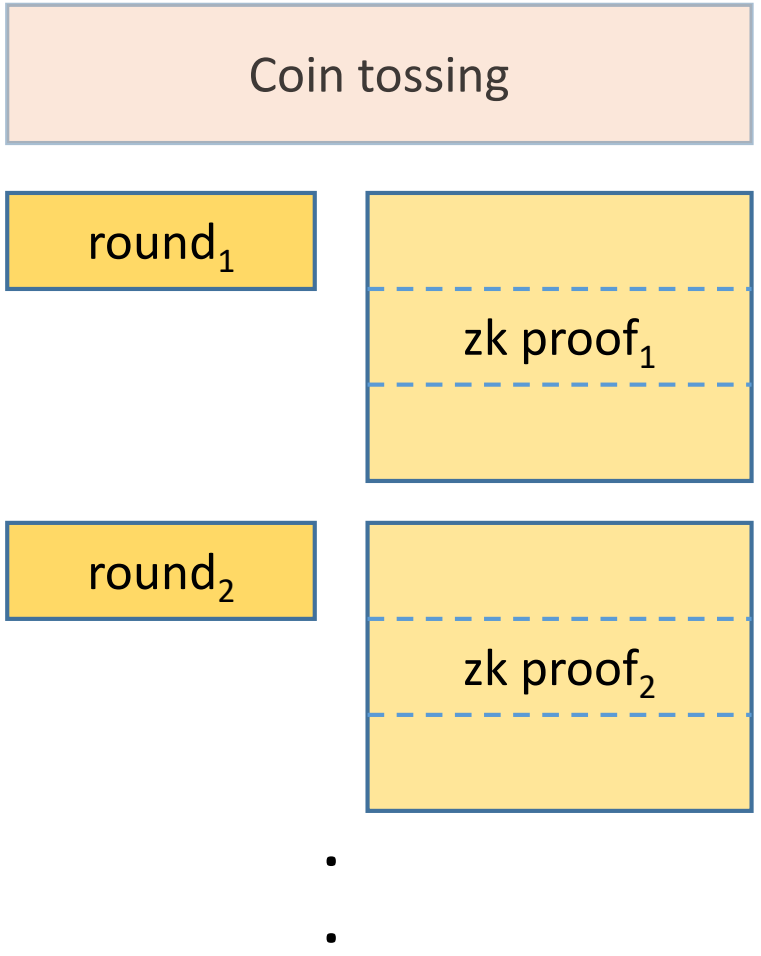
- Semi-honest to malicious security.
- Proof of honest behavior with each round.



[Goldreich-Micali-Wigderson 87]

GMW compiler.

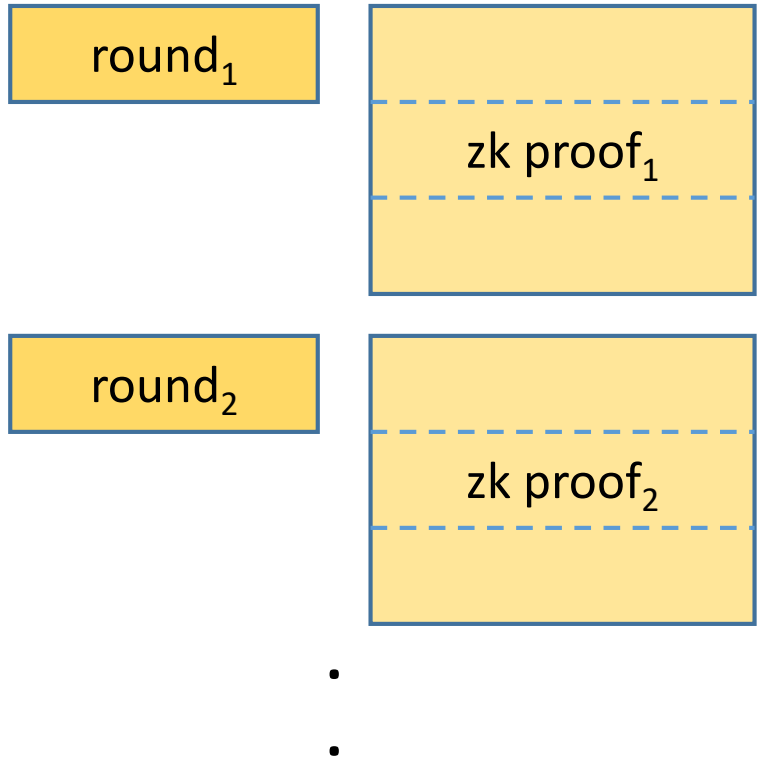
- Semi-honest to malicious security.
- Proof of honest behavior with each round.



[Goldreich-Micali-Wigderson 87]

GMW compiler.

- Semi-honest to malicious security.
- Proof of honest behavior with each round.



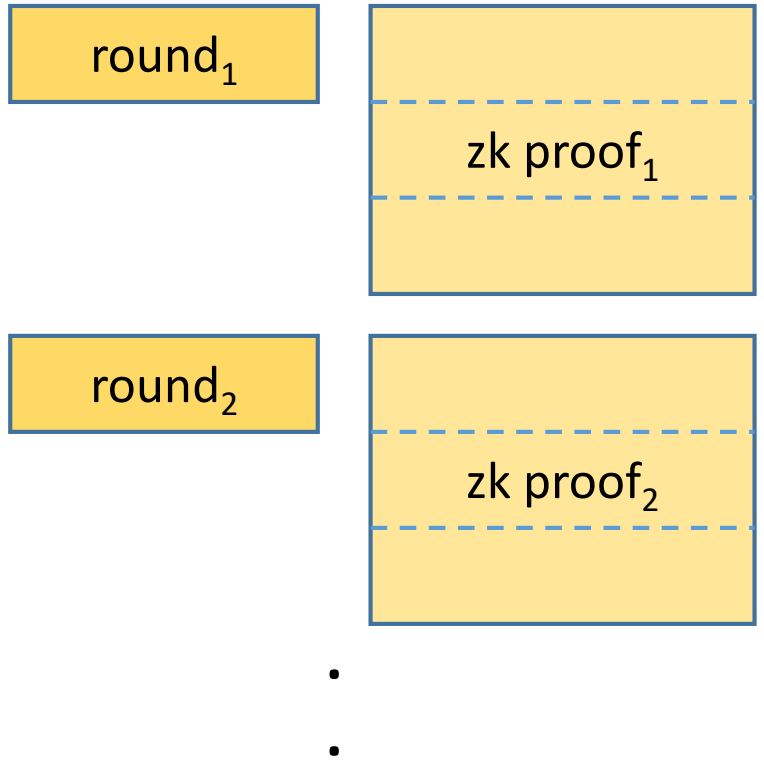
[Goldreich-Micali-Wigderson 87]

GMW compiler.

Semi-honest to malicious security.

Proof of honest behavior with each round.

Main challenge is to reduce the number of proofs.

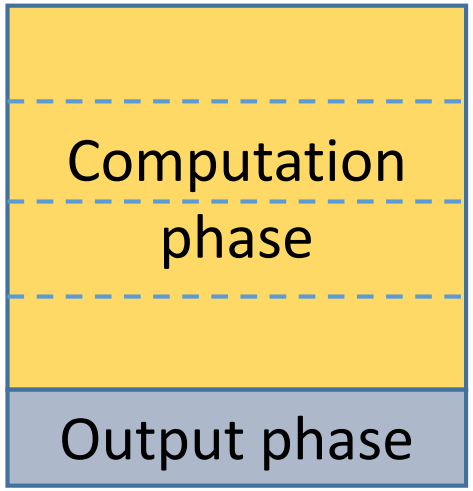


Our strategy

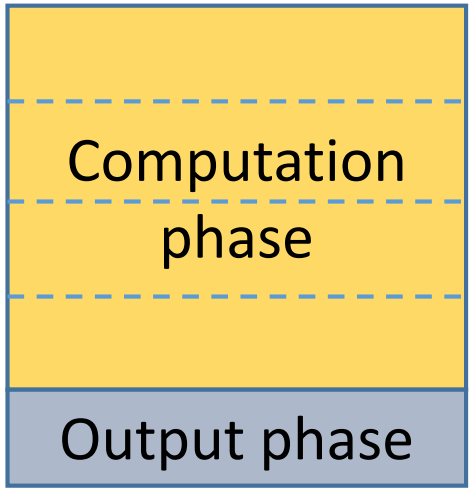
Semi-honest protocol

Our strategy

Semi-honest protocol

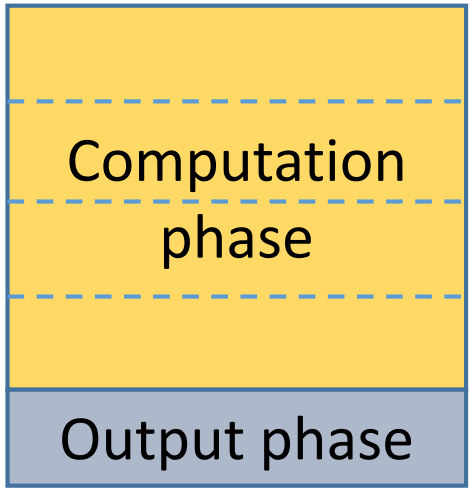


Our strategy



Semi-honest protocol whose structure is satisfied by most MPC protocols.

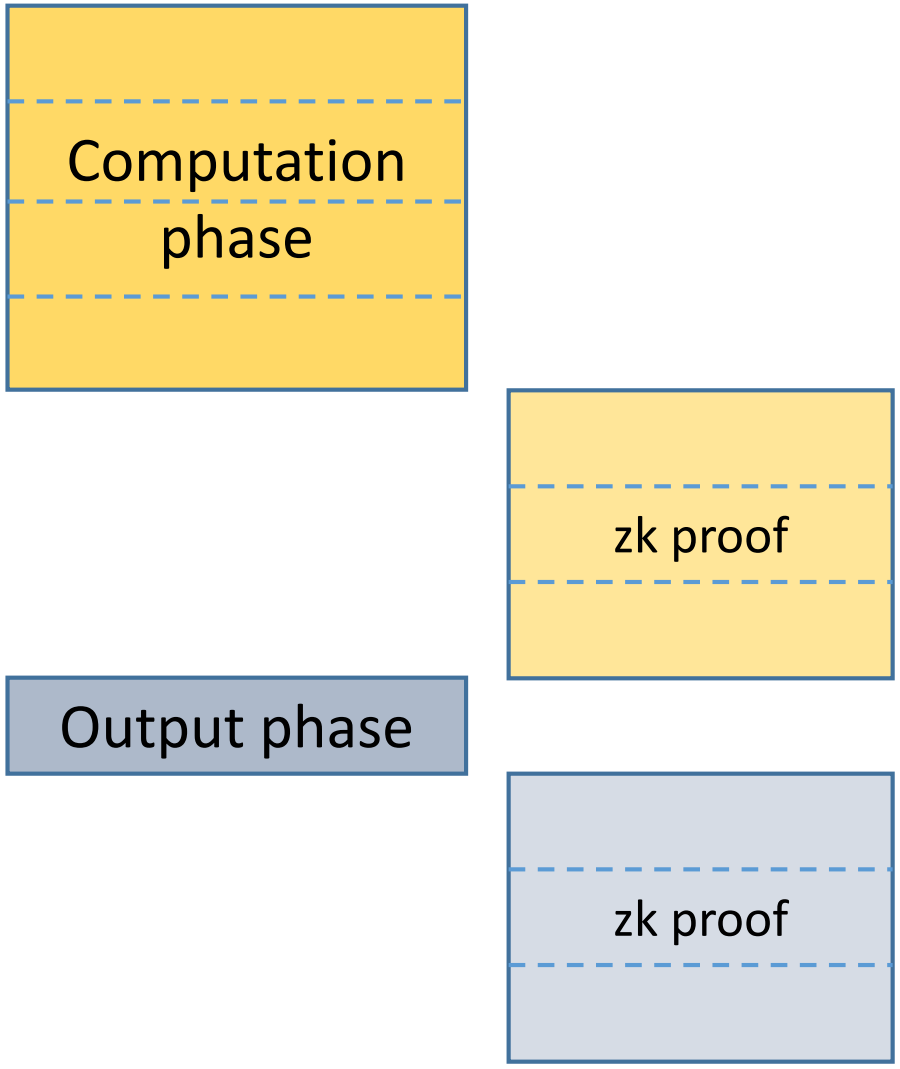
Our strategy



Semi-honest protocol whose structure is satisfied by most MPC protocols.

Prove honest behavior once for the computation phase?

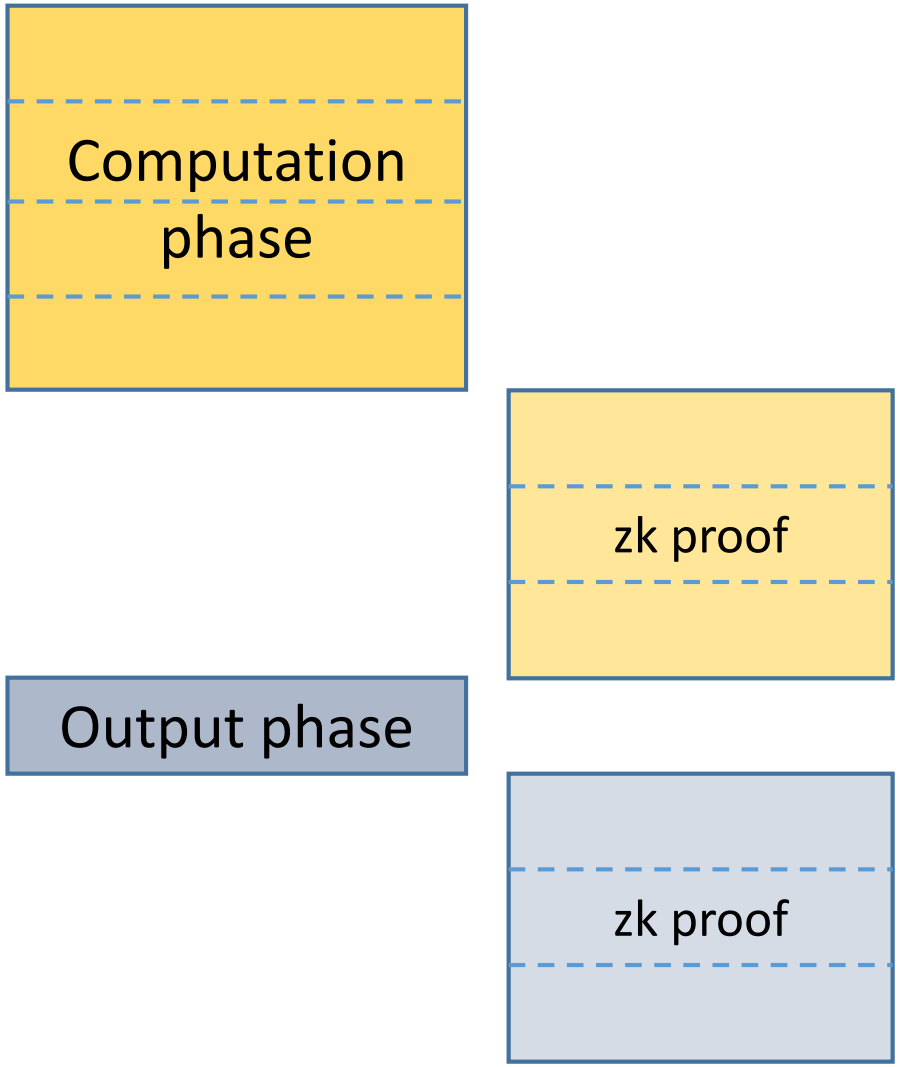
Our strategy



Semi-honest protocol whose structure is satisfied by most MPC protocols.

Prove honest behavior once for the computation phase?

Our strategy

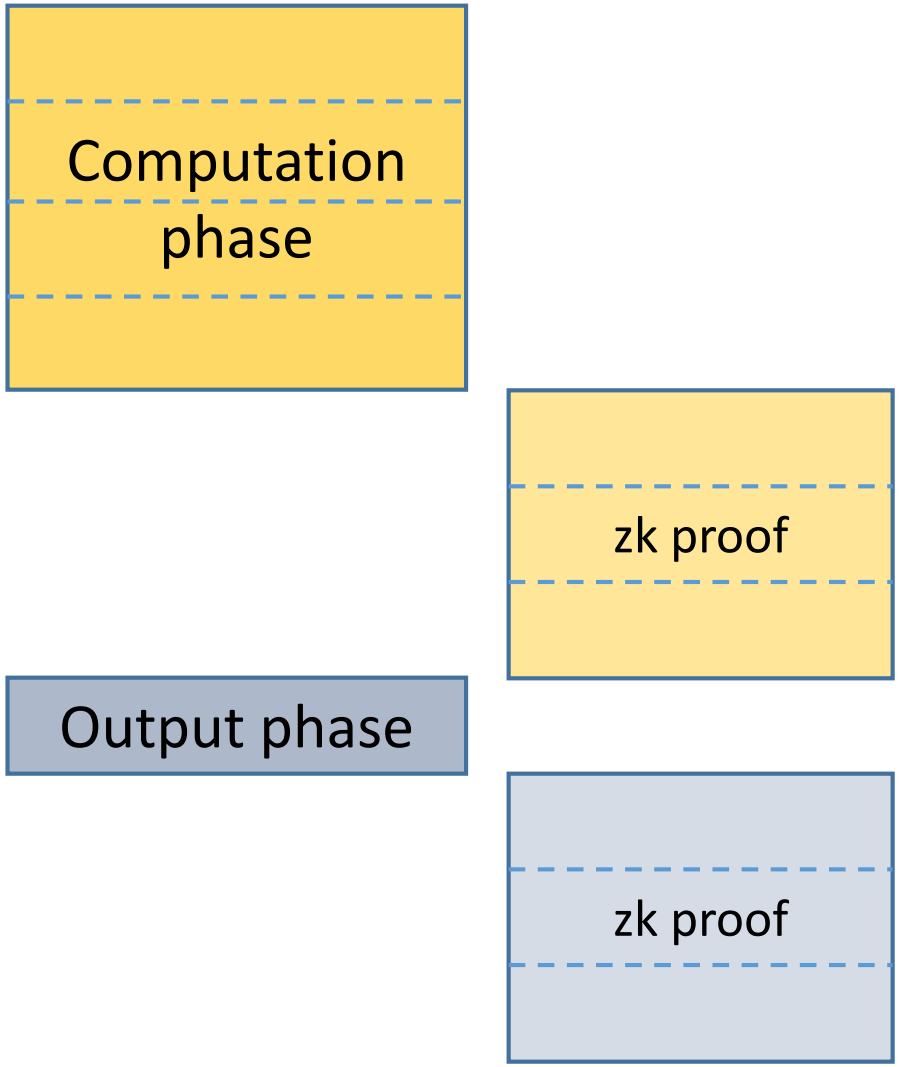


Semi-honest protocol whose structure is satisfied by most MPC protocols.

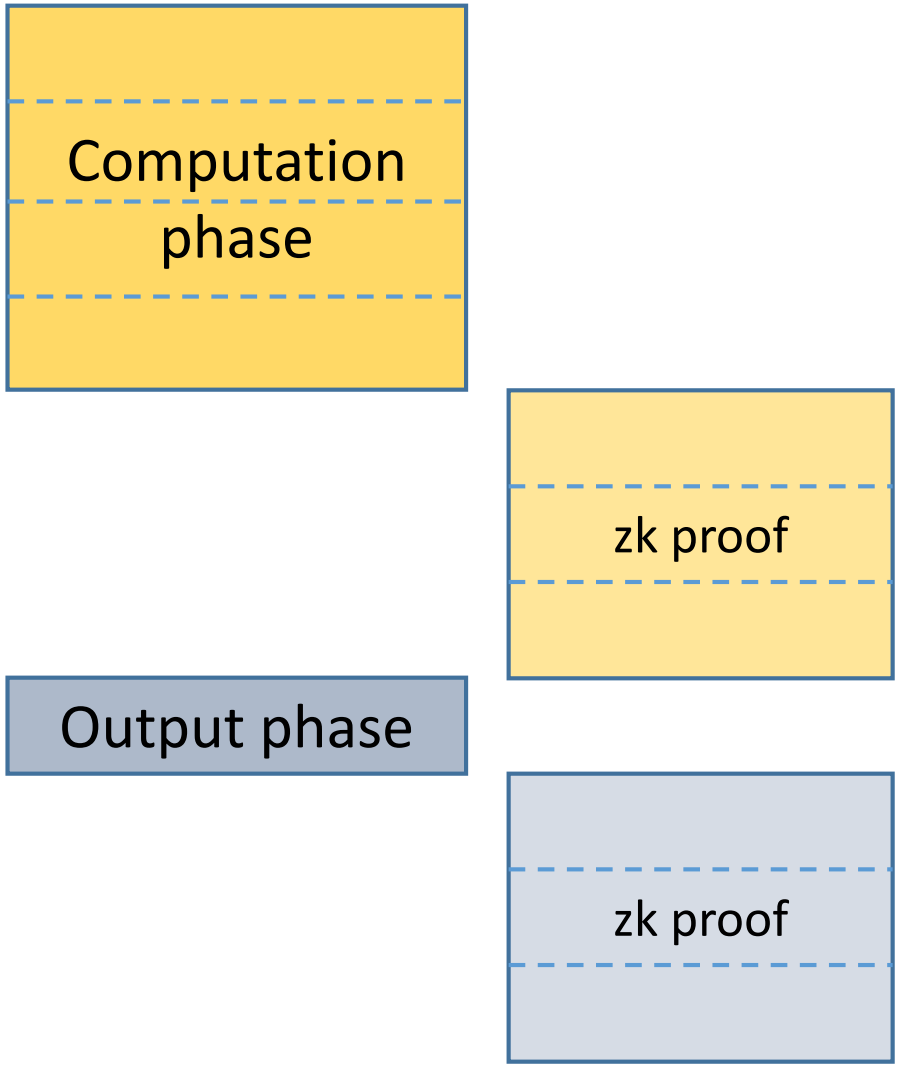
Prove honest behavior once for the computation phase?

