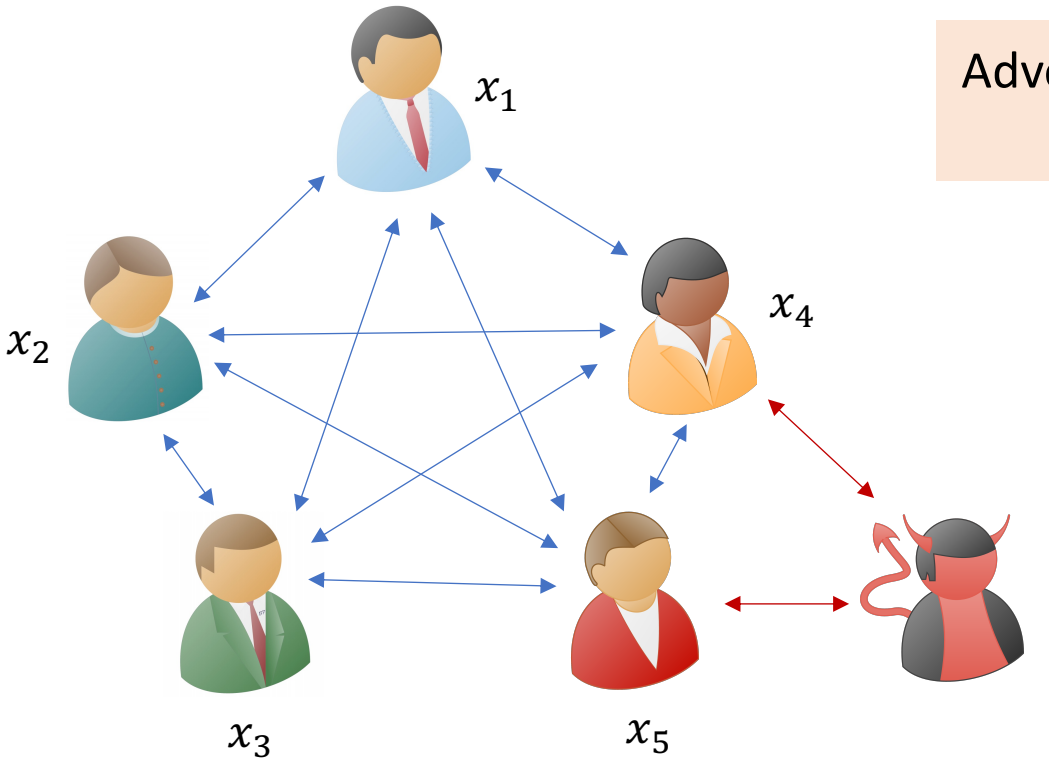
Fluid MPC: Secure Multiparty Computation with Dynamic Participants

Arka Rai Choudhuri Aarushi Goel Matthew Green Abhishek Jain Gabriel Kaptchuk

CRYPTO 2021

Secure Multiparty Computation



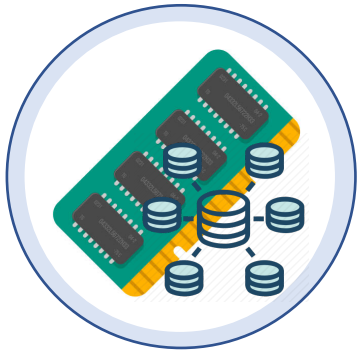
Adversary learns nothing beyond the output of the function, i.e.,

$$y = f(x_1, x_2, x_3, x_4, x_5)$$

MPC and Emerging Applications

- MPC protocols are becoming increasingly efficient.
- Can be used to compute large complex functionalities such as:

Training machine learning algorithms on massive, distributed datasets.



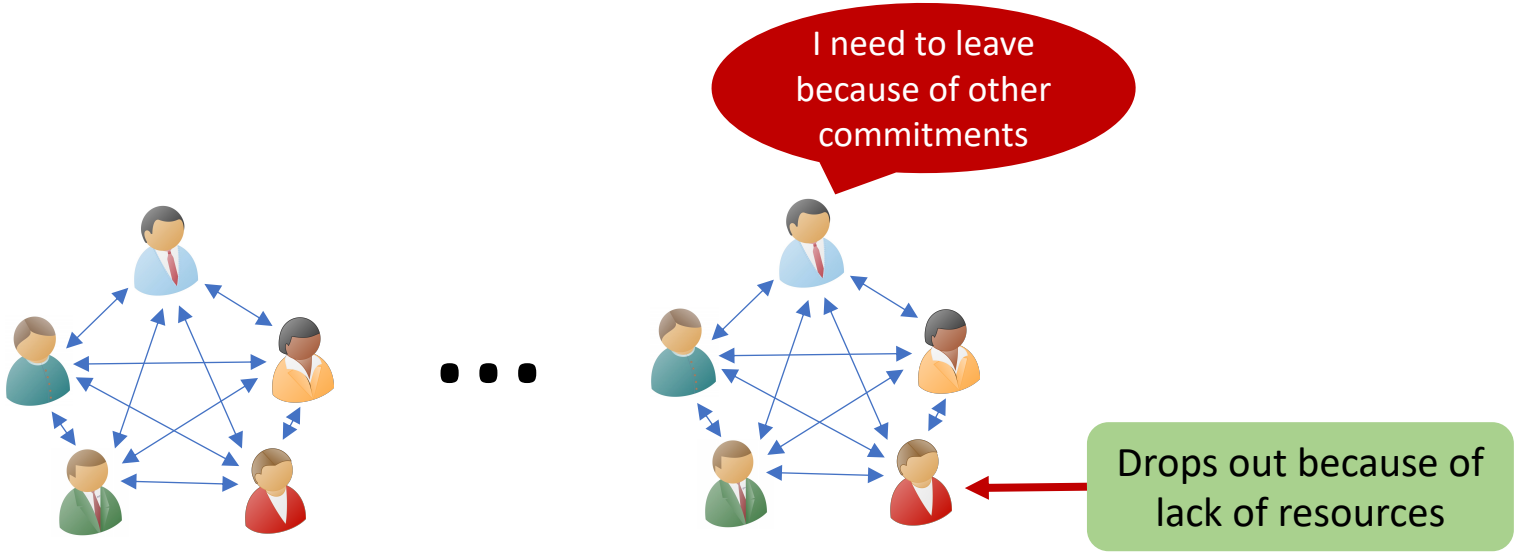
Simulating large RAM programs on distributed datasets

Issue: Evaluating these functionalities could take up to several hours or even days.

Problem with Static MPC
(Fixed Participants)

Entire Protocol Duration

After some time, in the middle of the protocol

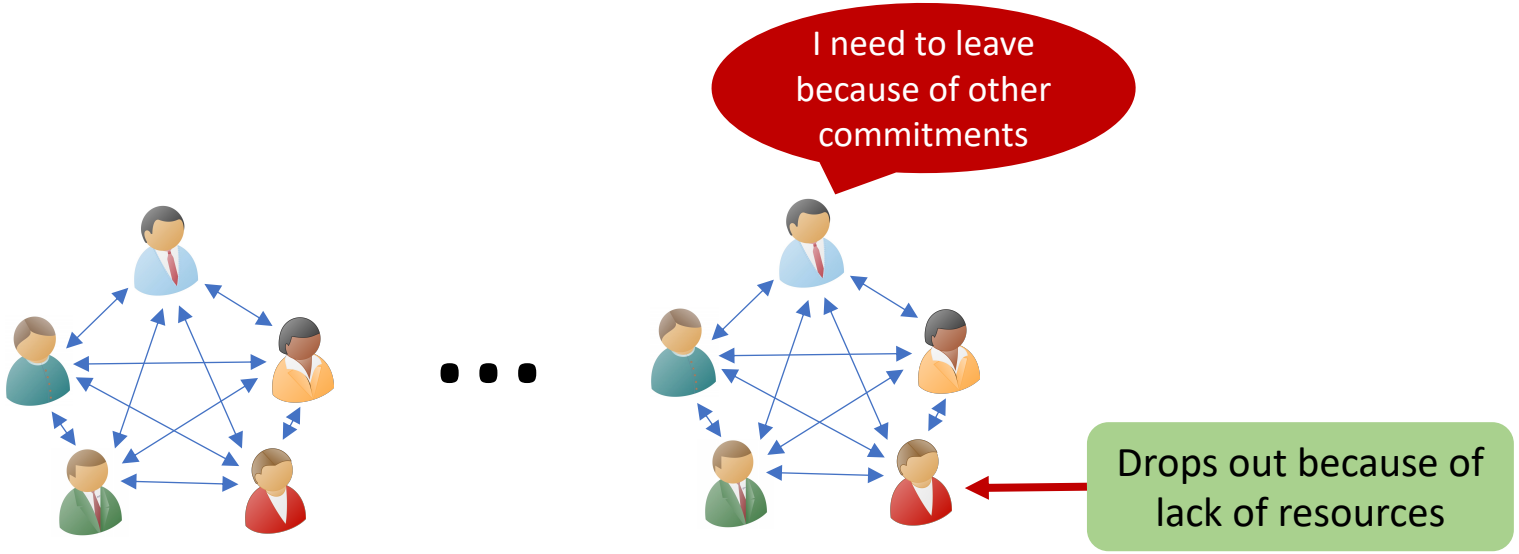


Requiring all participants to stay online throughout the computation is an unrealistic expectation.

Main Question

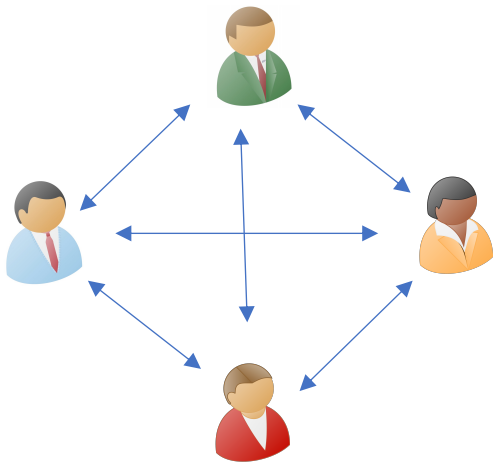
Entire Protocol Duration

After some time, in the middle of the protocol



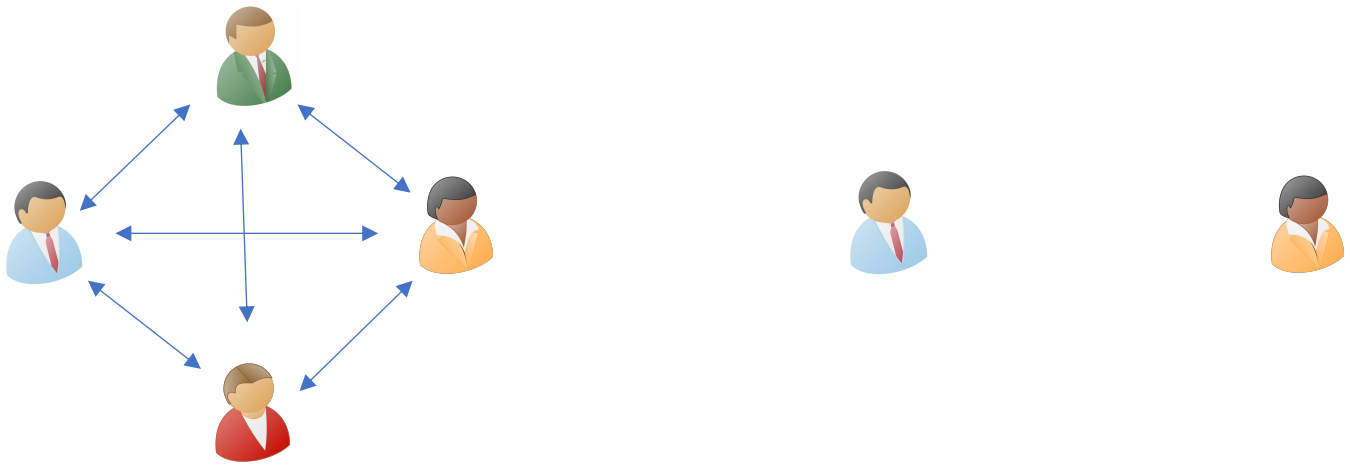
Can we design MPC protocols with Dynamic Participants?

MPC with Dynamic Participants



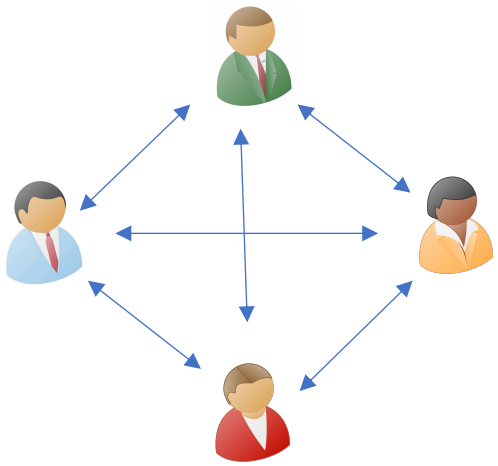
A group of parties start the computation