Might be too late.

Our strategy

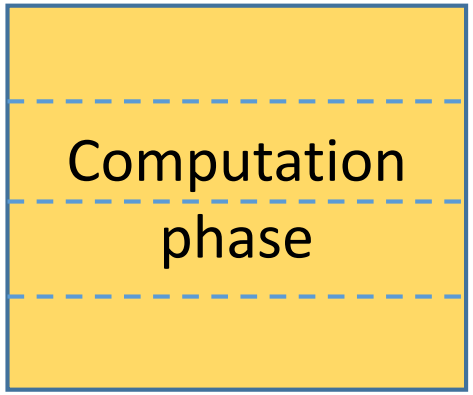


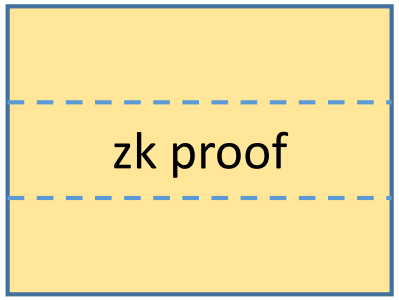
Our strategy

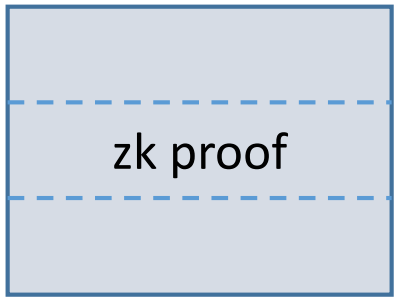


Require additional property

Our strategy



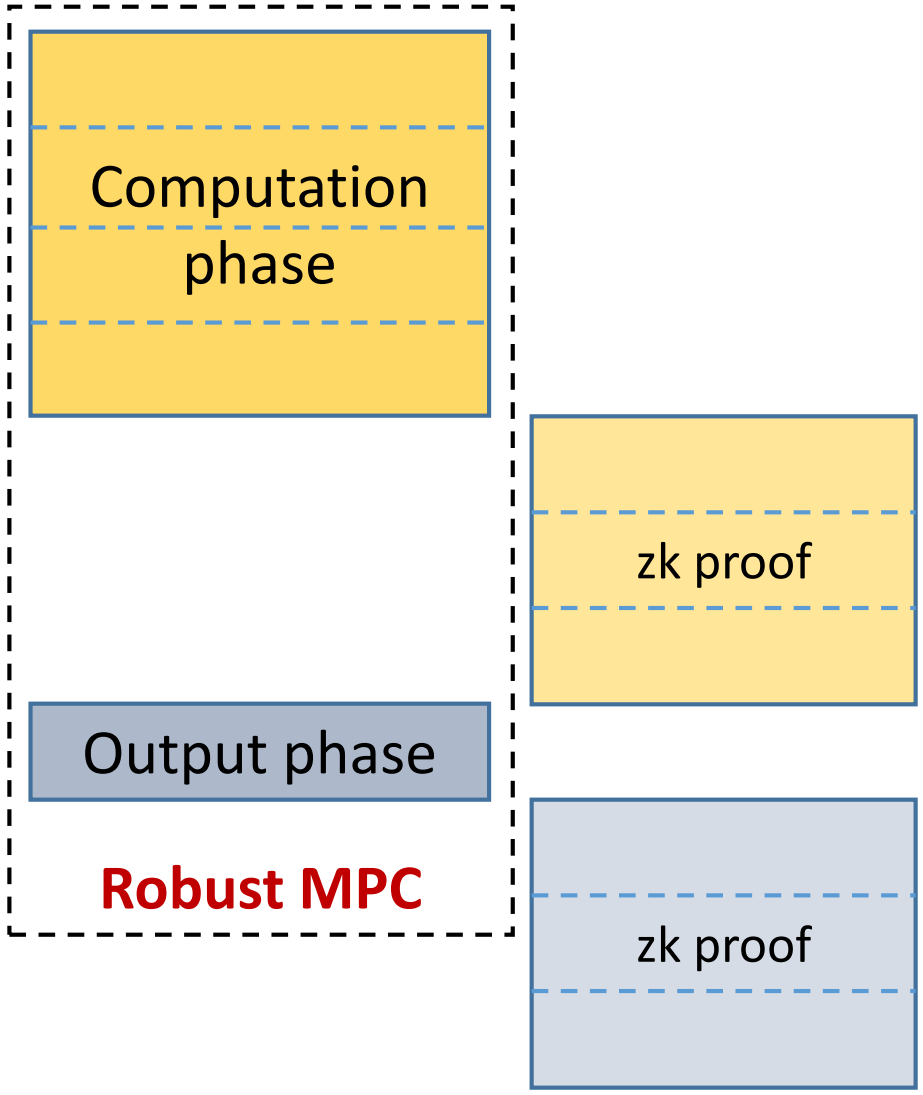




Require additional property: Robustness

Computation phase:
maintains privacy against malicious adversaries till end of phase, however the correctness of computation is not guaranteed.

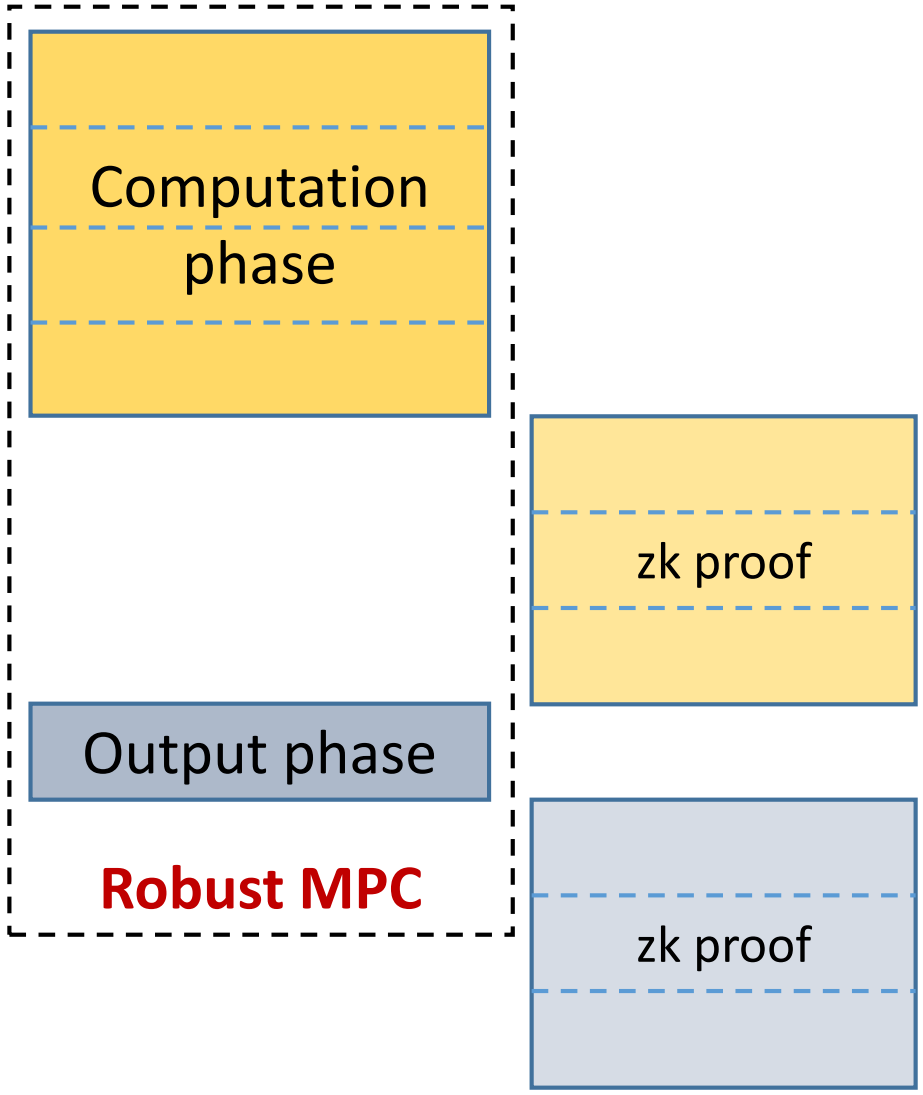
Our strategy



Require additional property: Robustness

Computation phase:
maintains privacy against malicious adversaries till end of phase, however the correctness of computation is not guaranteed.

Our strategy: Delayed verification

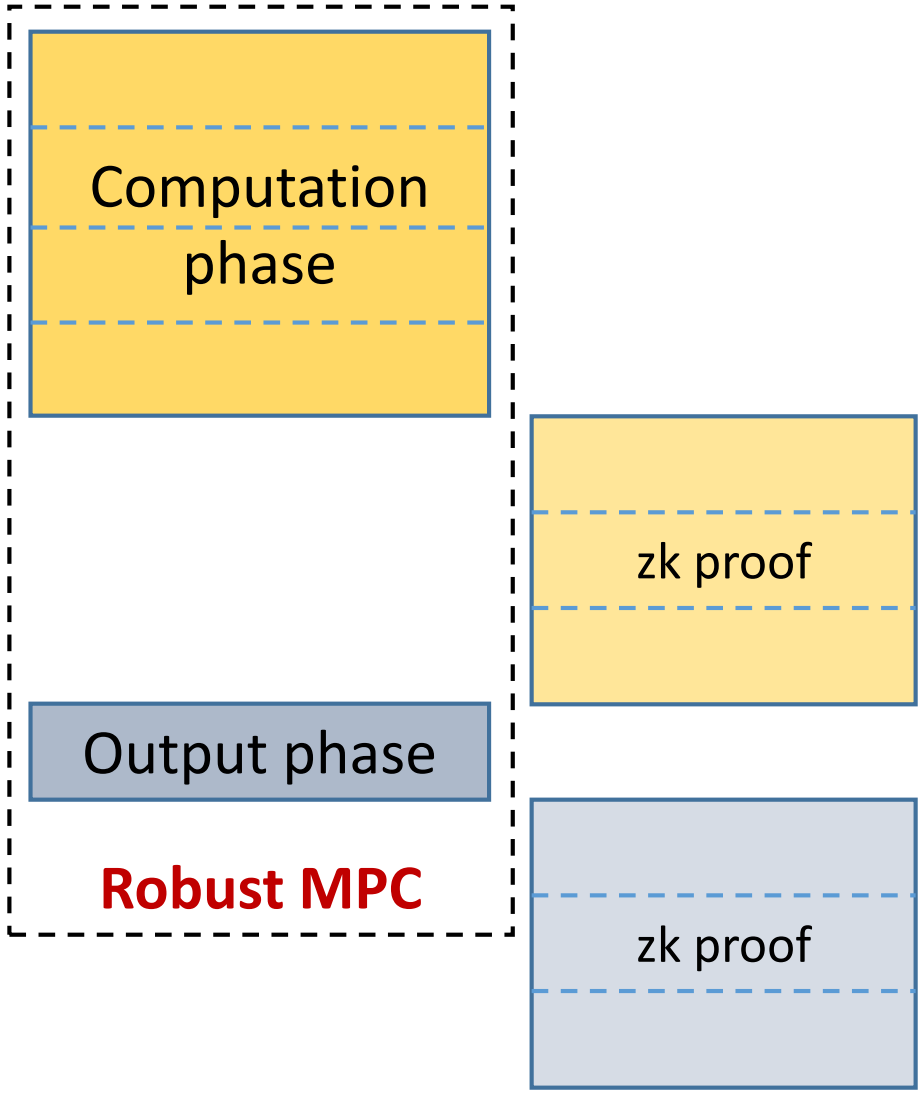


Require additional property: Robustness

Computation phase:
maintains privacy against malicious adversaries till end of phase, however the correctness of computation is not guaranteed.

Delayed verification.

Our strategy: Delayed verification



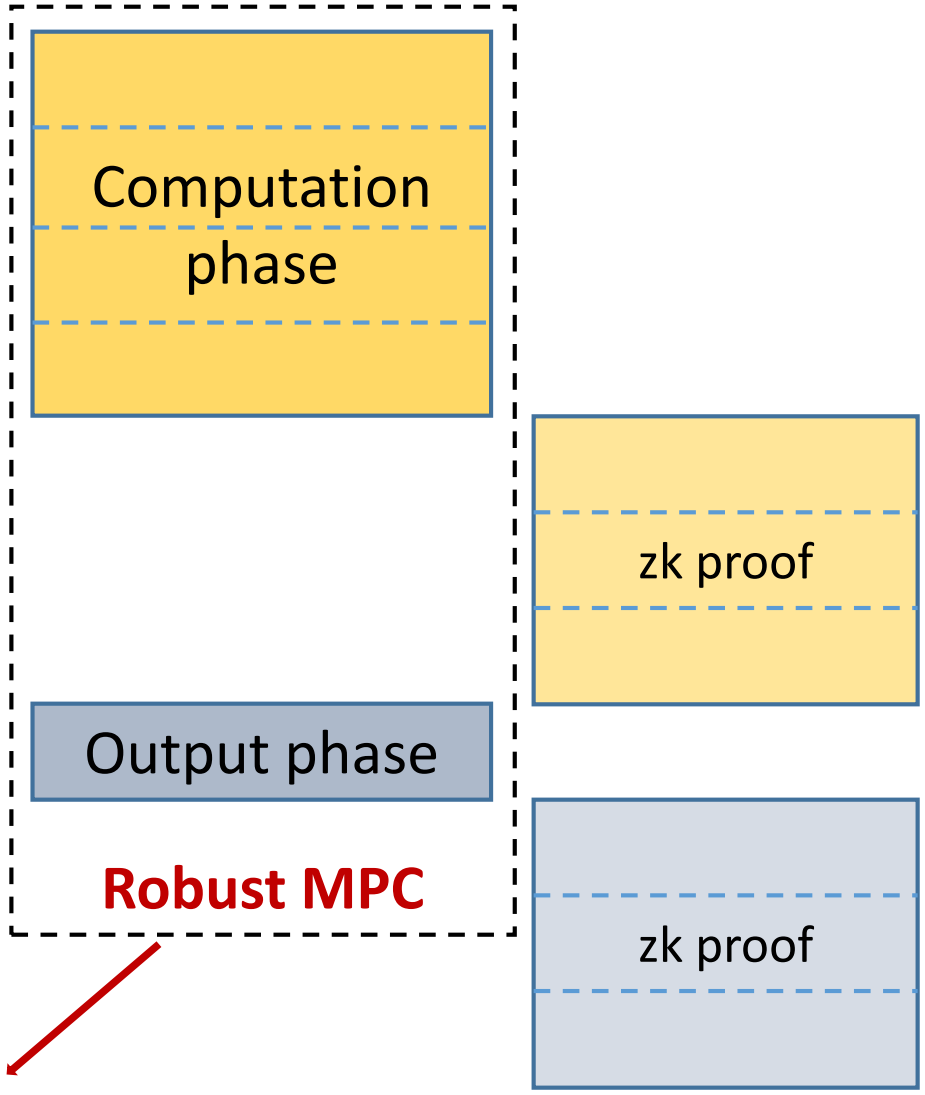
Require additional property: Robustness

Computation phase:
maintains privacy against malicious adversaries till end of phase, however the correctness of computation is not guaranteed.

Delayed verification.

Developed by [Chandran-Goyal-Ostrovsky-Sahai07] in a different context.

Our strategy: Delayed verification



Require additional property: Robustness

Computation phase:
maintains privacy against malicious adversaries till end of phase, however the correctness of computation is not guaranteed.

Delayed verification.

Developed by [Chandran-Goyal-Ostrovsky-Sahai07] in a different context.

Already secure against bad randomness.

Rest of the talk

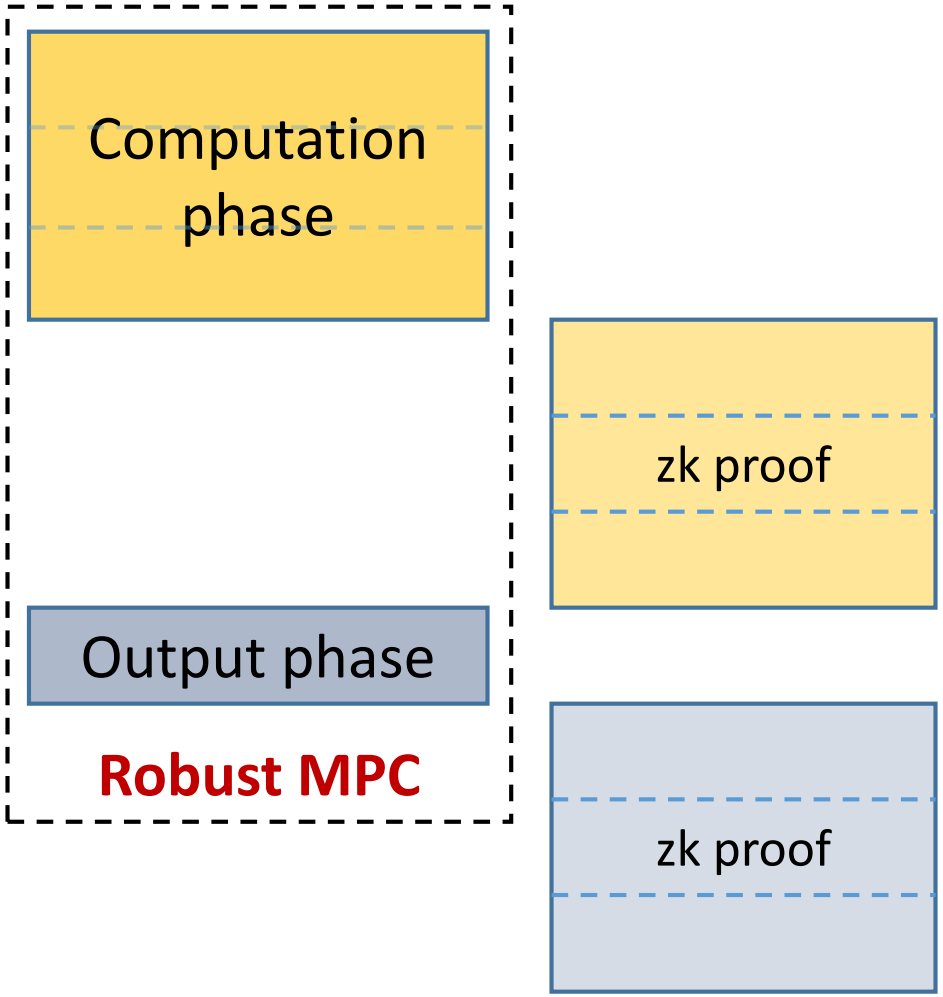
Compiler from

- 4 round robust MPC to 5 round protocol
- 4 round robust MPC to 4 round protocol