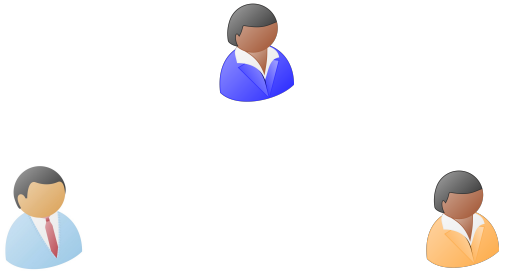
MPC with Dynamic Participants



After some time two parties have to leave

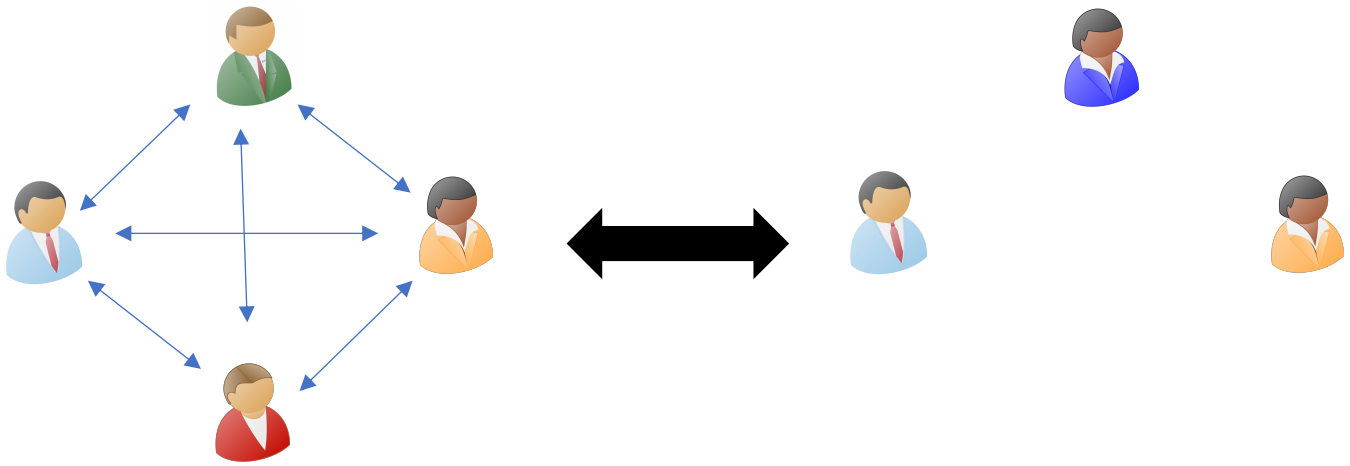
MPC with Dynamic Participants





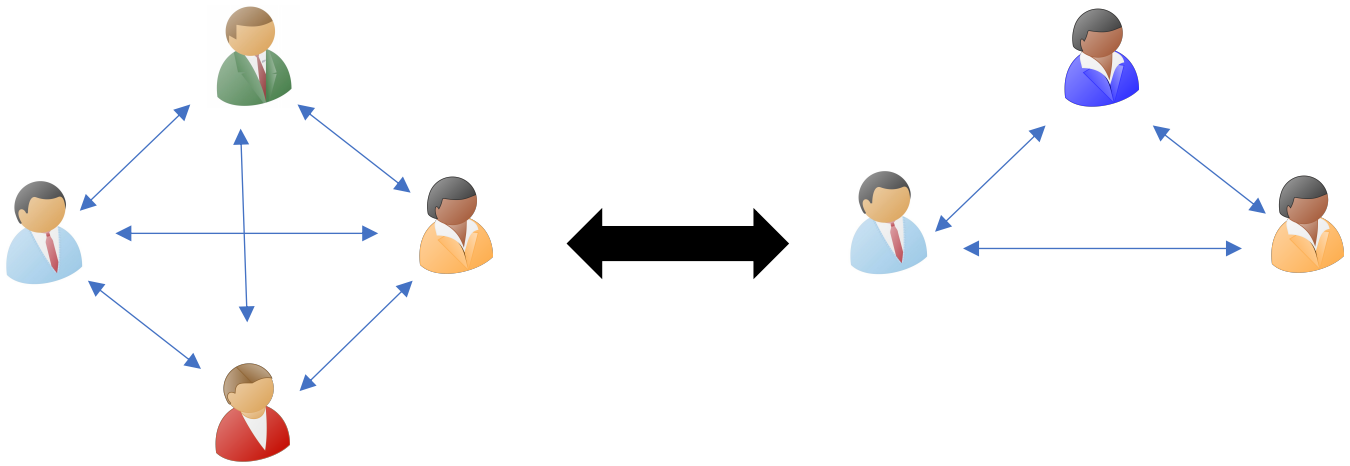
And a new party wants to join the computation

MPC with Dynamic Participants



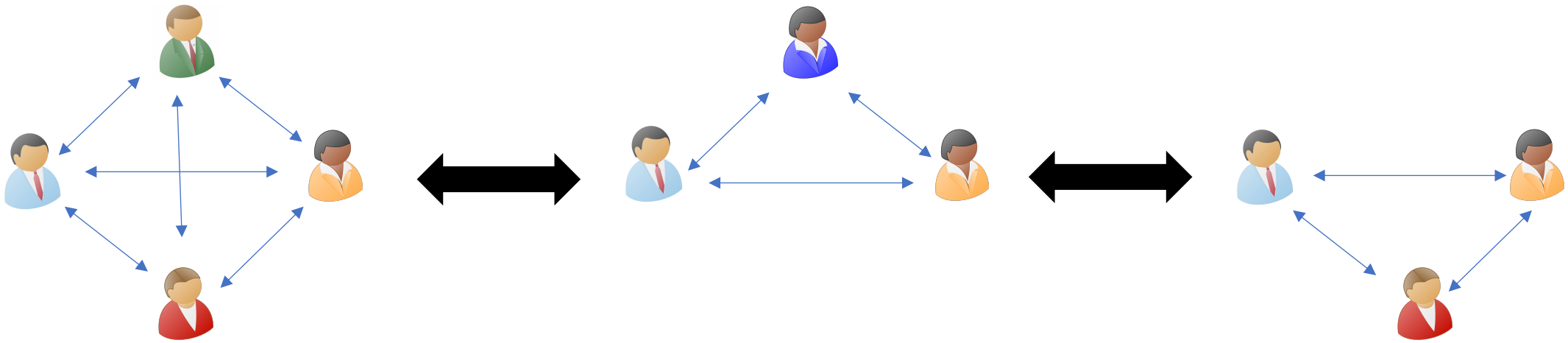
The previous group of parties securely distributes information about the computation so far, to the new group

MPC with Dynamic Participants

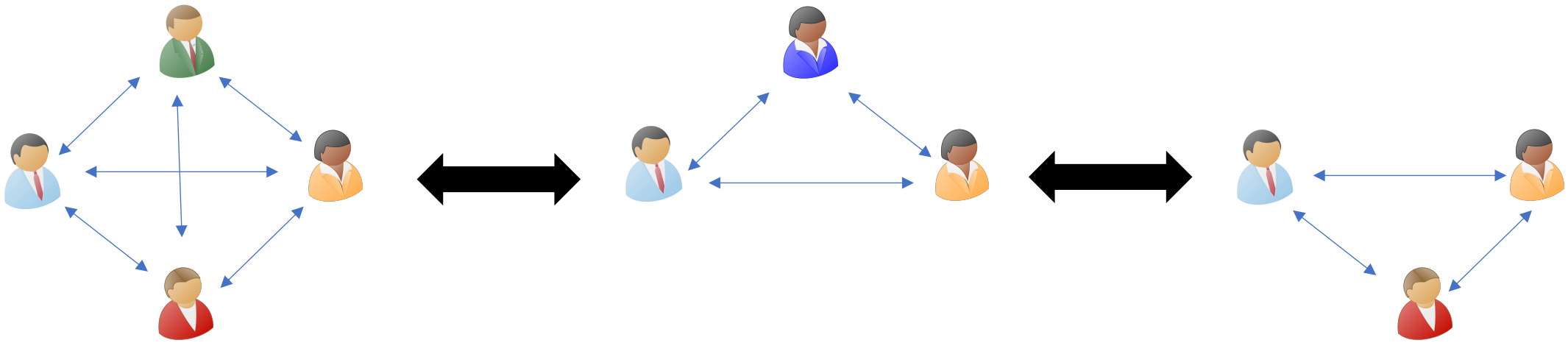


Given this information, the new group
continues with the rest of the computation

MPC with Dynamic Participants

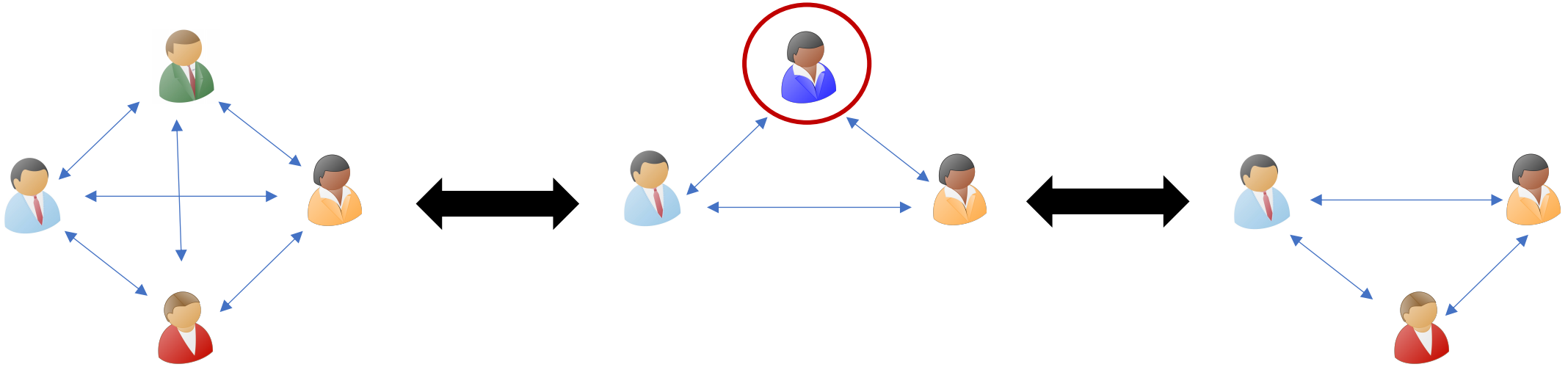


MPC with Dynamic Participants



This reduces the burden of computation on individual parties

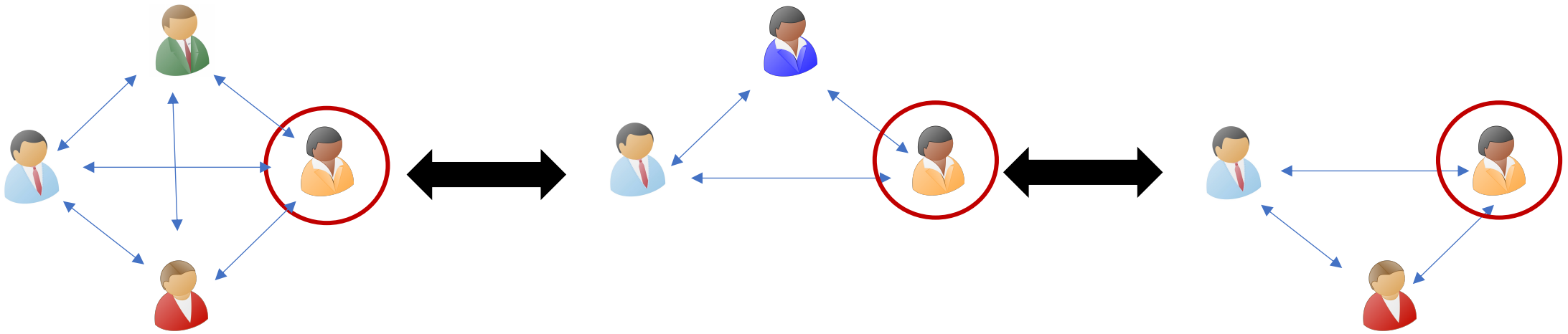
MPC with Dynamic Participants



This reduces the burden of computation on individual parties

Parties with low computational resources can also participate for a small time

MPC with Dynamic Participants

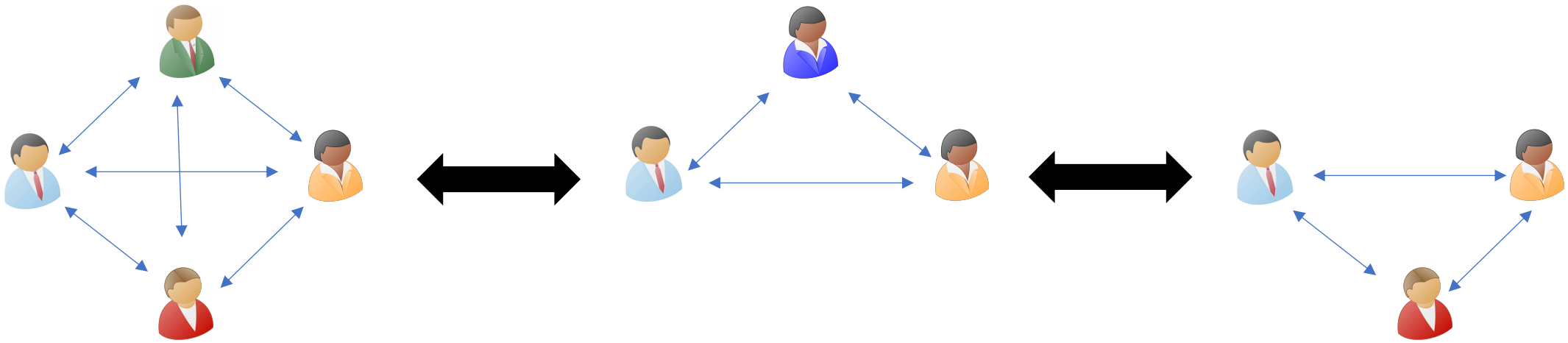


This reduces the burden of computation on individual parties

Parties with low computational resources can also participate for a small time

While parties with more time and computational resources can help with the computation for a longer time

MPC with Dynamic Participants



This will result in a weighted, privacy preserving distributed computing system.

Can be used as an MPC-as-a-service framework

Player Replaceability

- Byzantine Agreement [Mic17, CM19] : After every round, the current set of players can be replaced by new ones.

- Blockchains [GHMVZ17]: This idea is used in the design of Algorand.
  - Helps mitigate targeted attacks on chosen participants after their identity is revealed.

Related Work

- Proactive MPC [OY91]
  - Static participants
  - Mobile adversaries

- Secret Sharing with dynamic participants [GKMPS20, BGGHKLRR20]
  - Computational setting
  - Guaranteed output delivery