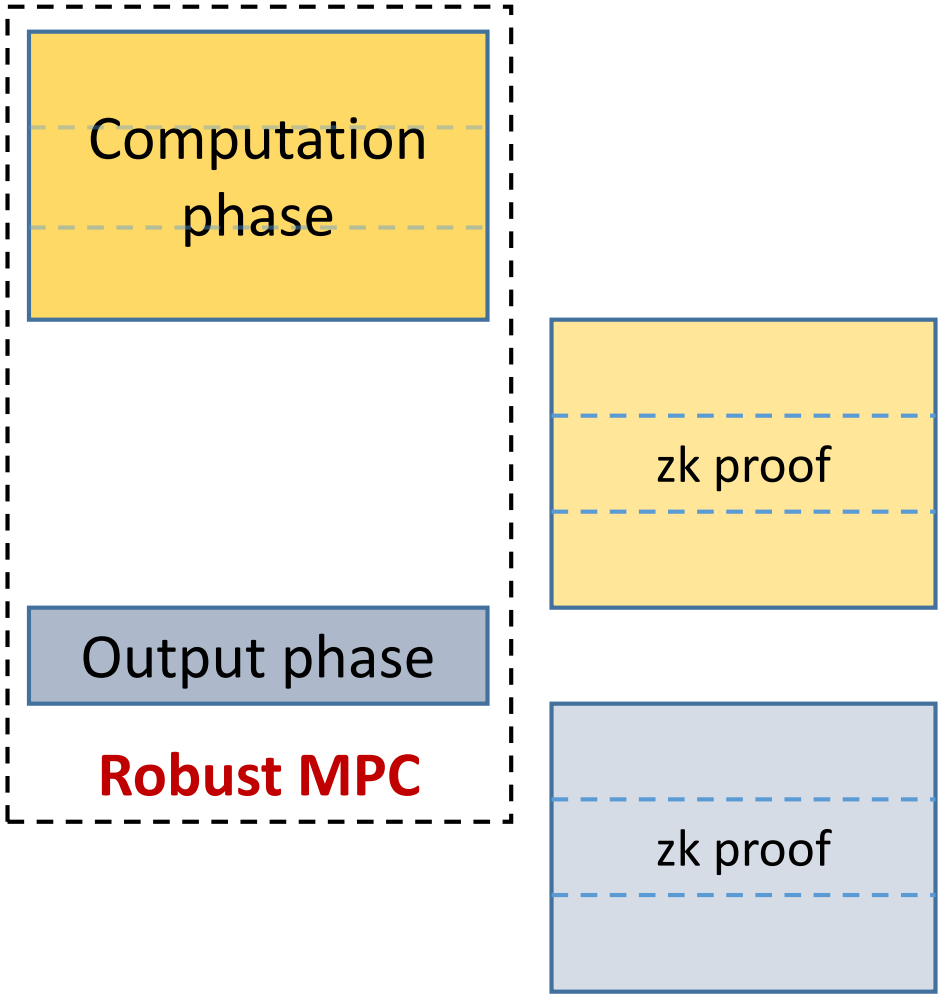
Construction of 4 round robust MPC

5 Round Protocol

Blueprint of 5 round protocol

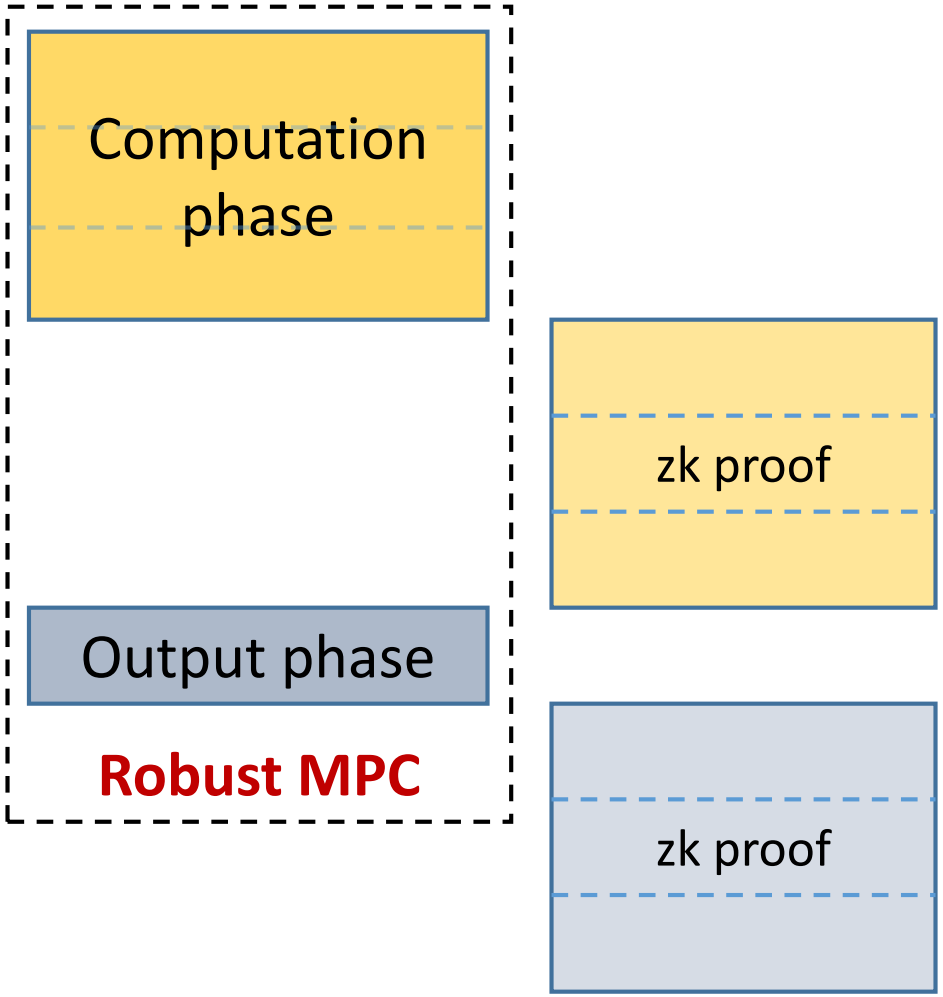


Blueprint of 5 round protocol



Parallelize proofs.

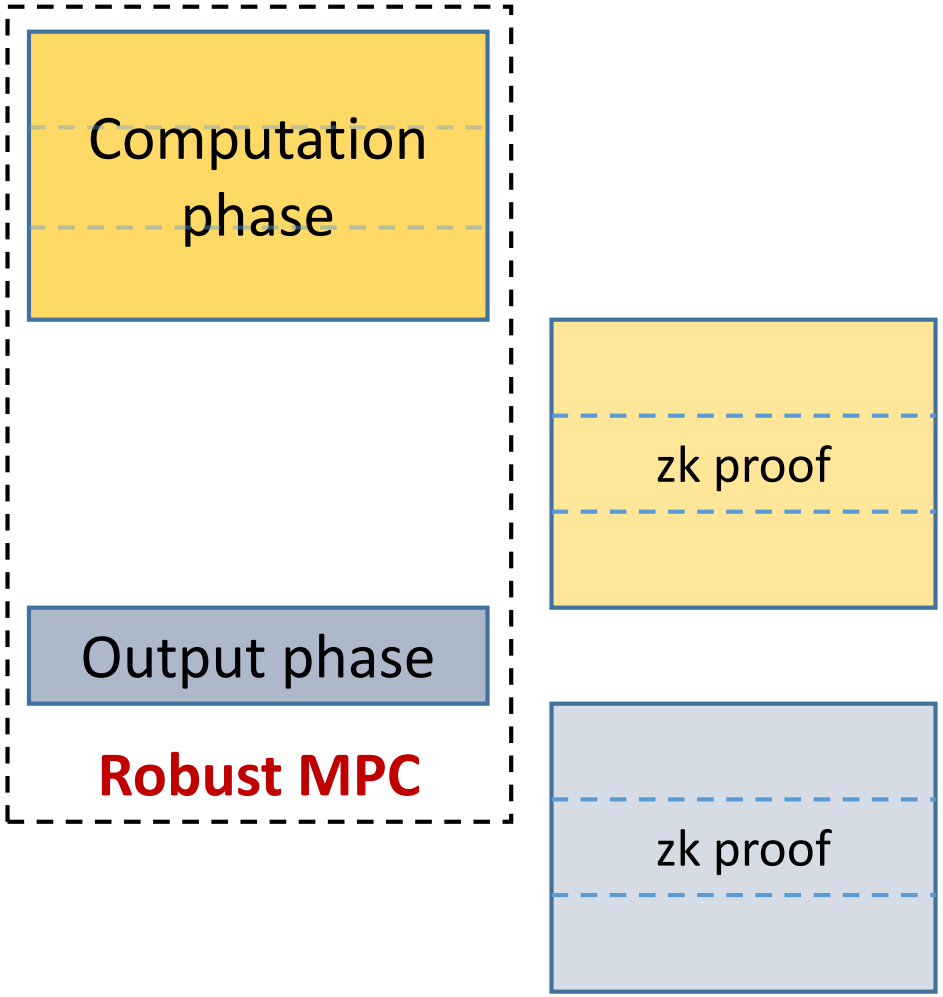
Blueprint of 5 round protocol



Parallelize proofs.

Input delayed proofs [LS90].

Blueprint of 5 round protocol

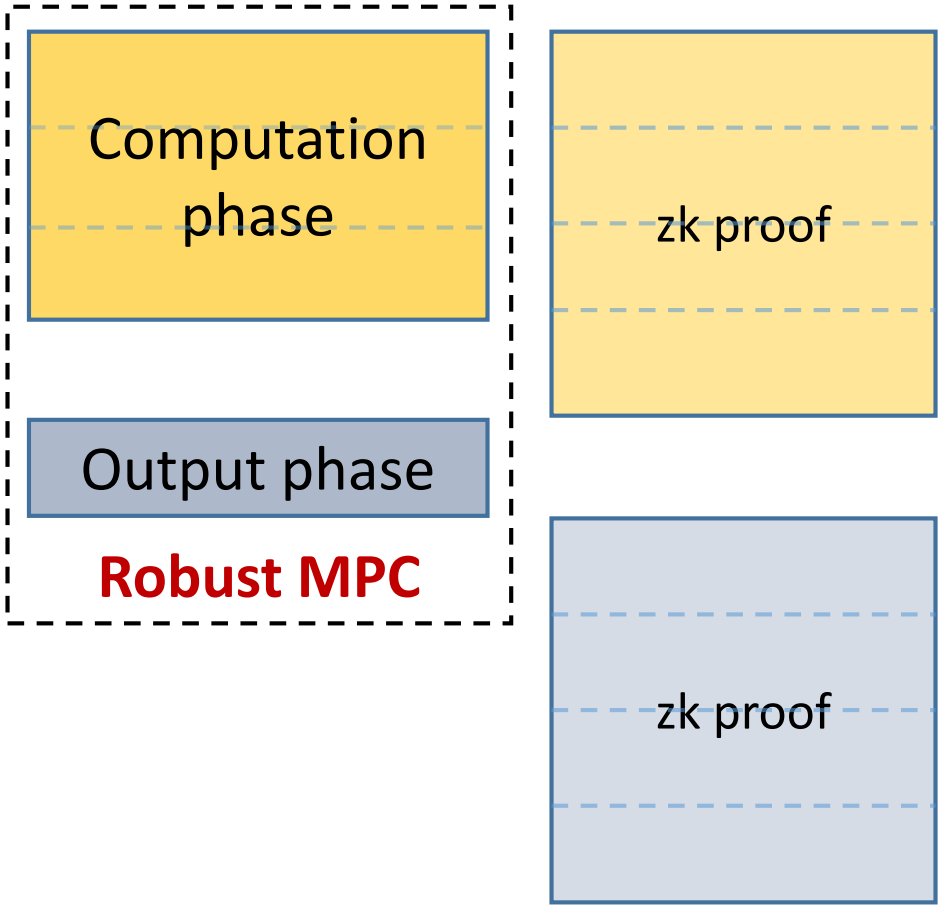


Parallelize proofs.

Input delayed proofs [LS90].

3 round ZK with black-box simulation impossible [GK96].

Blueprint of 5 round protocol

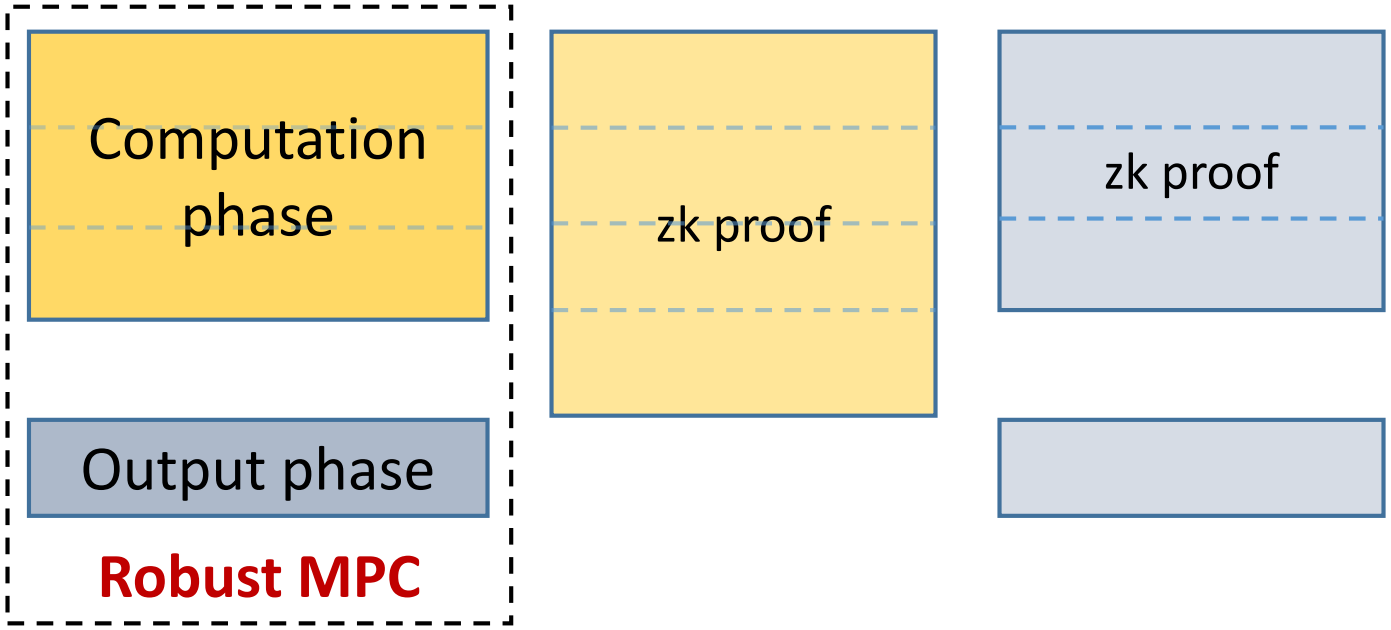


Parallelize proofs.

Input delayed proofs [LS90].

3 round ZK with black-box simulation impossible [GK96].

Blueprint of 5 round protocol

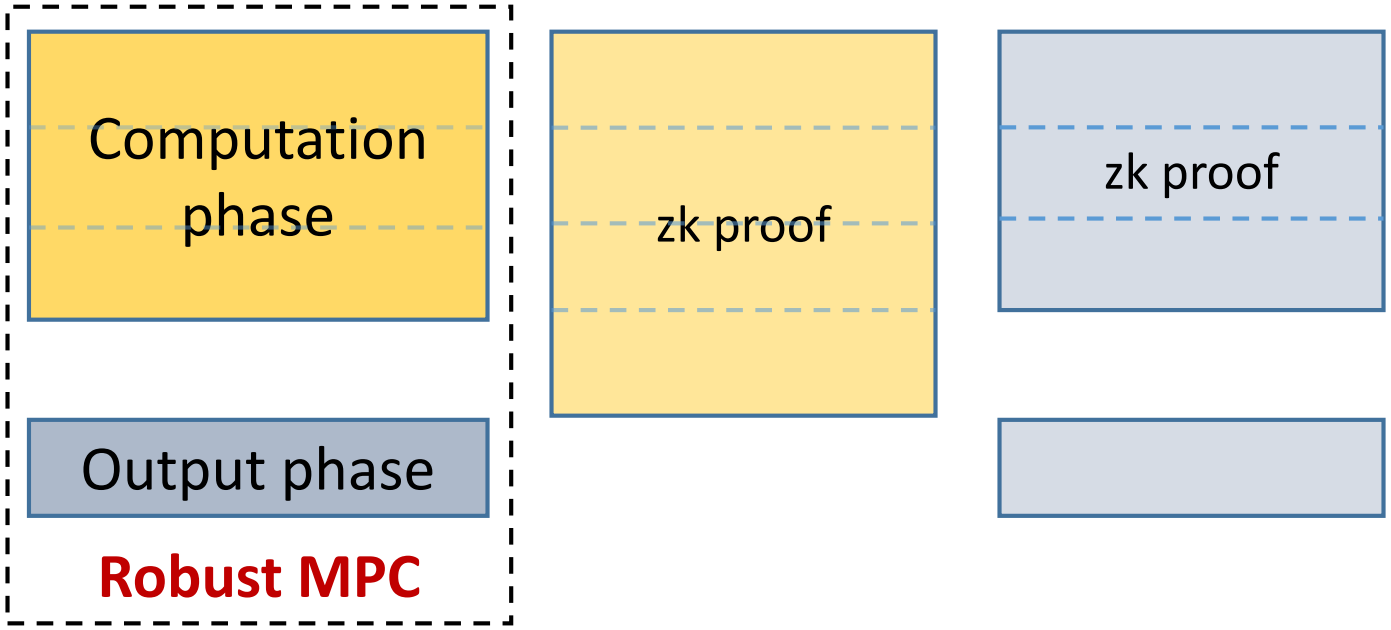


Parallelize proofs.

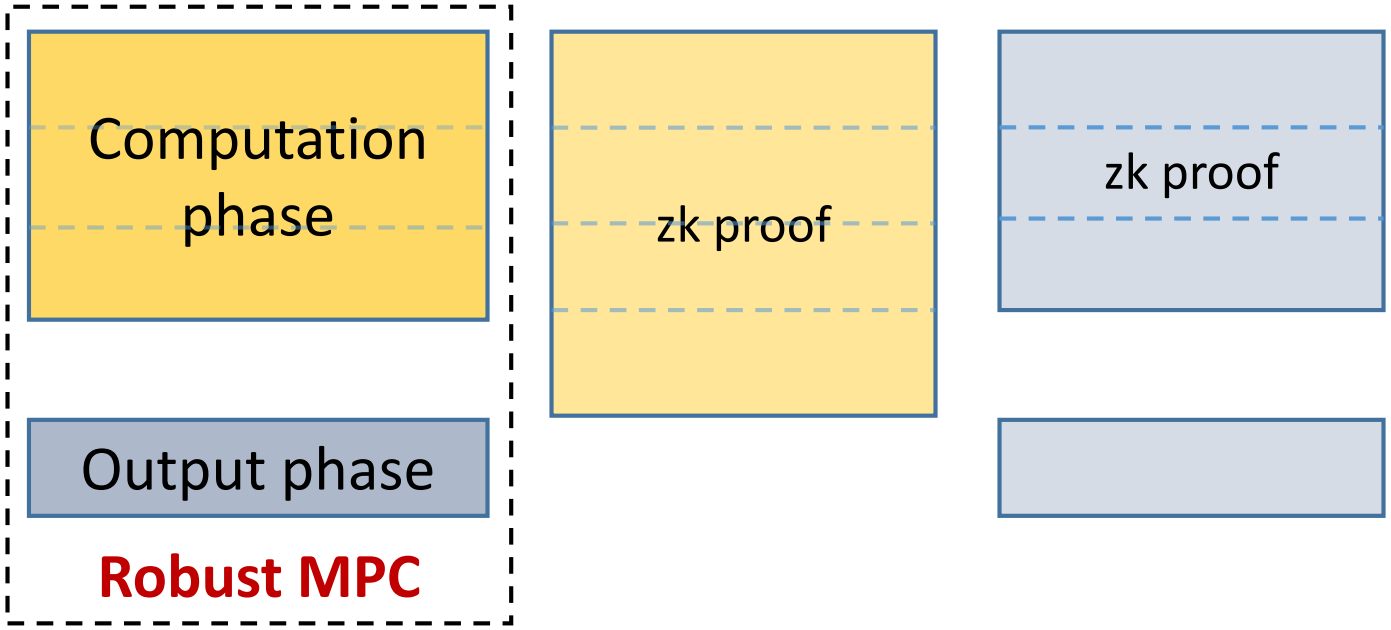
Input delayed proofs [LS90].

3 round ZK with black-box simulation impossible [GK96].

Blueprint of 5 round protocol

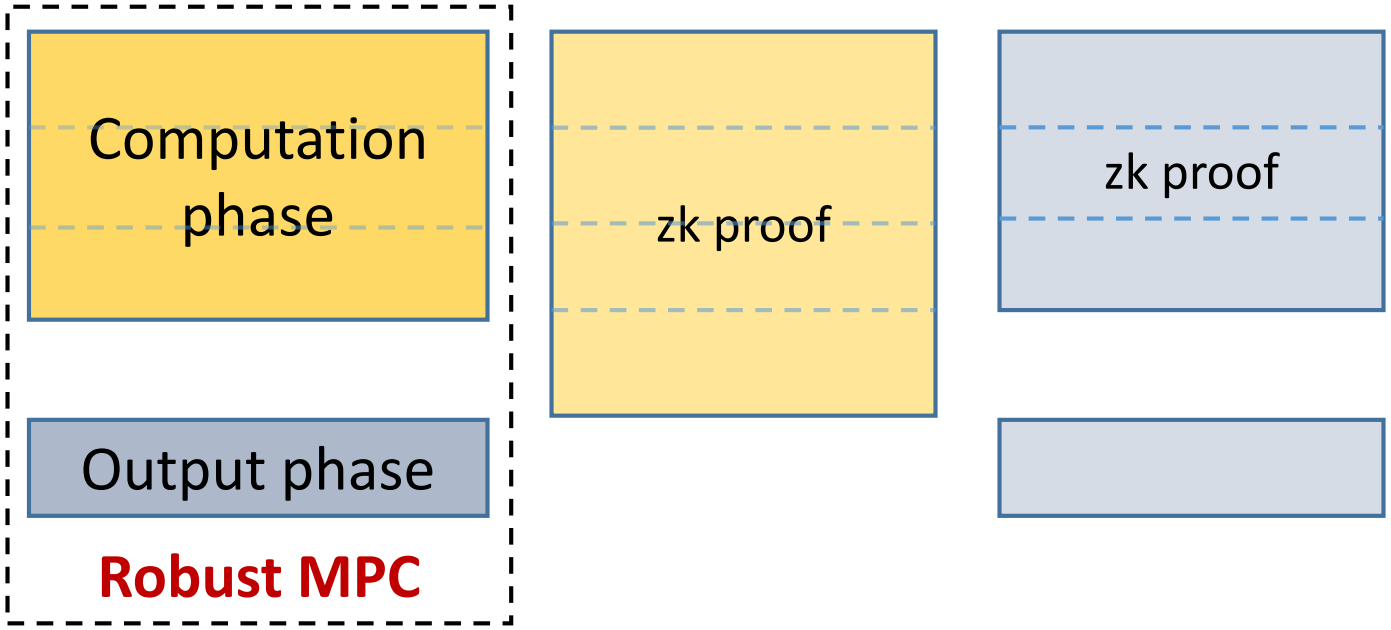


Blueprint of 5 round protocol



Non-malleability is a big challenge.

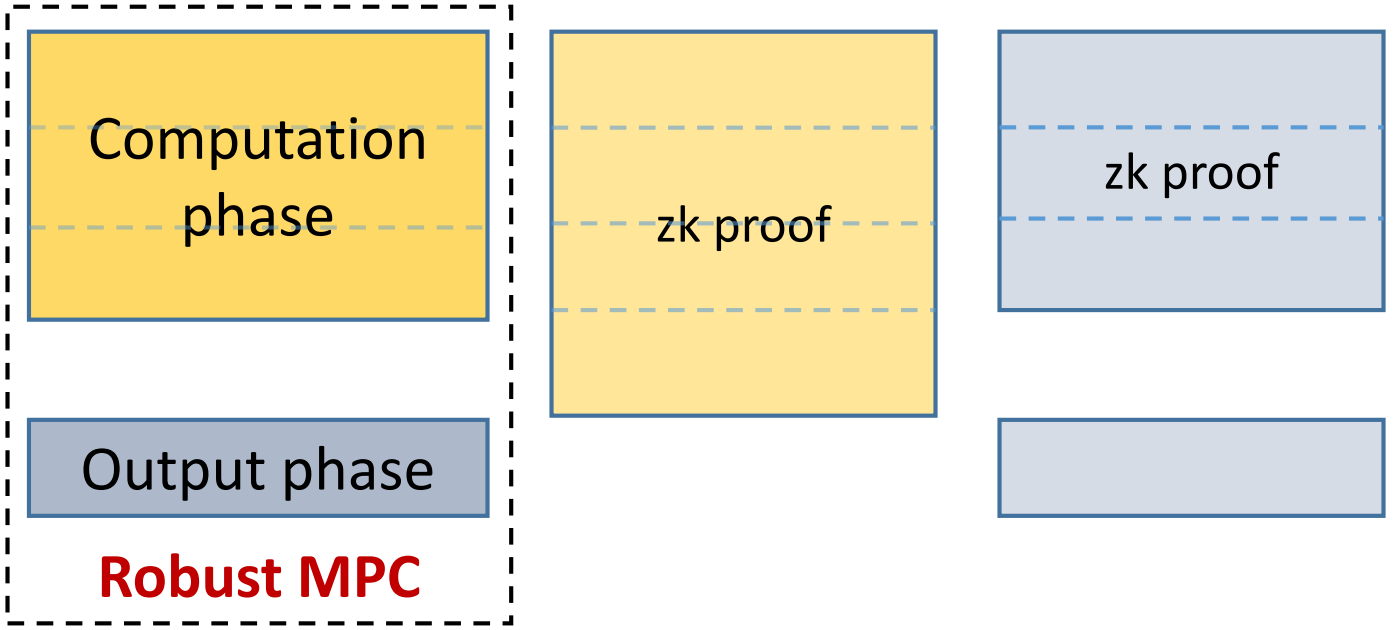
Blueprint of 5 round protocol



Non-malleability is a big challenge.

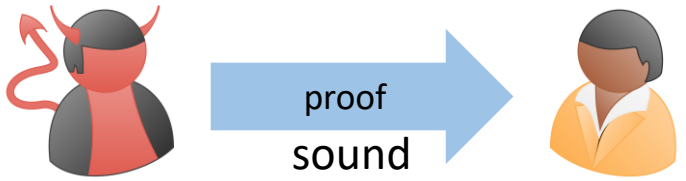
Standard soundness does not suffice.

Blueprint of 5 round protocol

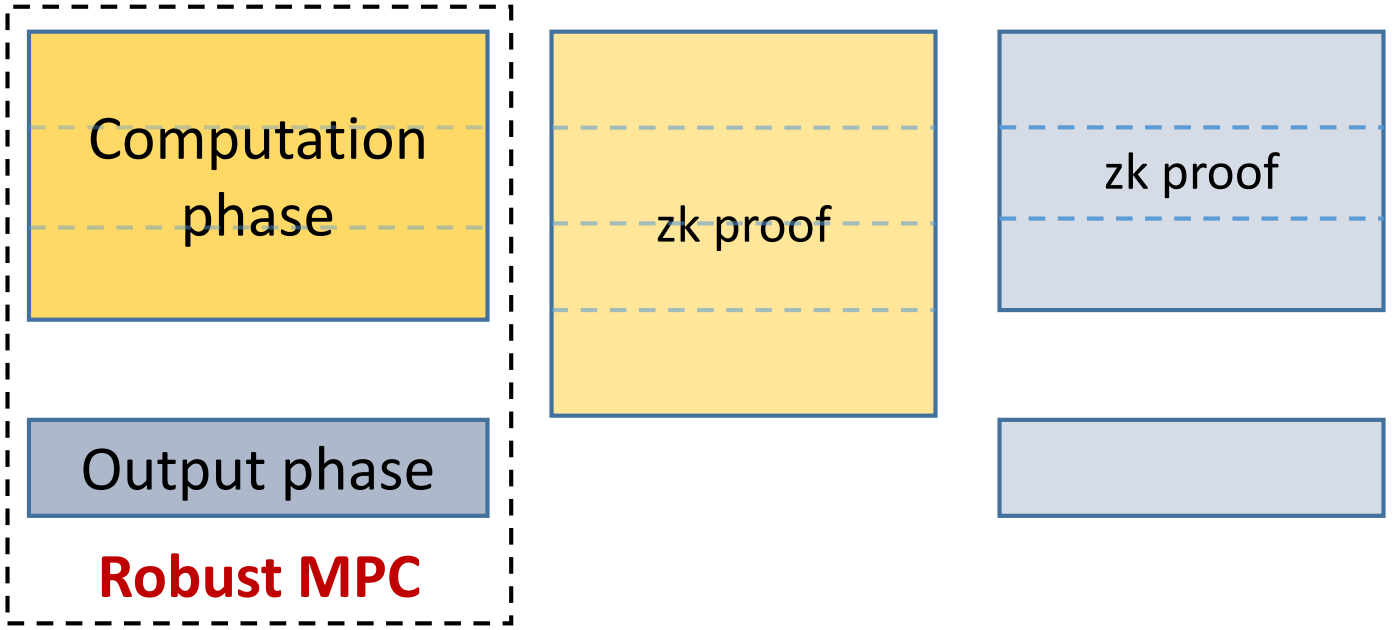


Non-malleability is a big challenge.

Standard soundness does not suffice.



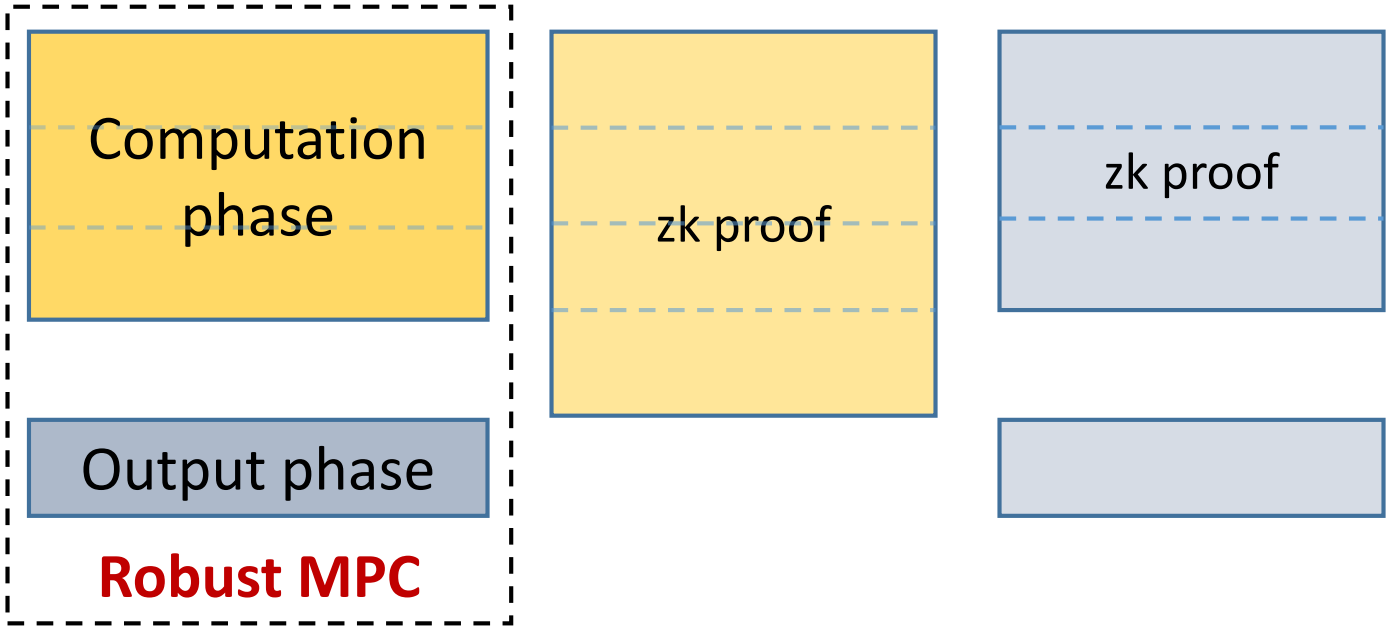
Blueprint of 5 round protocol



Non-malleability is a big challenge.

Standard soundness does not suffice.

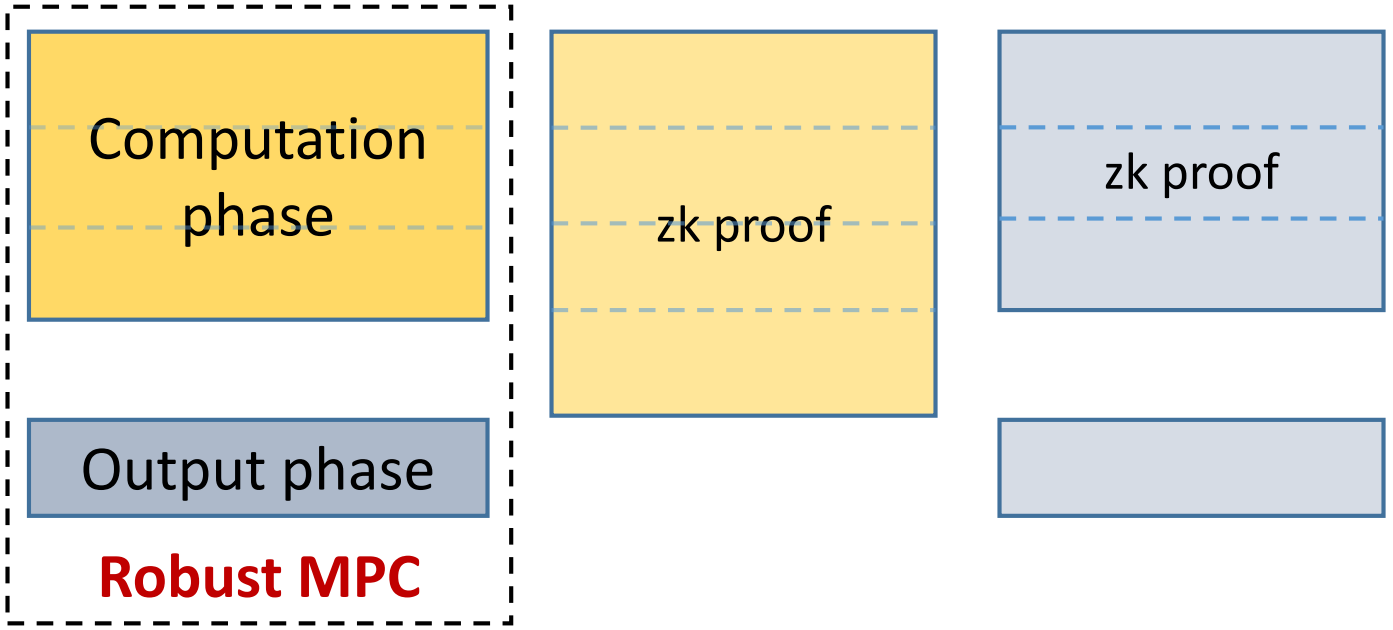
Blueprint of 5 round protocol



Non-malleability is a big challenge.

Standard soundness does not suffice.

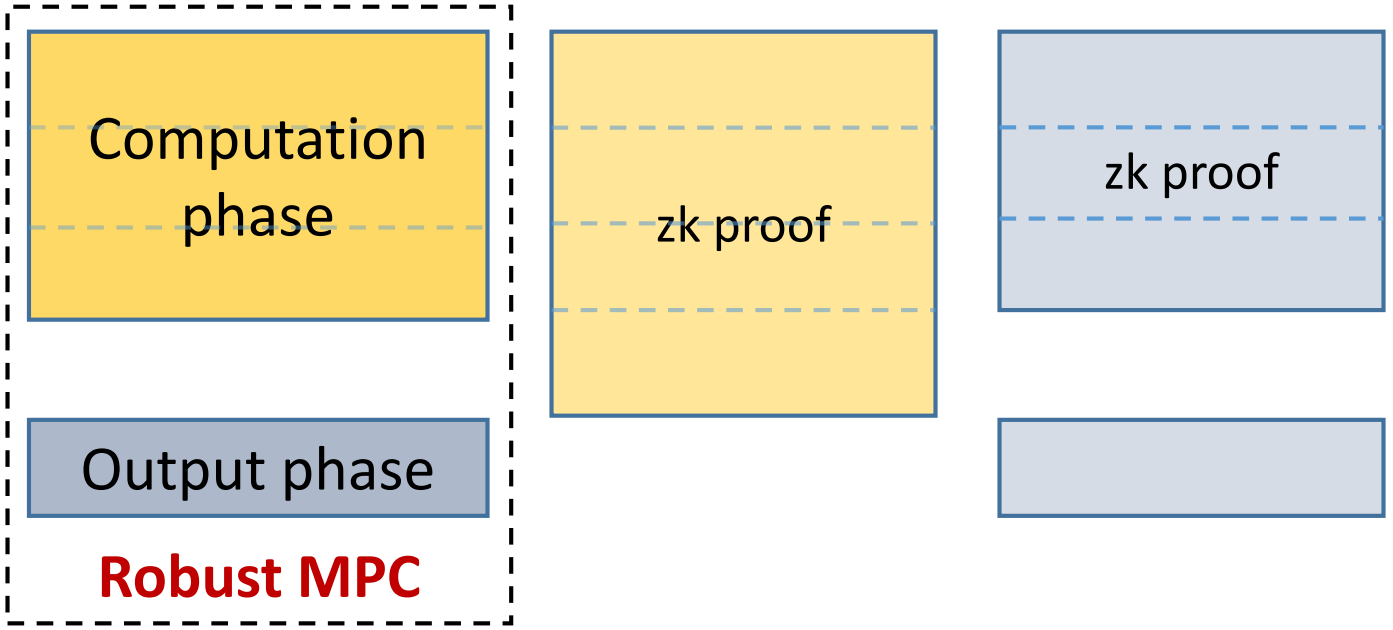
Blueprint of 5 round protocol



Non-malleability is a big challenge.

Standard soundness does not suffice.

Blueprint of 5 round protocol

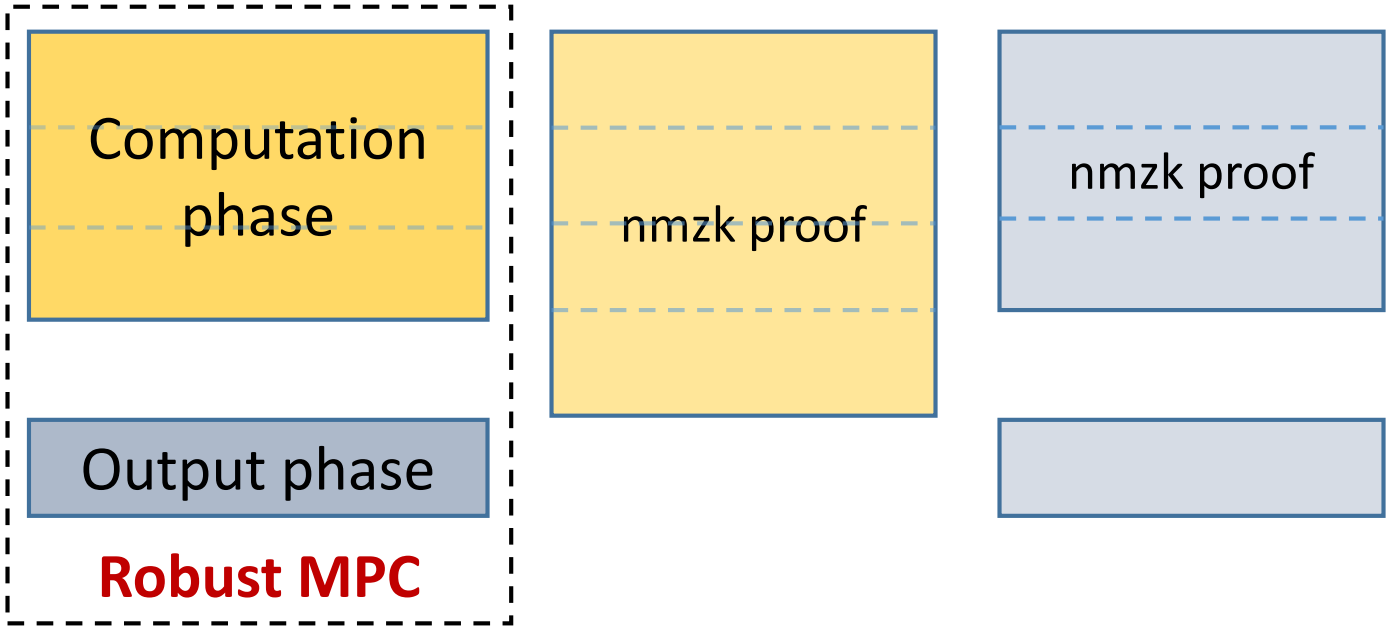


Non-malleability is a big challenge.