Our Contributions

Fluid MPC: A formal model for MPC with dynamic participants

Semi-honest and maliciously secure Fluid MPC protocols

Fluid MPC Model

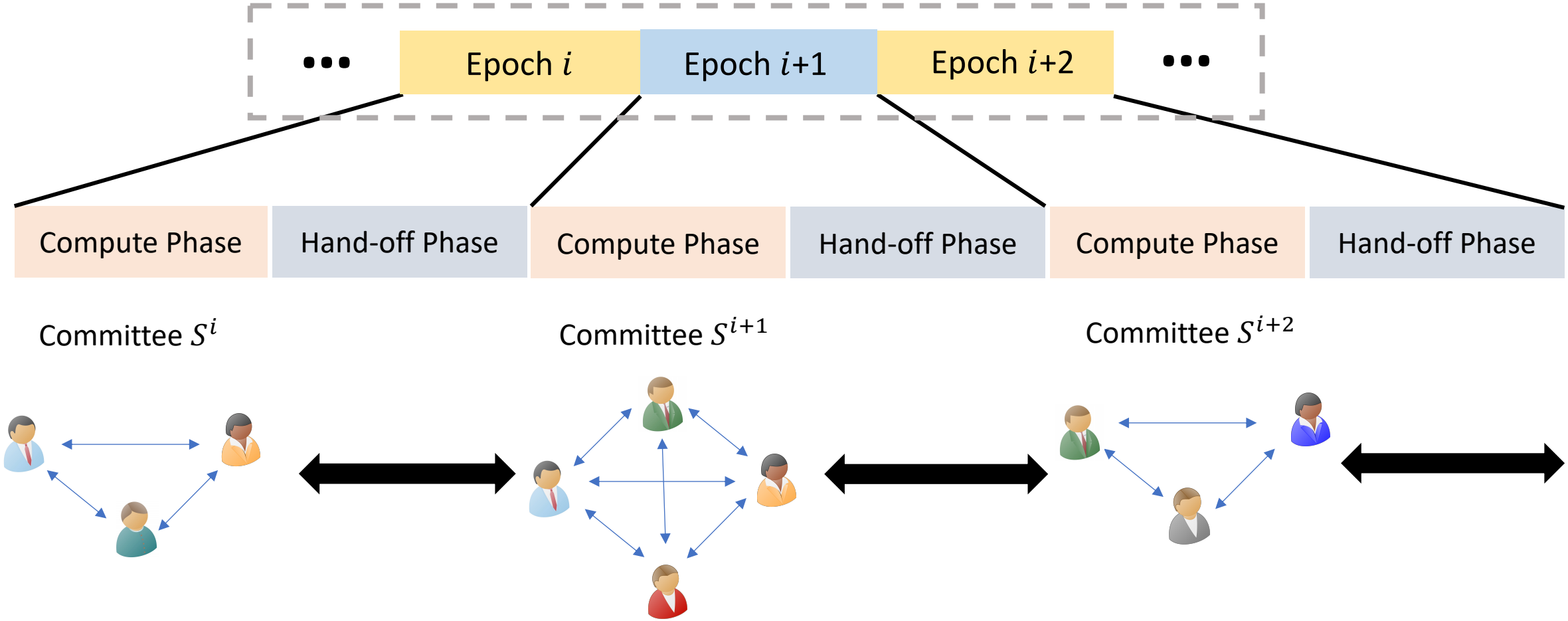
Modeling Dynamic Computation

- Client-server model
- Clients delegate computation to volunteer servers

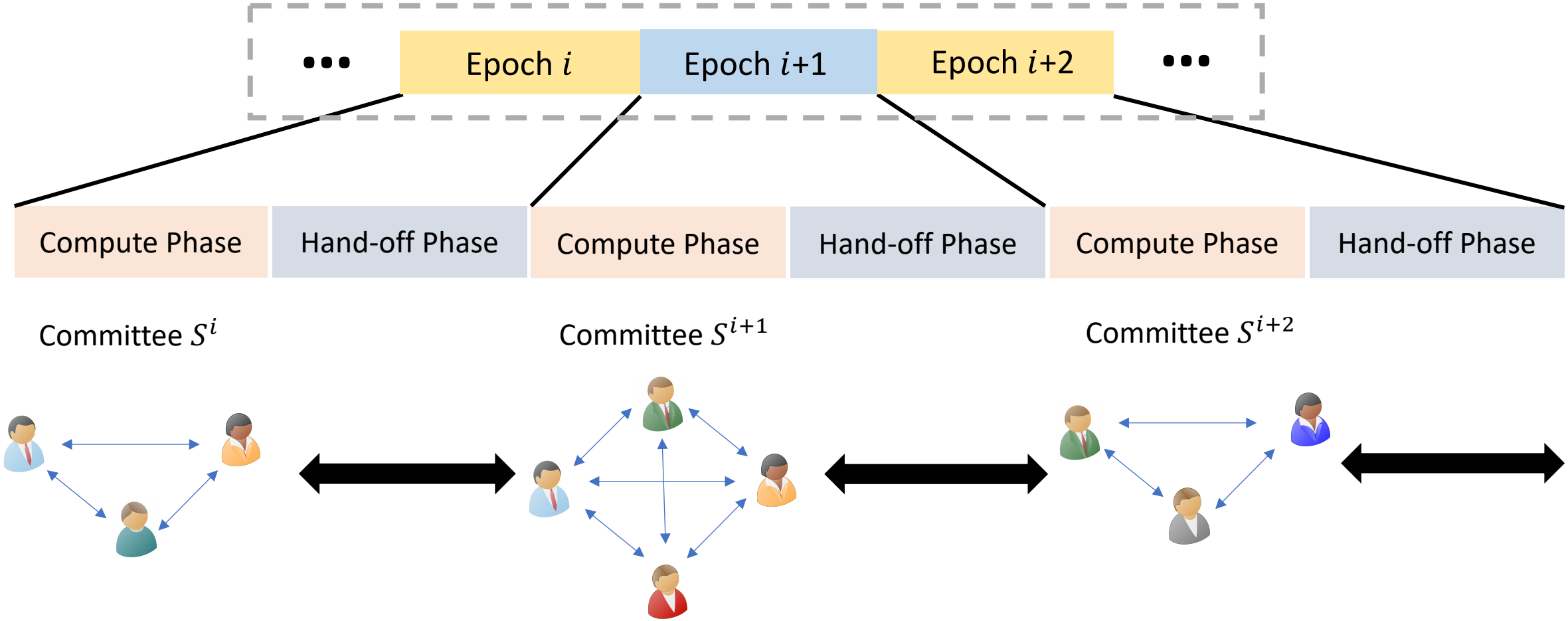
Input Stage	Execution Stage	Output Stage
Clients pre-process their inputs and hand them to the servers	Dynamic servers participate to compute the function	Clients reconstruct the output of the function

Modeling Execution Stage

Modeling Execution Stage



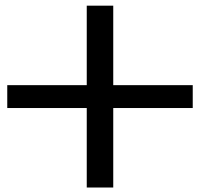
Modeling Execution Stage



We require honest majority of clients and an honest majority of servers in each committee