Standard soundness does not suffice.

simulation-soundness [DDN91,Sah99]

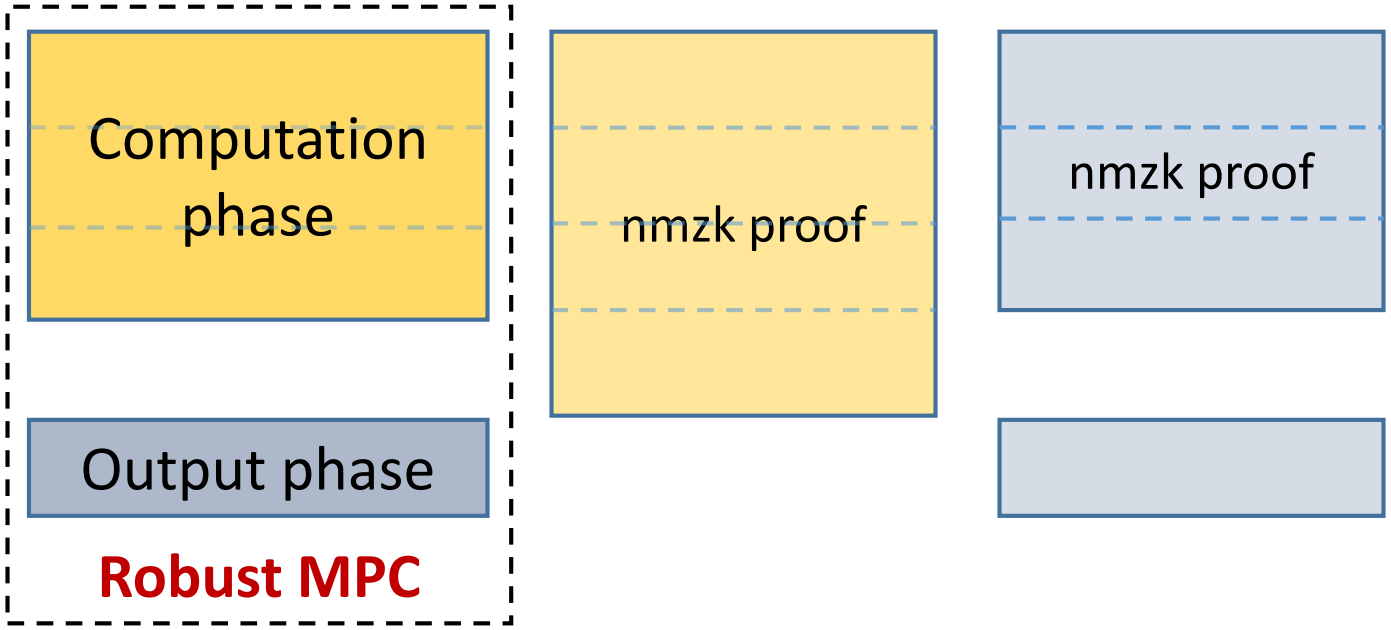
Blueprint of 5 round protocol



Non-malleability is a big challenge.

Standard soundness does not suffice.

Blueprint of 5 round protocol



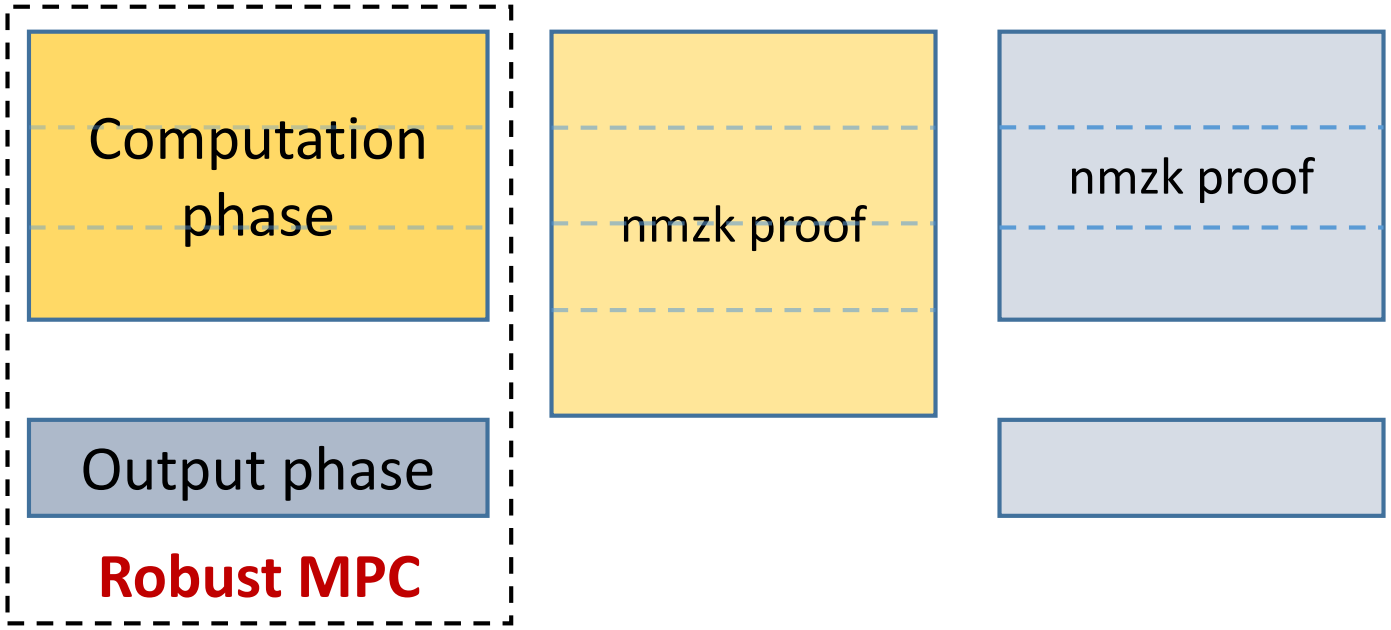
Non-malleability is a big challenge.

Standard soundness does not suffice.

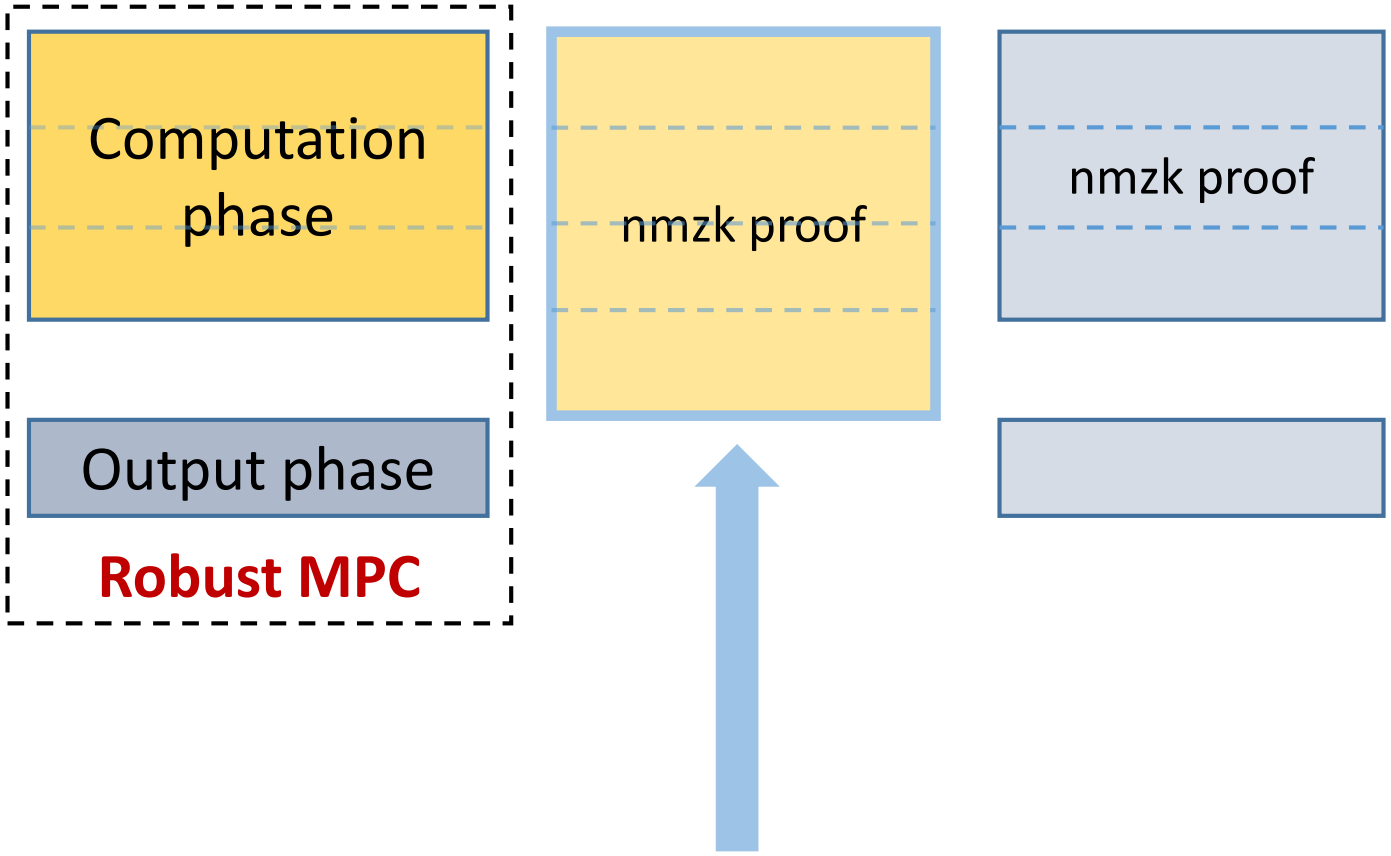
4 round input delayed NMZK can be constructed from CRHF [Ciampi-Ostrovsky-Siniscalchi-Visconti17].

4 Round Protocol

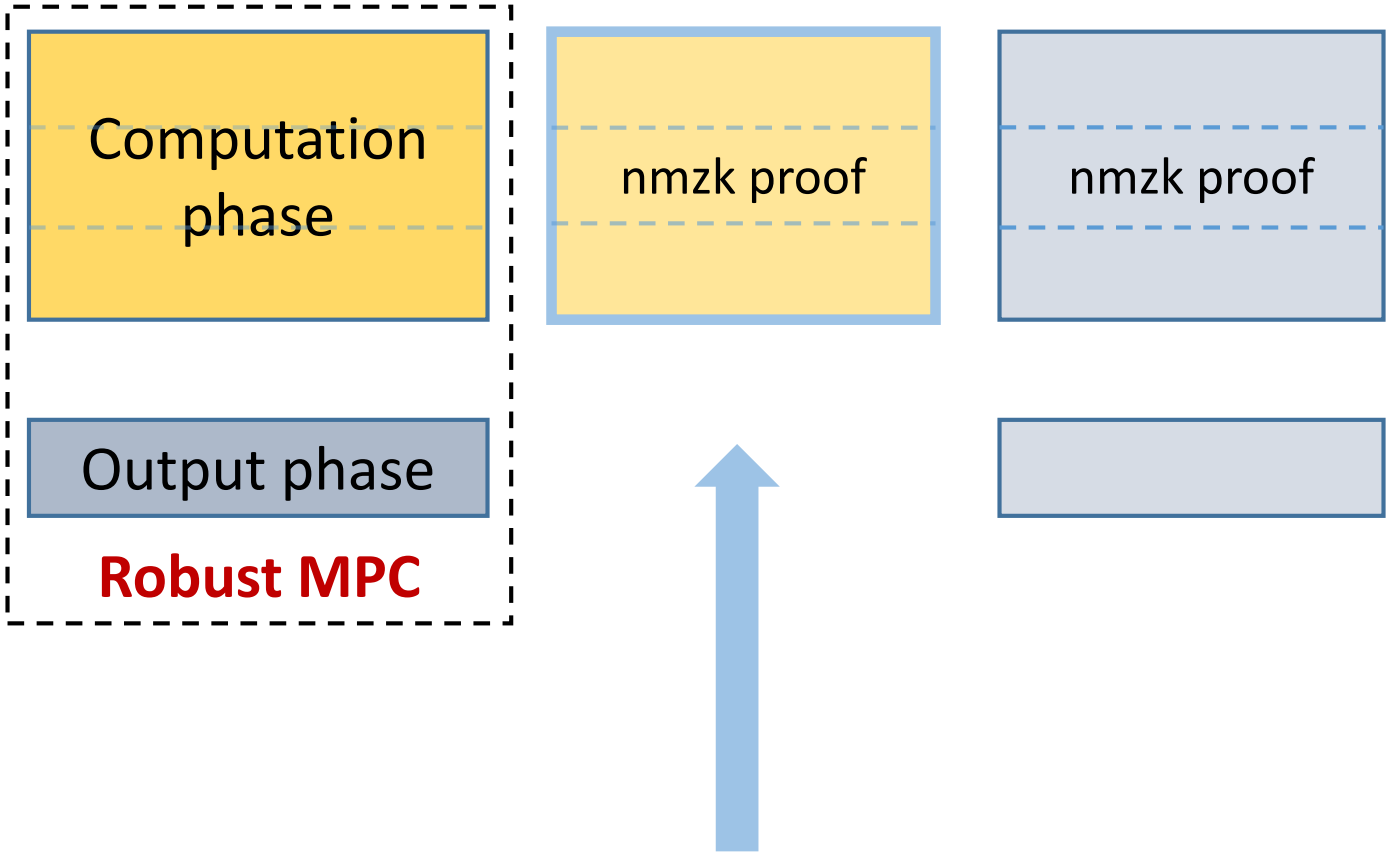
Main challenge



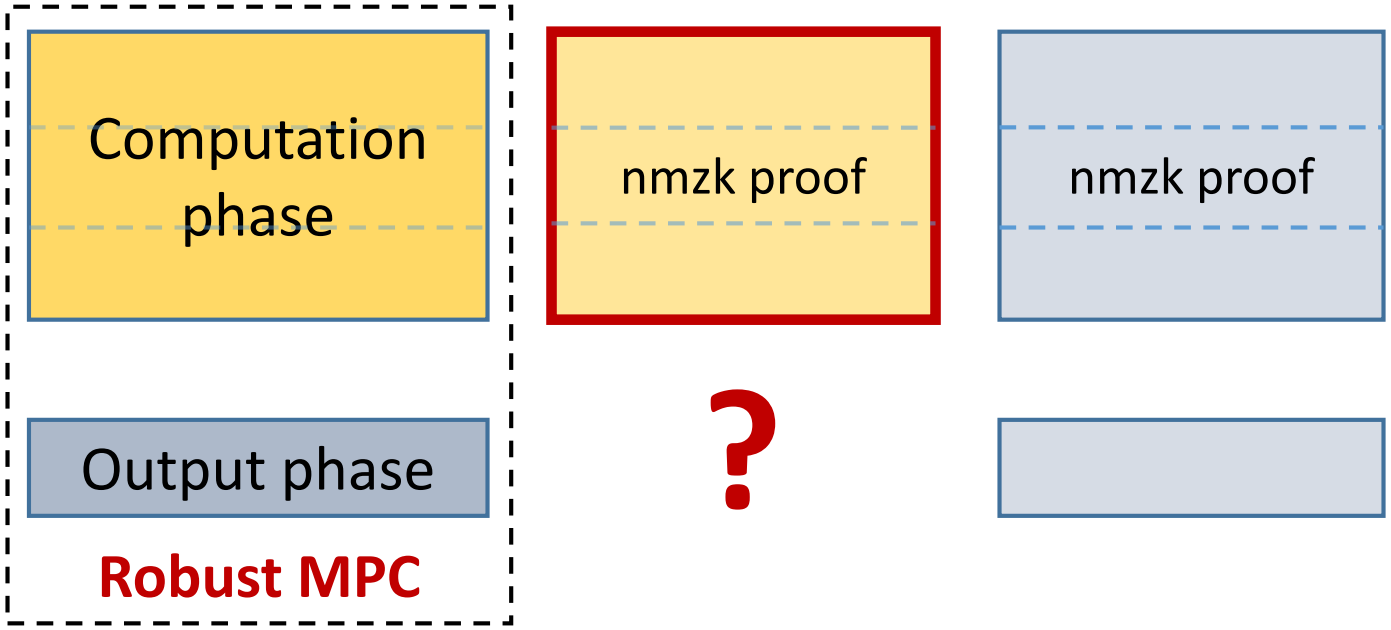
Main challenge



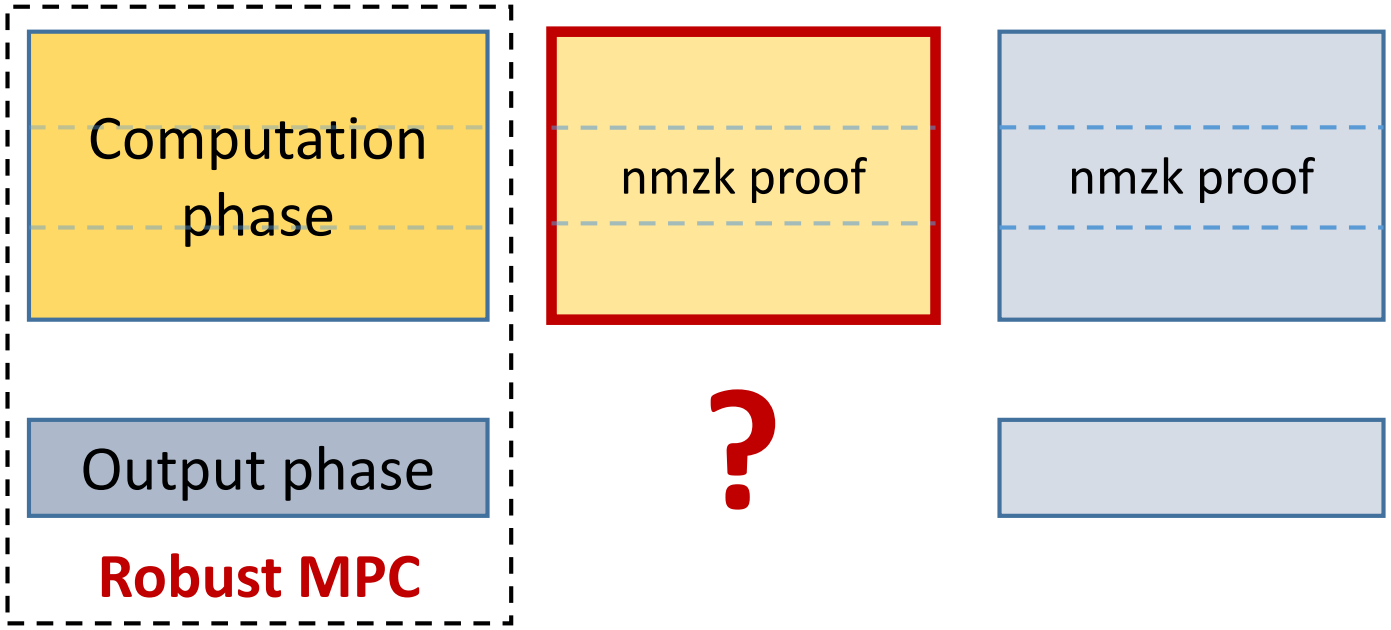
Main challenge



Main challenge



Main challenge



Not clear how to go beyond 5 rounds.

Key idea

Robust MPC:

Simulator needs to cheat only in the output phase.

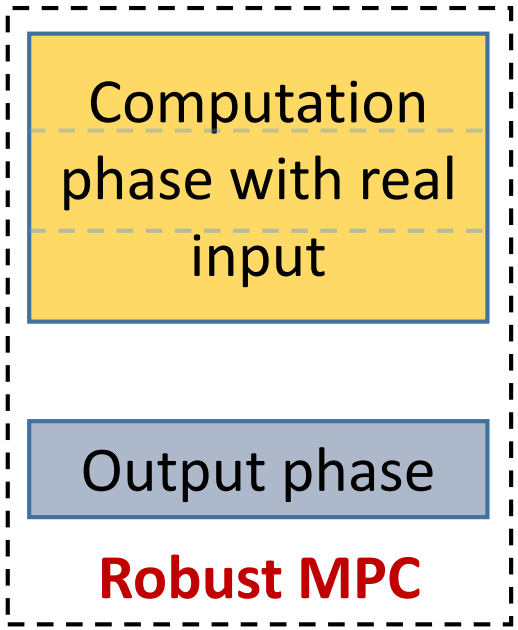
In the computation phase, simulator uses a *random input*.

Key idea

Robust MPC:

Simulator needs to cheat only in the output phase.

In the computation phase, simulator uses a *random input*.

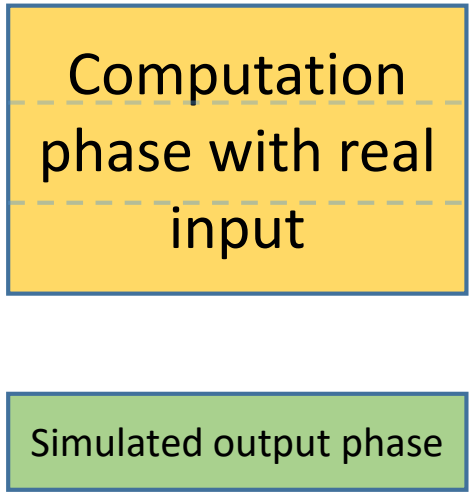


Key idea

Robust MPC:

Simulator needs to cheat only in the output phase.