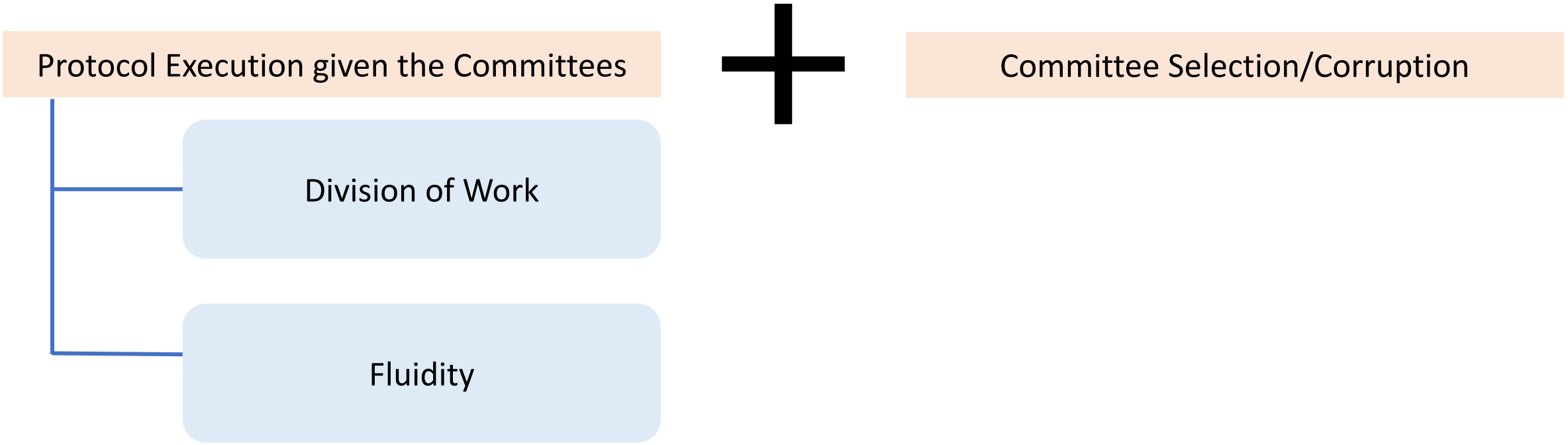
Fluid MPC Protocol

Protocol Execution given the Committees

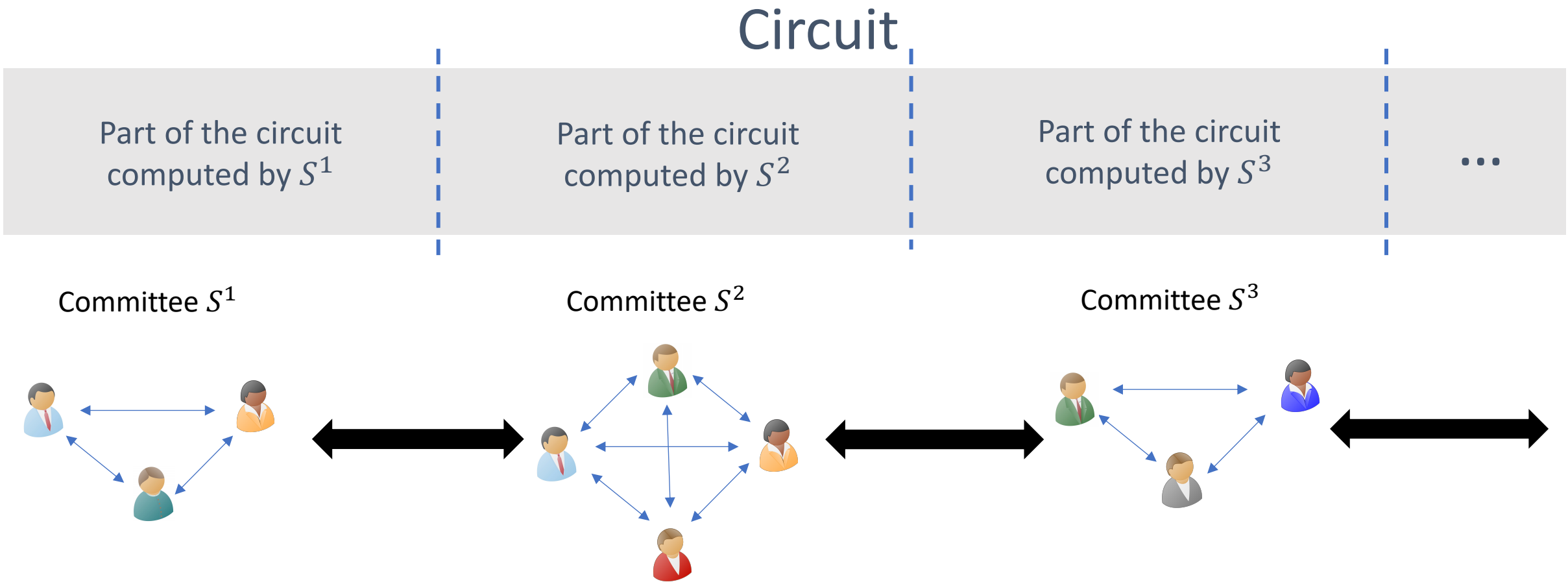


Committee Selection/Corruption

Fluid MPC Protocol

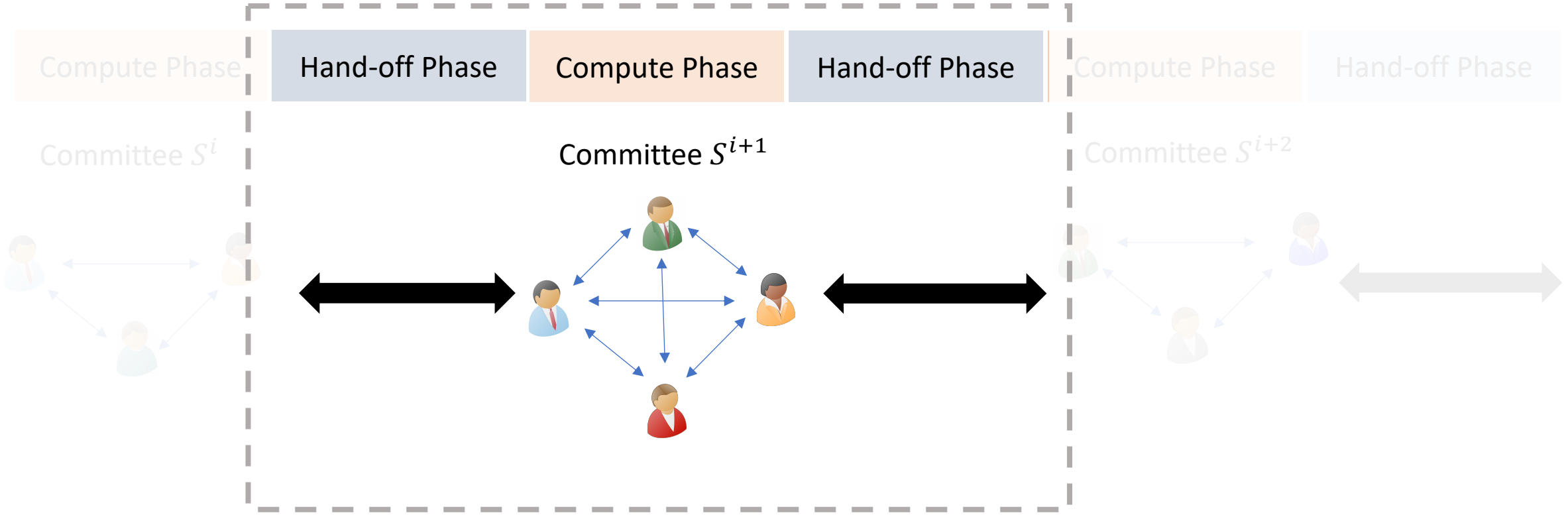


Division of Work



Per-committee work independent of the depth of the circuit

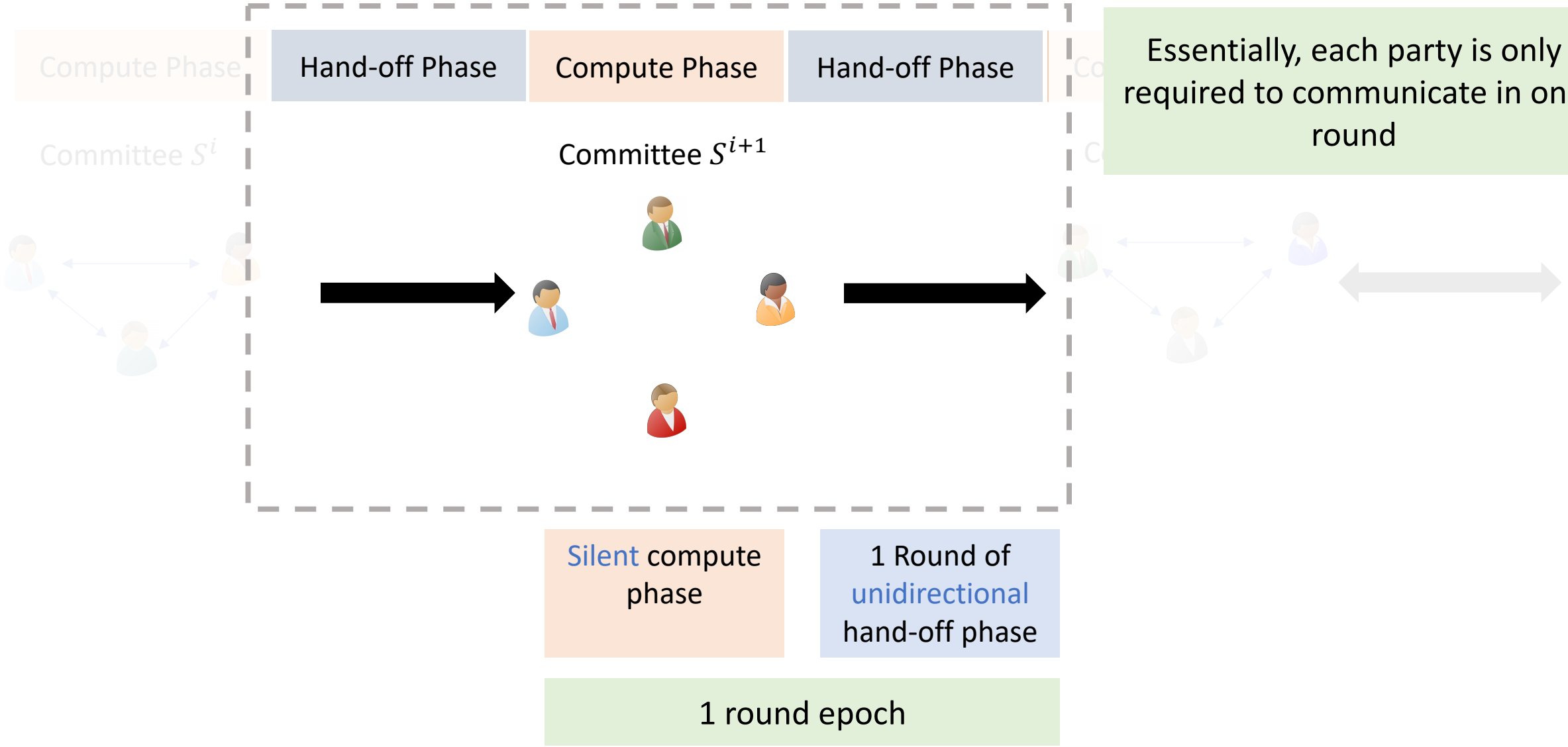
Fluidity