In the computation phase, simulator uses a *random input*.

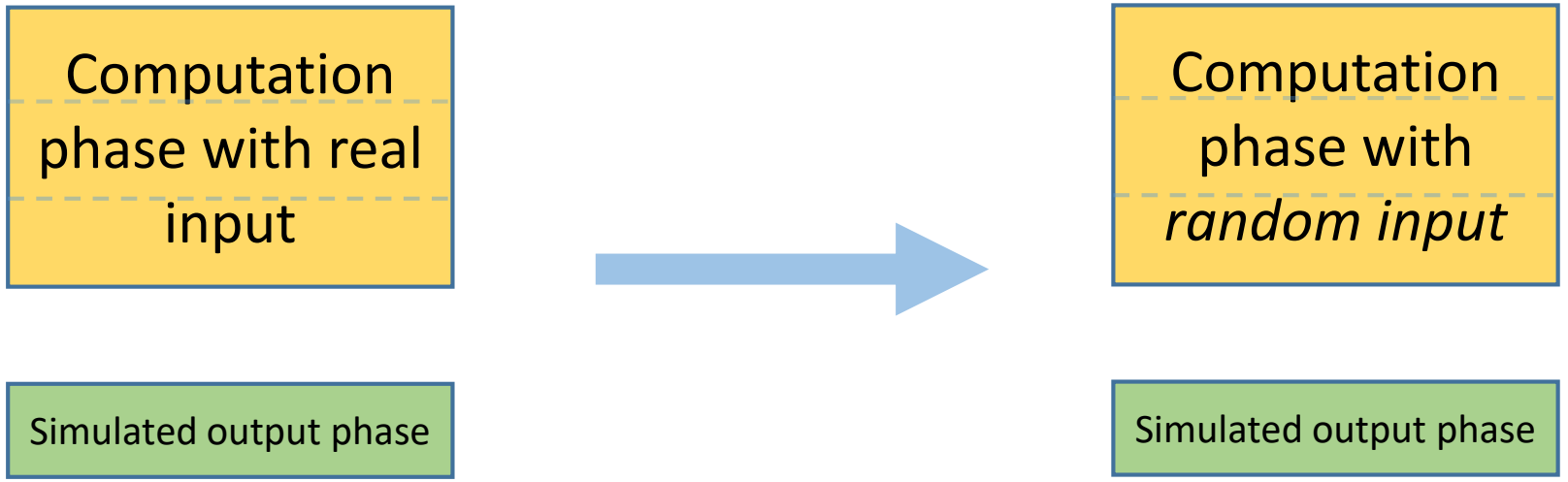


Key idea

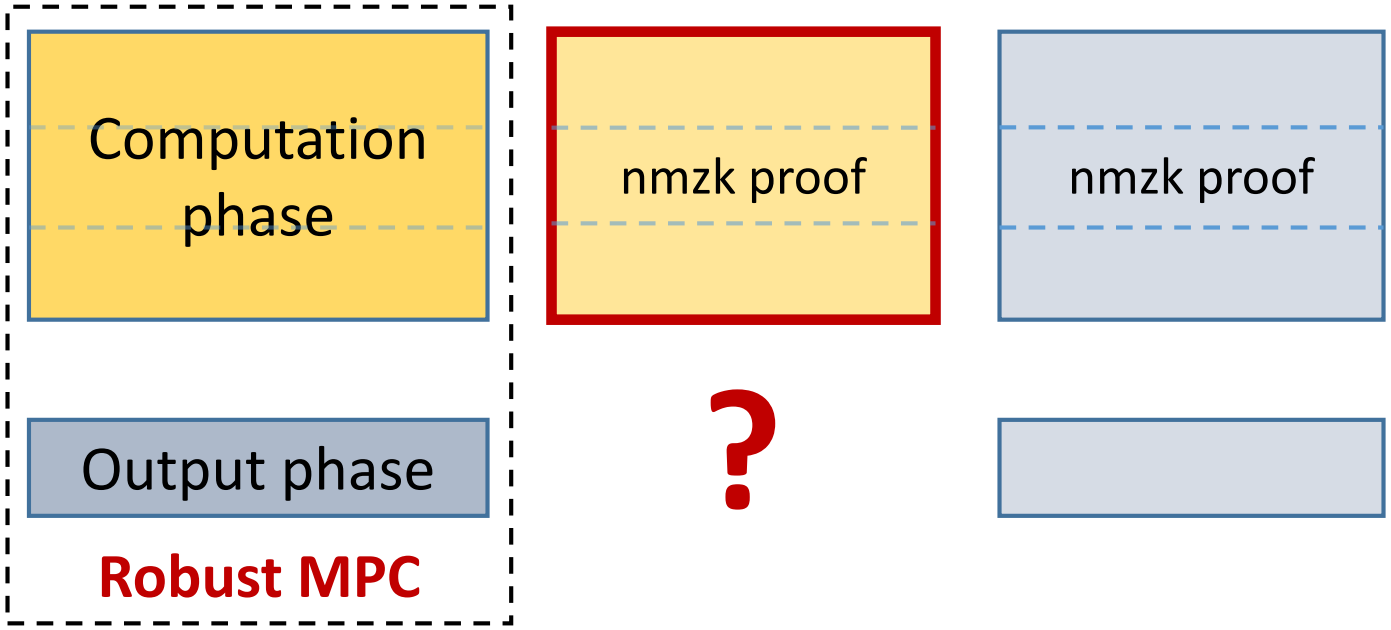
Robust MPC:

Simulator needs to cheat only in the output phase.

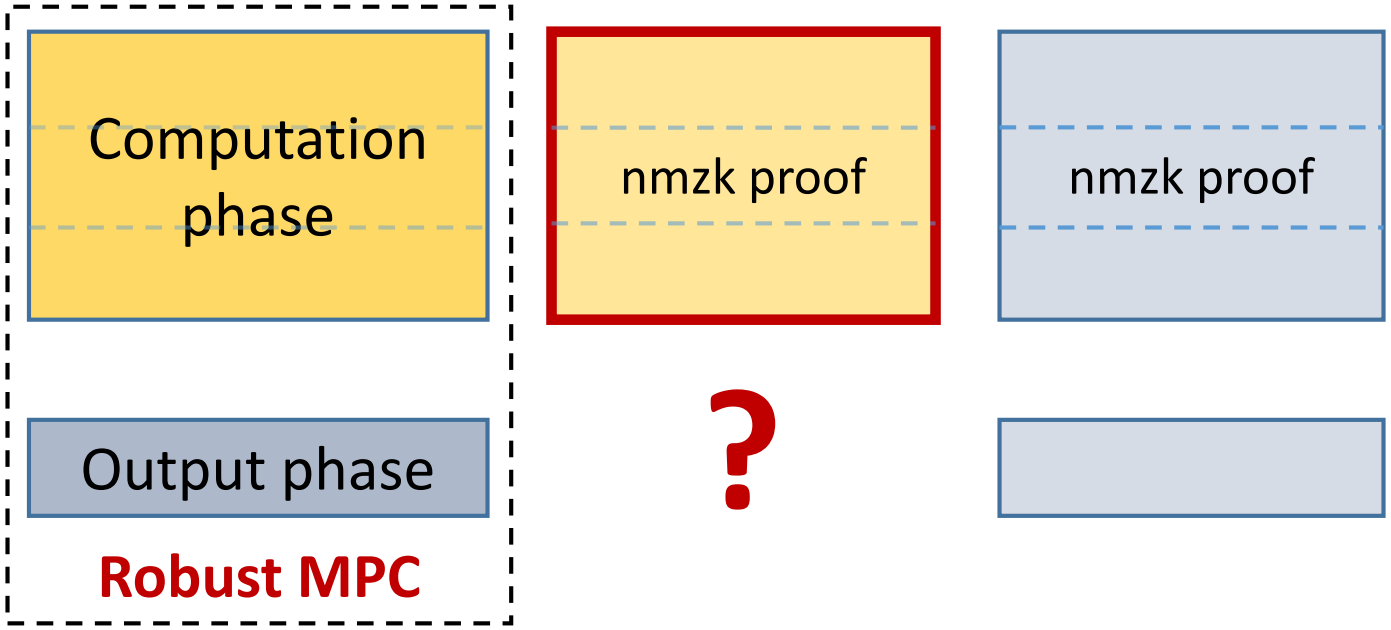
In the computation phase, simulator uses a *random input*.



Key idea

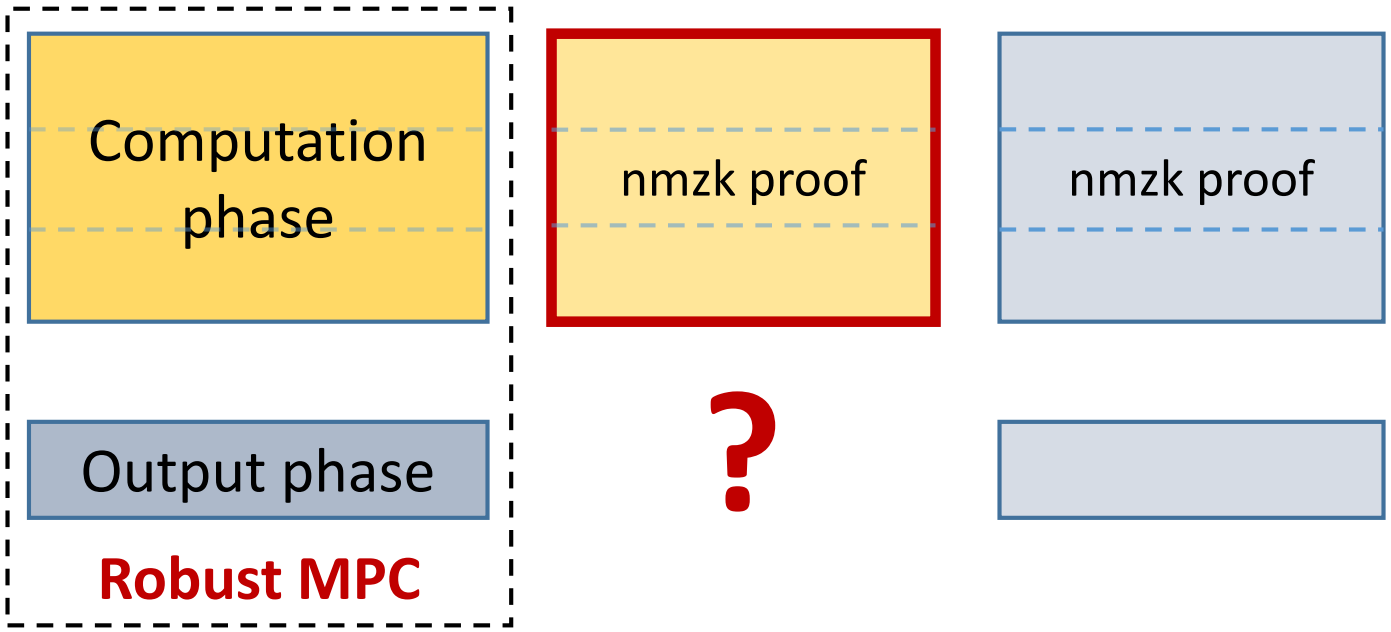

Computation phase
Output phase
Robust MPC
nmzk proof
?
nmzk proof

Key idea



Not necessary to simulate the NMZK.

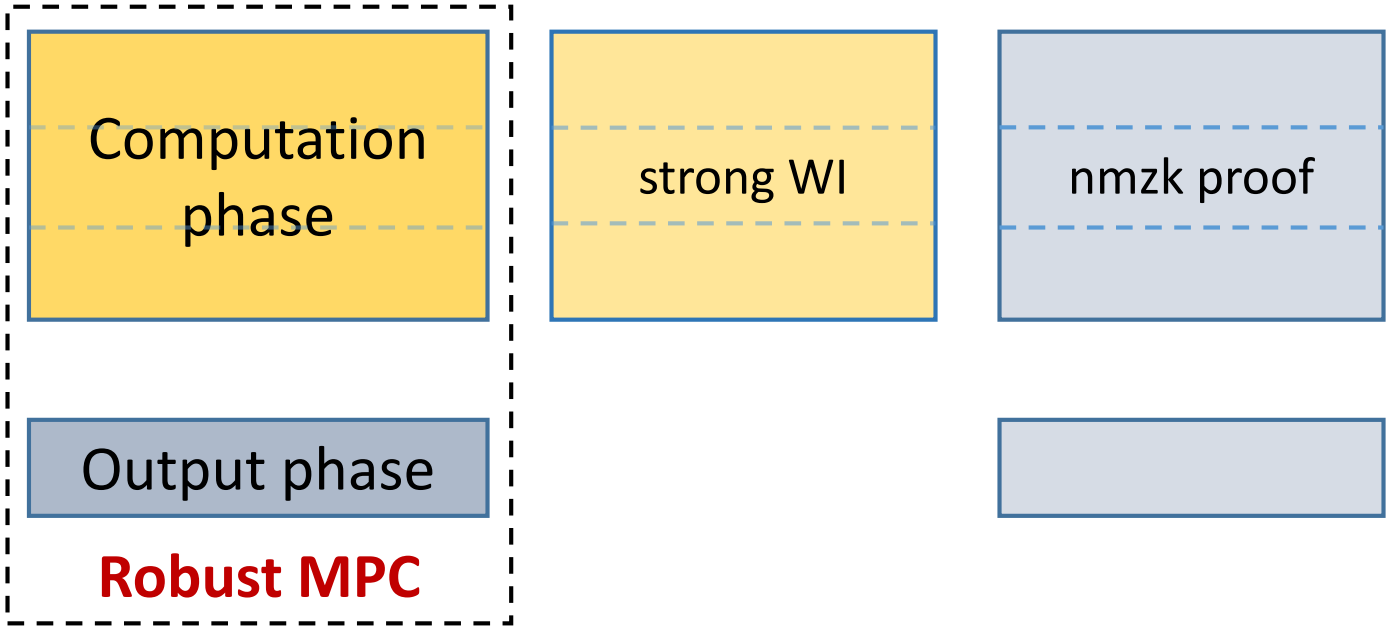
Key idea



Not necessary to simulate the NMZK.

Suffices to use a weaker notion of strong witness indistinguishability (WI).

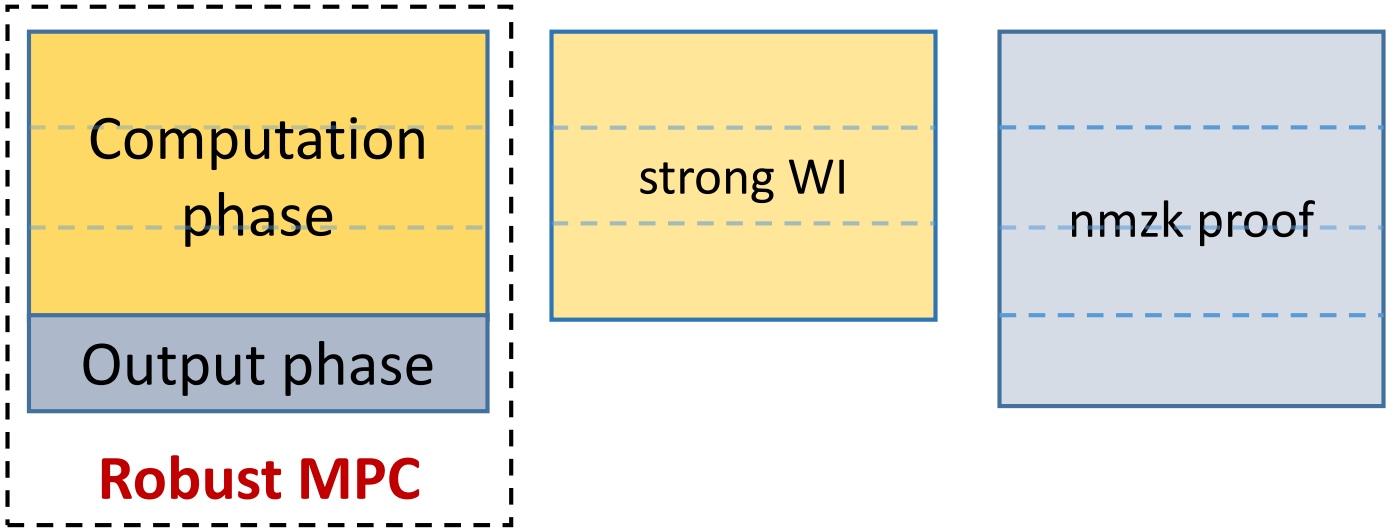
Key idea



Not necessary to simulate the NMZK.

Suffices to use a weaker notion of strong witness indistinguishability (WI).

Key idea

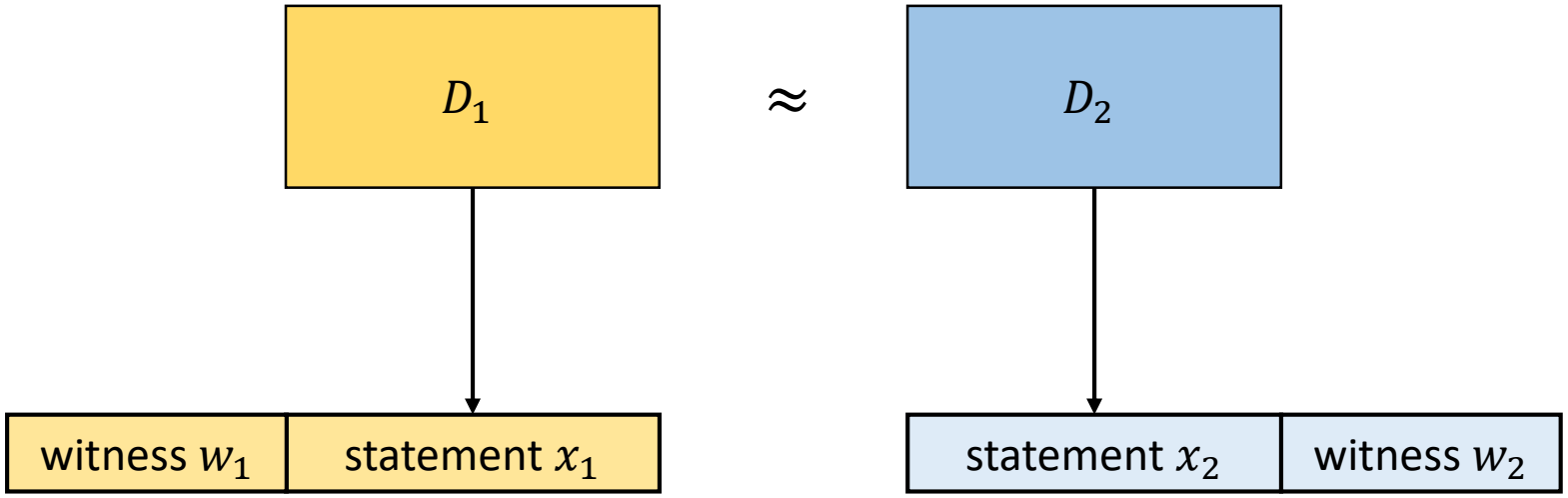


Not necessary to simulate the NMZK.

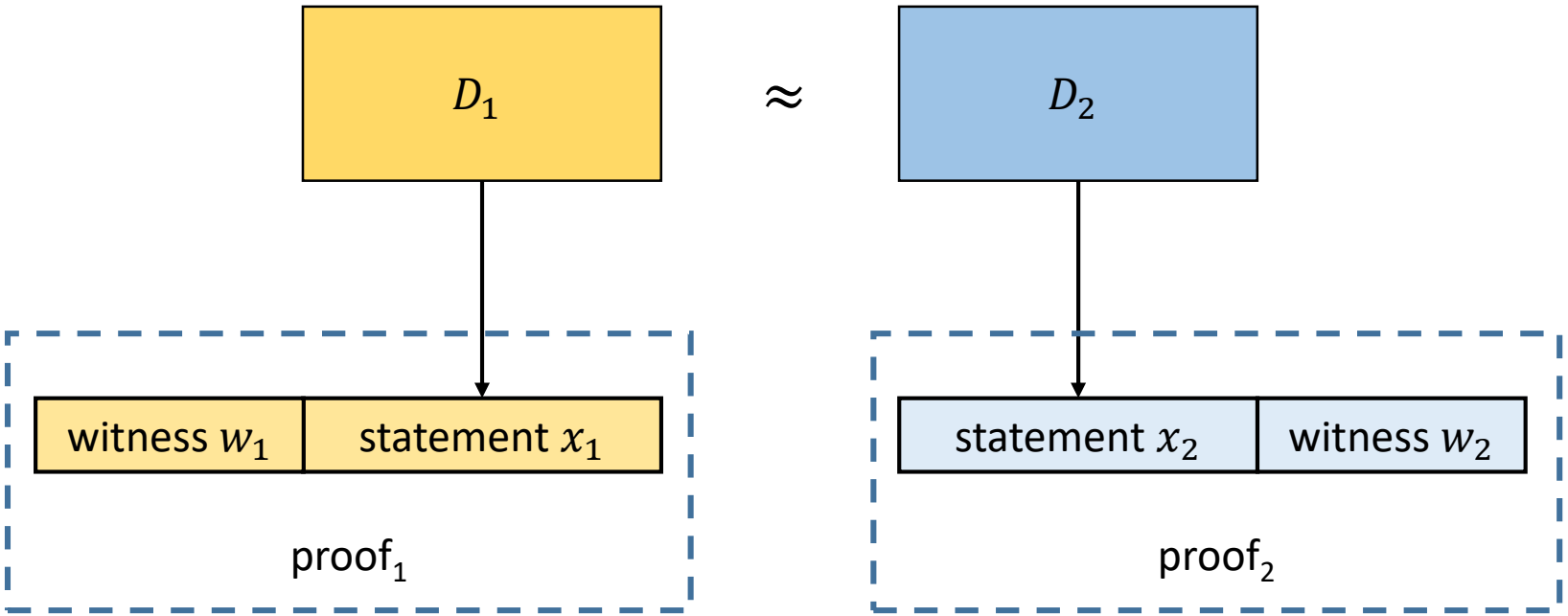
Suffices to use a weaker notion of strong witness indistinguishability (WI).

Strong WI proof system

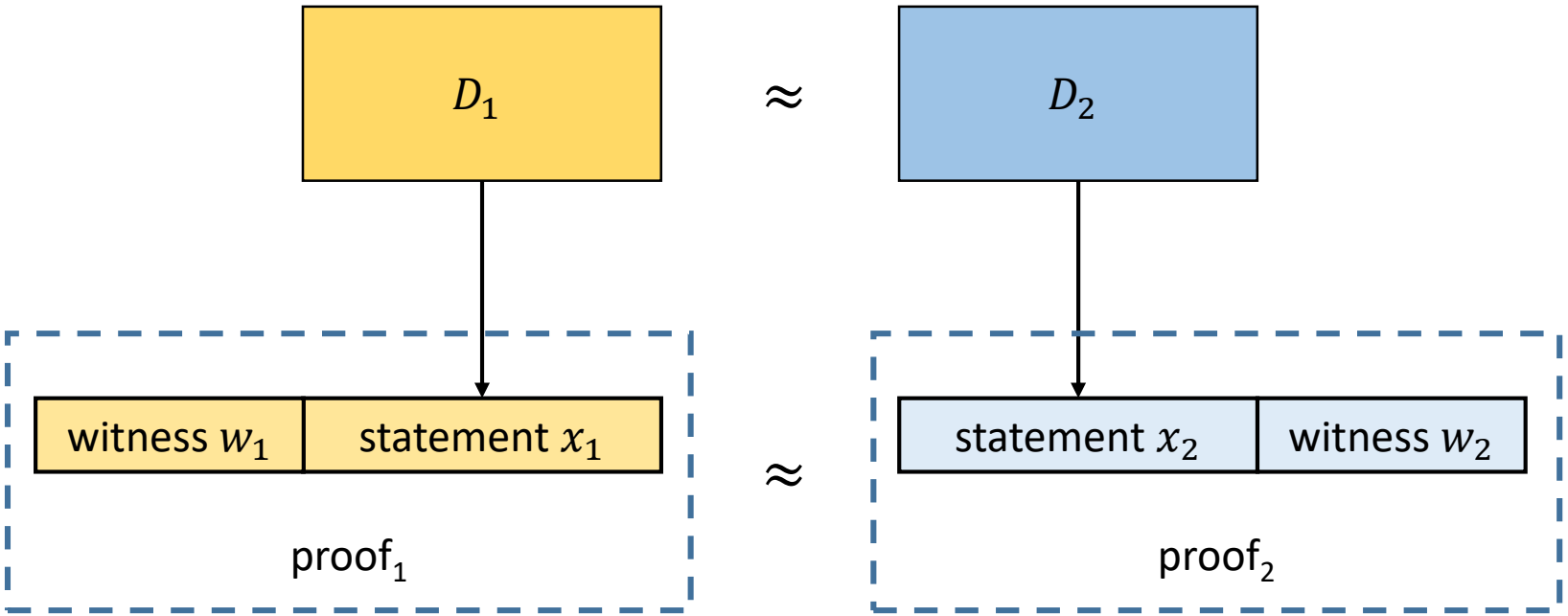
Strong WI proof system



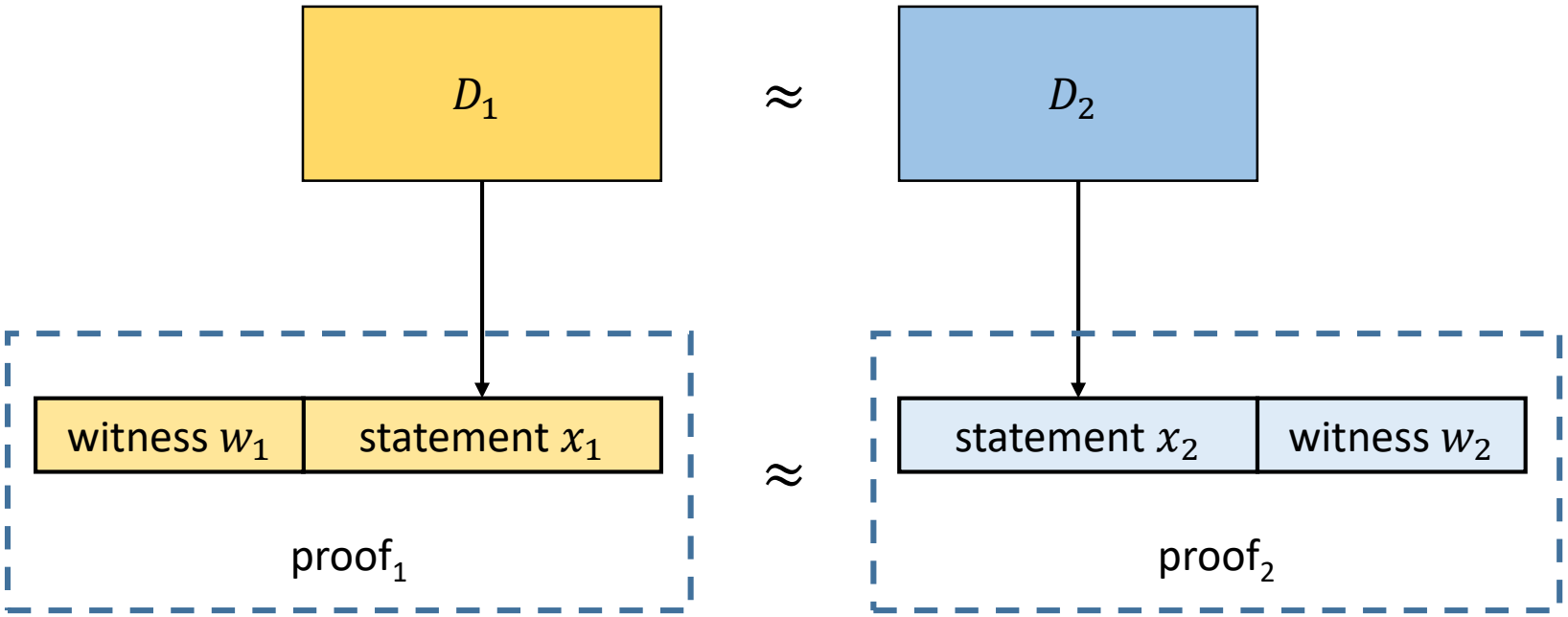
Strong WI proof system



Strong WI proof system

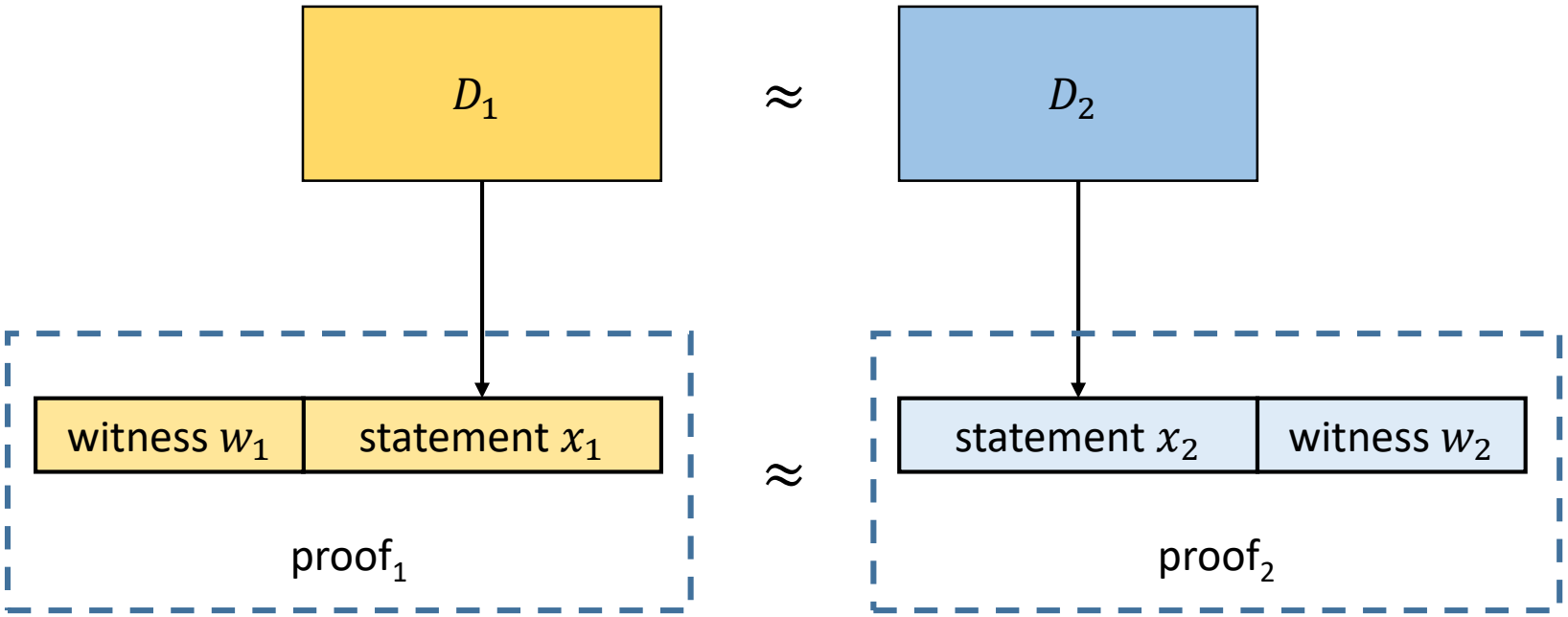


Strong WI proof system



We change both witness and statement during simulation.

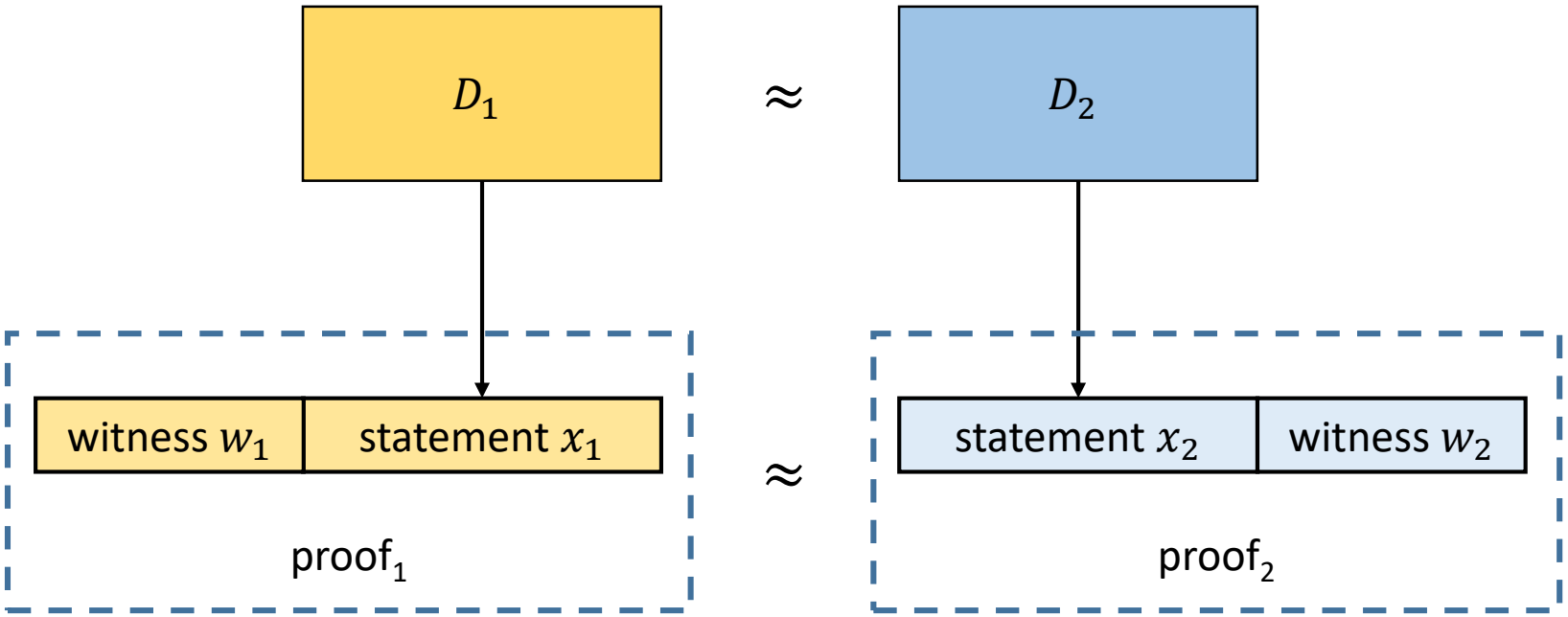
Strong WI proof system



We change both witness and statement during simulation.

[JKKR17] constructed 3 round strong WI from DDH in a limited setting.

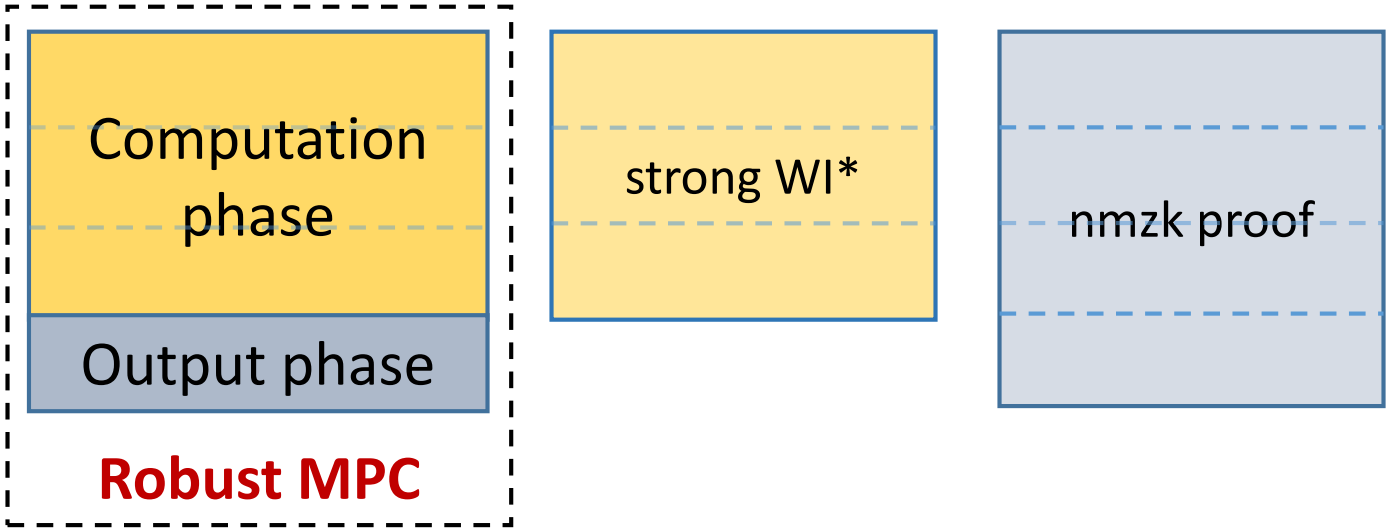
Strong WI proof system



We change both witness and statement during simulation.

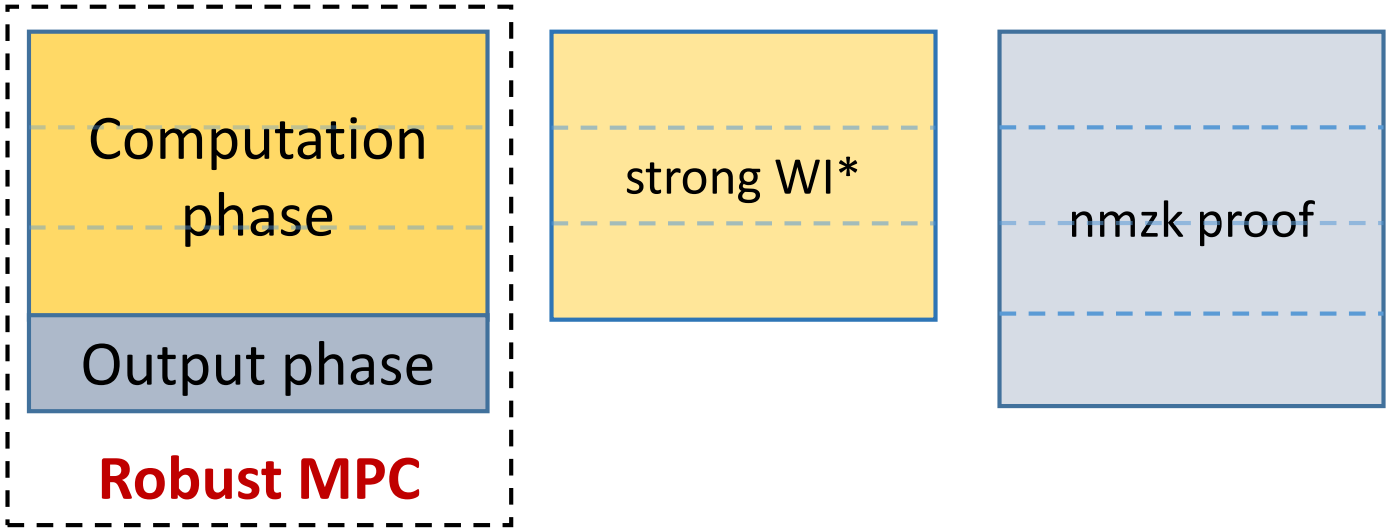
[JKKR17] constructed 3 round strong WI from DDH in a limited setting. Not applicable to our setting.

Blueprint of 4 round protocol



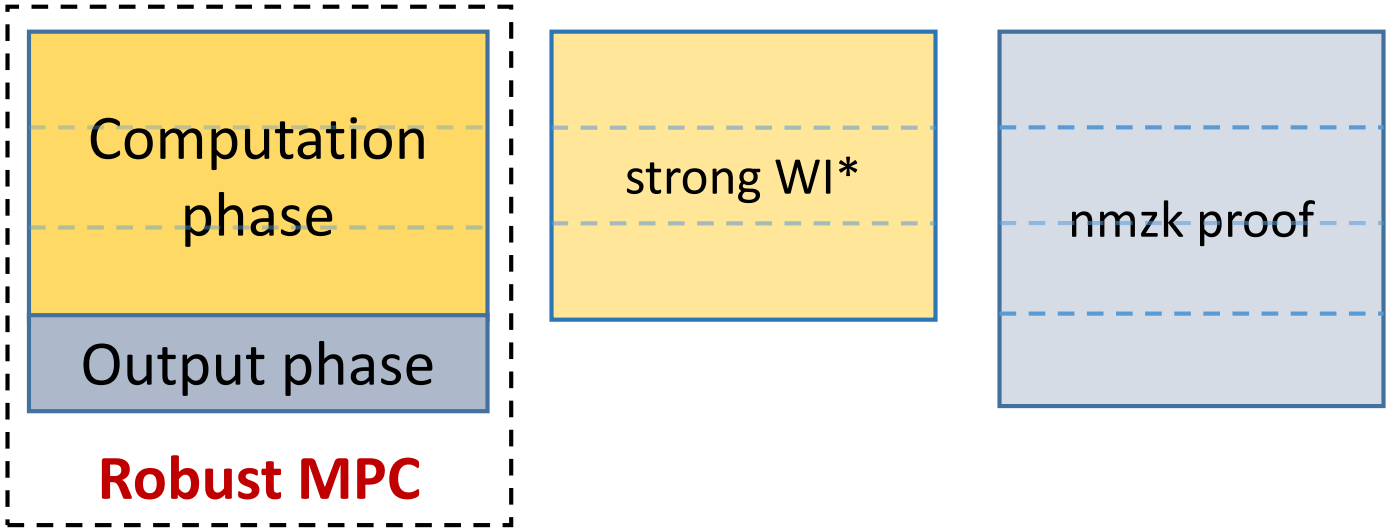
We construct 3 round strong WI*

Blueprint of 4 round protocol



We construct 3 round strong WI* assuming OWP and sub-exponentially secure DDH with requisite non-malleability properties [GPR16, KS17].