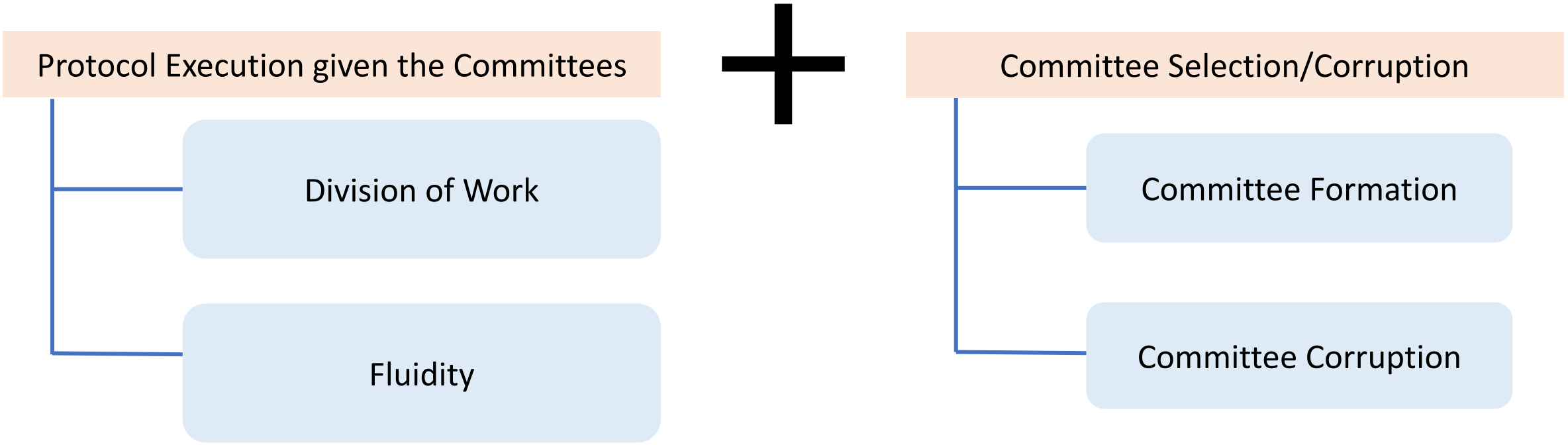
Fluidity is the minimum commitment a server needs to make for participating in the protocol.

Measured by the number of rounds in an epoch

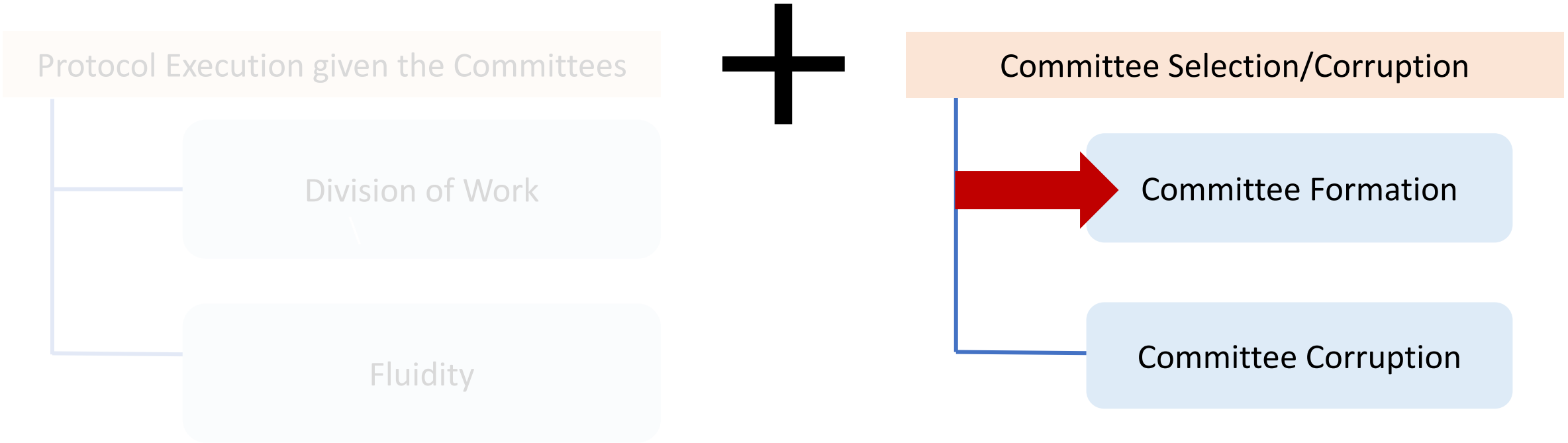
Maximal Fluidity



Fluid MPC Protocol



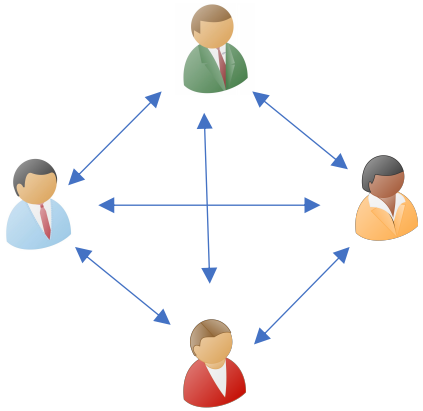
Fluid MPC Protocol



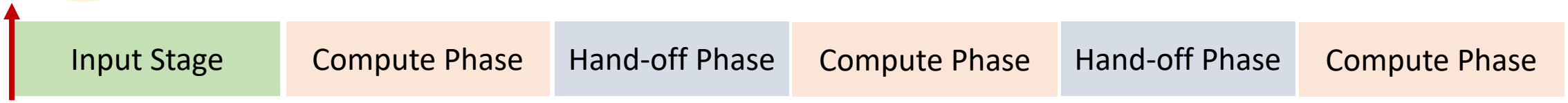
Committees: When are they formed?