Blueprint of 4 round protocol

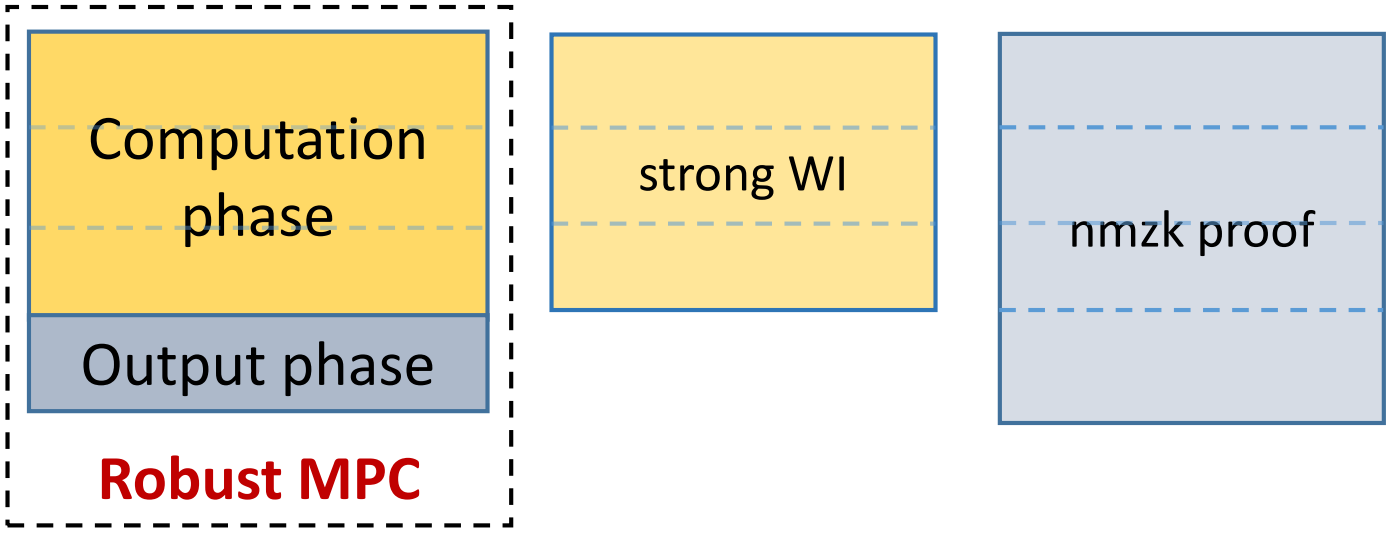


Final **simulator polynomial time**. Sub-exponential hardness used only in the hybrids.

We construct 3 round strong WI* assuming OWP and sub-exponentially secure DDH with requisite non-malleability properties [GPR16, KS17].

Remarks on security proofs

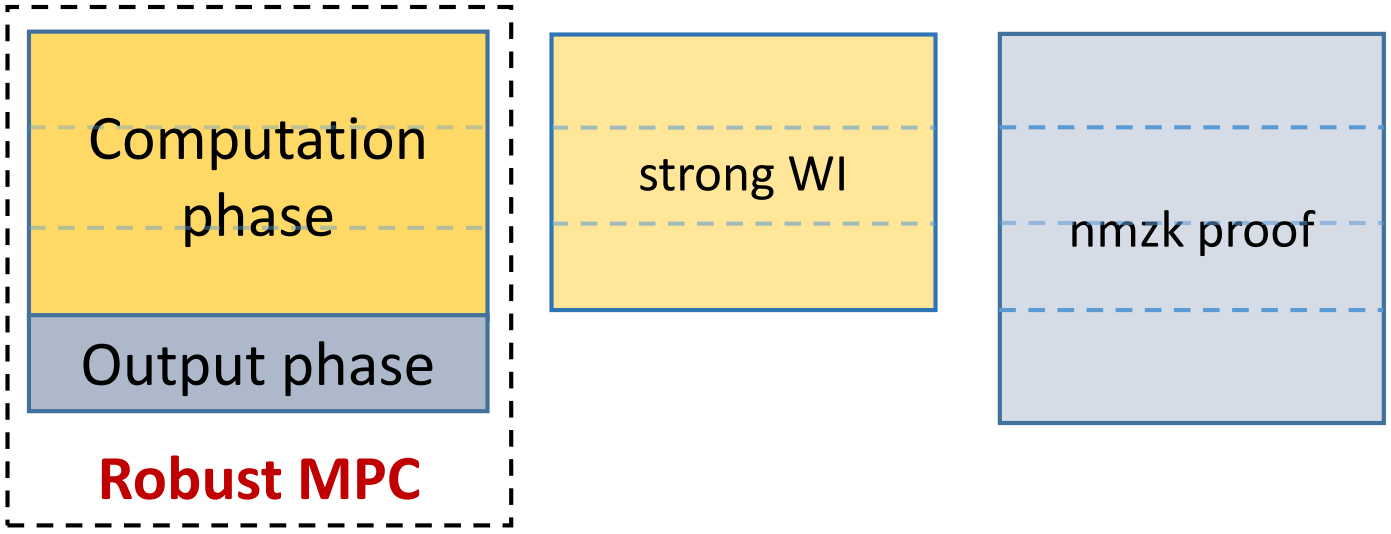
Several challenges, and specific constructions modified accordingly.



Remarks on security proofs

Several challenges, and specific constructions modified accordingly.

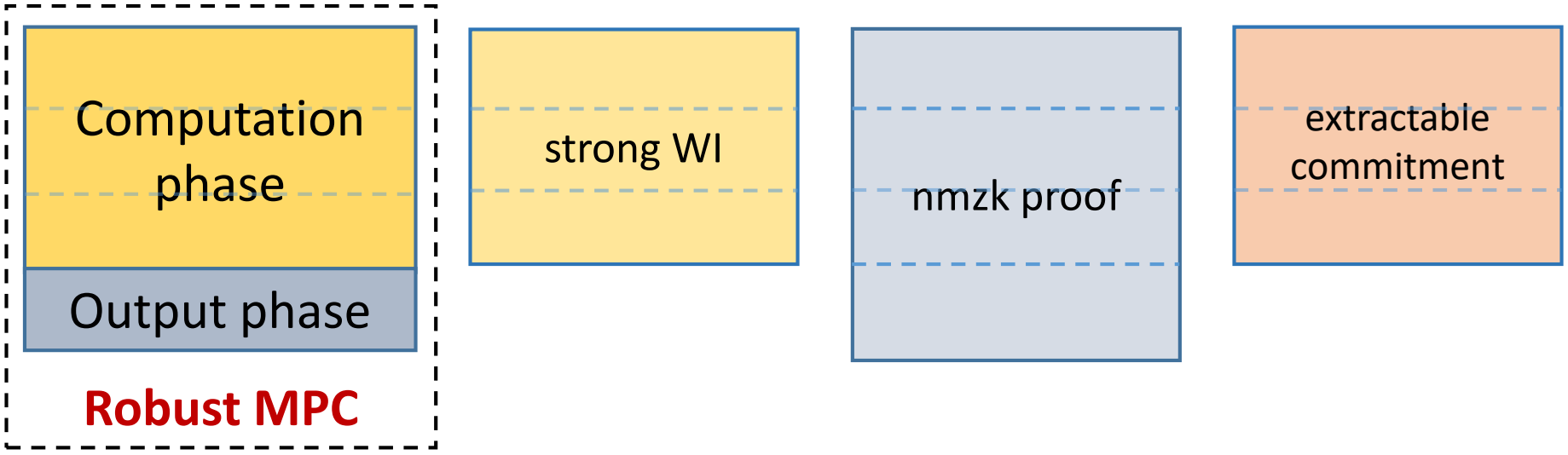
Simulator needs to extract input to argue security.



Remarks on security proofs

Several challenges, and specific constructions modified accordingly.

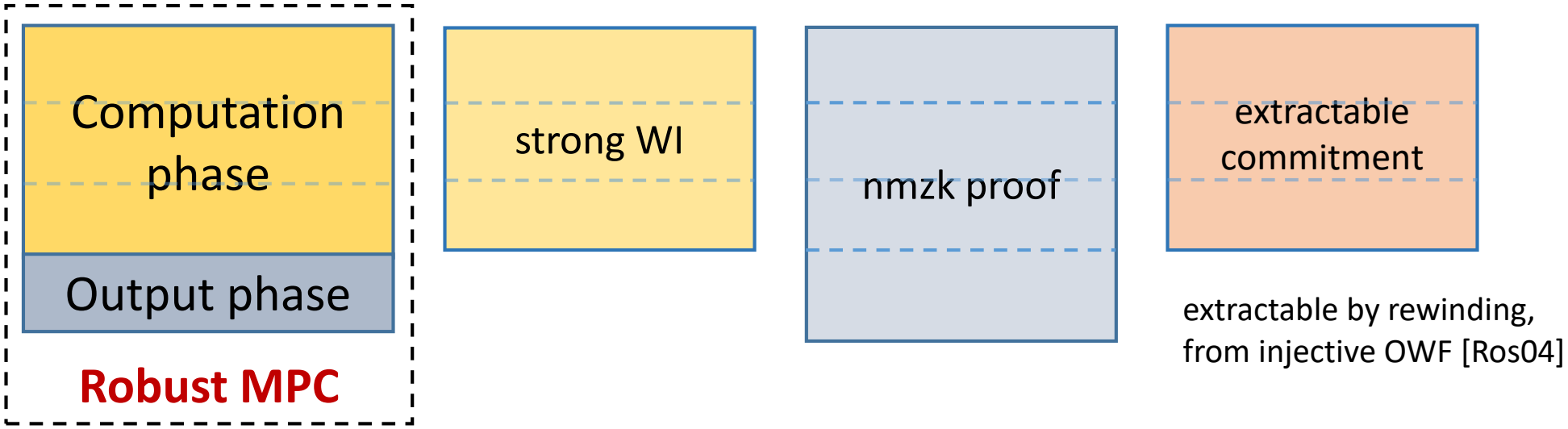
Simulator needs to extract input to argue security.



Remarks on security proofs

Several challenges, and specific constructions modified accordingly.

Simulator needs to extract input to argue security.



Remarks on security proofs

Several challenges, and specific constructions modified accordingly.

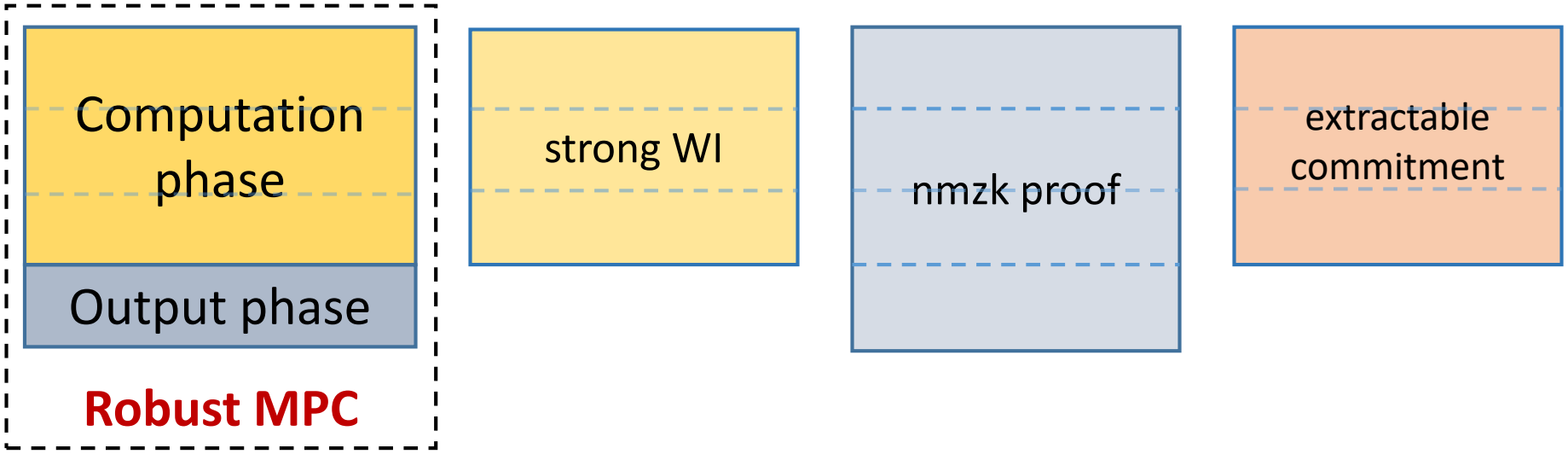
Simulator needs to extract input to argue security.

Primitives need to be secure in the presence of rewinding.

Remarks on security proofs

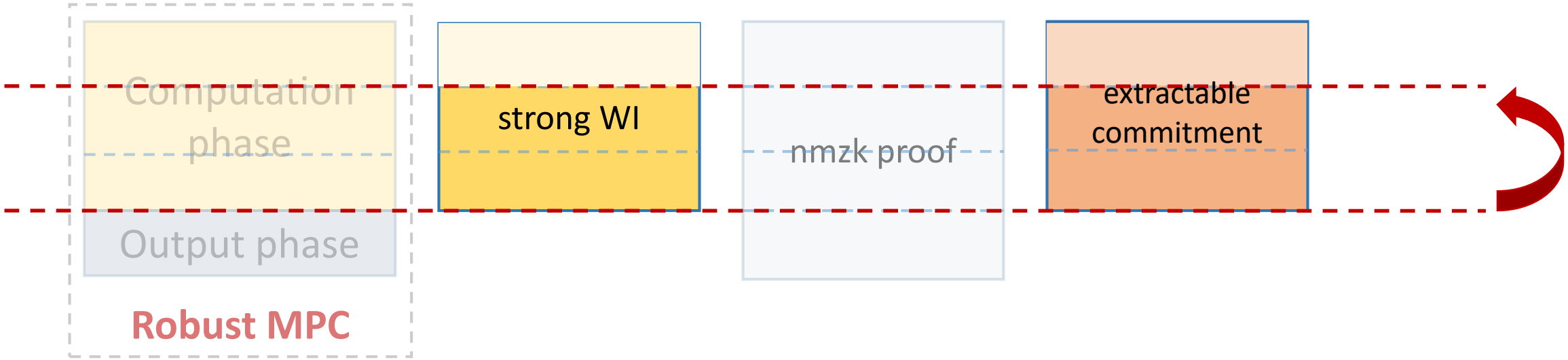
Primitives need to be secure in the presence of rewinding.

Remarks on security proofs



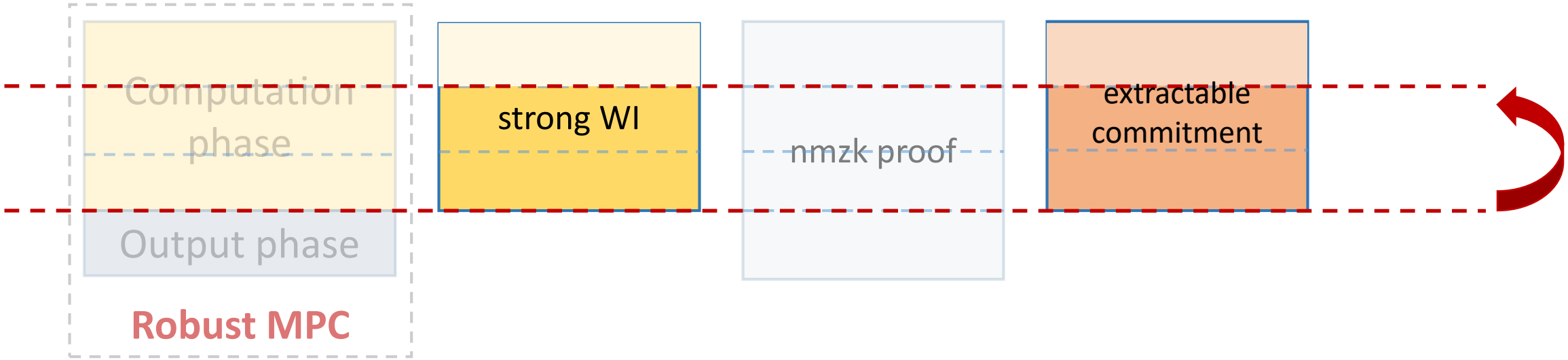
Primitives need to be secure in the presence of rewinding.

Remarks on security proofs



Primitives need to be secure in the presence of rewinding.

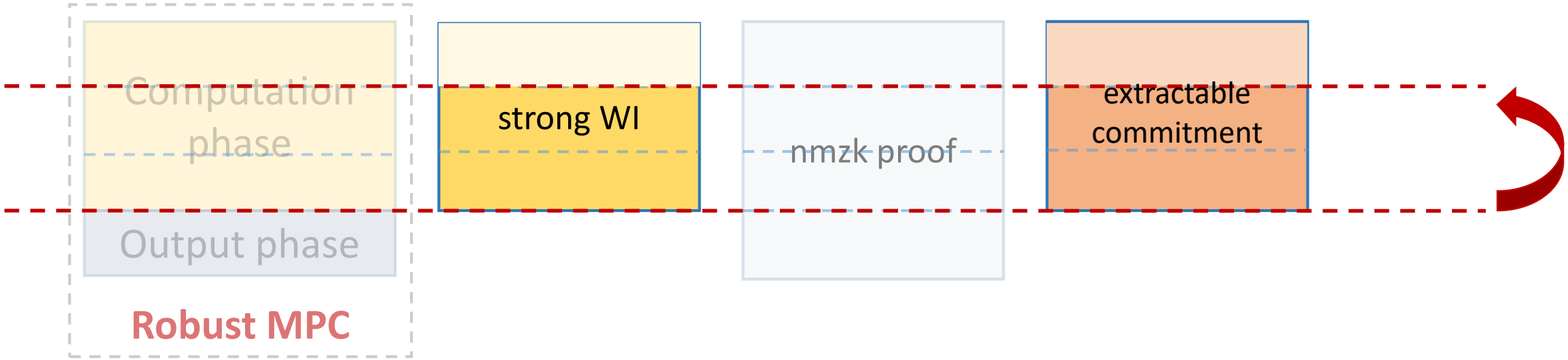
Remarks on security proofs



Primitives need to be secure in the presence of rewinding.

Overcome this issue by using rewinding secure primitives

Remarks on security proofs



Primitives need to be secure in the presence of rewinding.

Overcome this issue by using rewinding secure primitives, or use complexity leveraging to bypass it.

4 Round Robust MPC

Key points

[GMW87]

Round complexity proportional to the depth.

Key points

[GMW87]

Round complexity proportional to the depth.

Use randomized encodings to reduce depth of computation.

Key points

[GMW87]

Round complexity proportional to the depth.

Use randomized encodings to reduce depth of computation.

[AIK06] reduce computing arbitrary functions to computing degree 3 polynomials.

Key points

[GMW87]

Round complexity proportional to the depth.

Use randomized encodings to reduce depth of computation.

[AIK06] reduce computing arbitrary functions to computing degree 3 polynomials.

Implemented using

Key points

[GMW87]

Round complexity proportional to the depth.

Use randomized encodings to reduce depth of computation.

[AIK06] reduce computing arbitrary functions to computing degree 3 polynomials.

Implemented using

semi honest OT: 6 round semi-honest protocol.

Key points

[GMW87]

Round complexity proportional to the depth.

Use randomized encodings to reduce depth of computation.

[AIK06] reduce computing arbitrary functions to computing degree 3 polynomials.

Implemented using

semi honest OT: 6 round semi-honest protocol.

2 round malicious OT: 6 round robust MPC.

Key points

[GMW87]

Round complexity proportional to the depth.

Use randomized encodings to reduce depth of computation.

[AIK06] reduce computing arbitrary functions to computing degree 3 polynomials.

Implemented using

semi honest OT: 6 round semi-honest protocol.

2 round malicious OT: 6 round robust MPC.

Main contribution is to bring it down to 4 rounds.

Thank you. Questions?

Arka Rai Choudhuri

achoud@cs.jhu.edu

ia.cr/2017/402