Committees: When are they formed?

Committee S^1

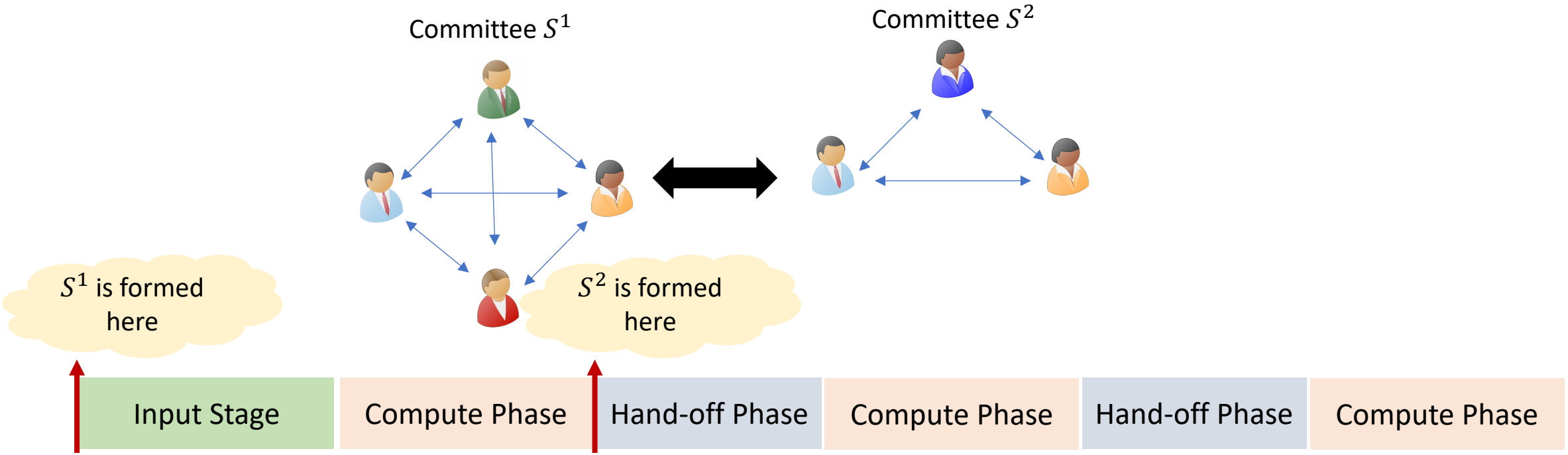


S^1 is formed here



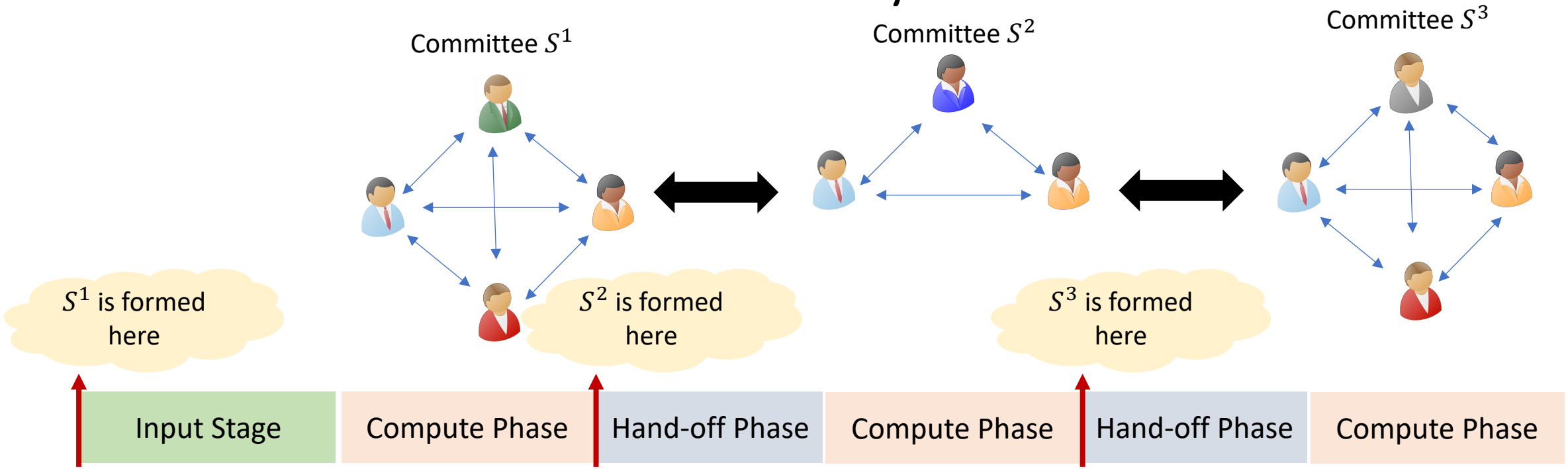
On-the-fly Committee Formation: Committee for each epoch is known at the start of the hand-off phase of the previous epoch.

Committees: When are they formed?



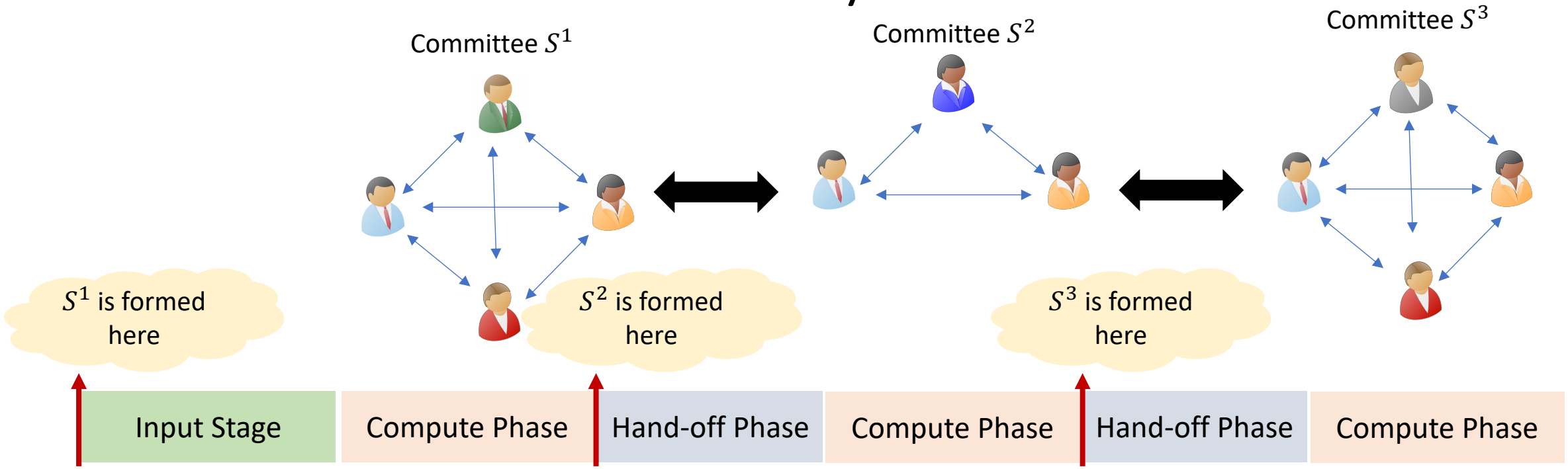
On-the-fly Committee Formation: Committee for each epoch is known at the start of the hand-off phase of the previous epoch.

Committees: When are they formed?



On-the-fly Committee Formation: Committee for each epoch is known at the start of the hand-off phase of the previous epoch.

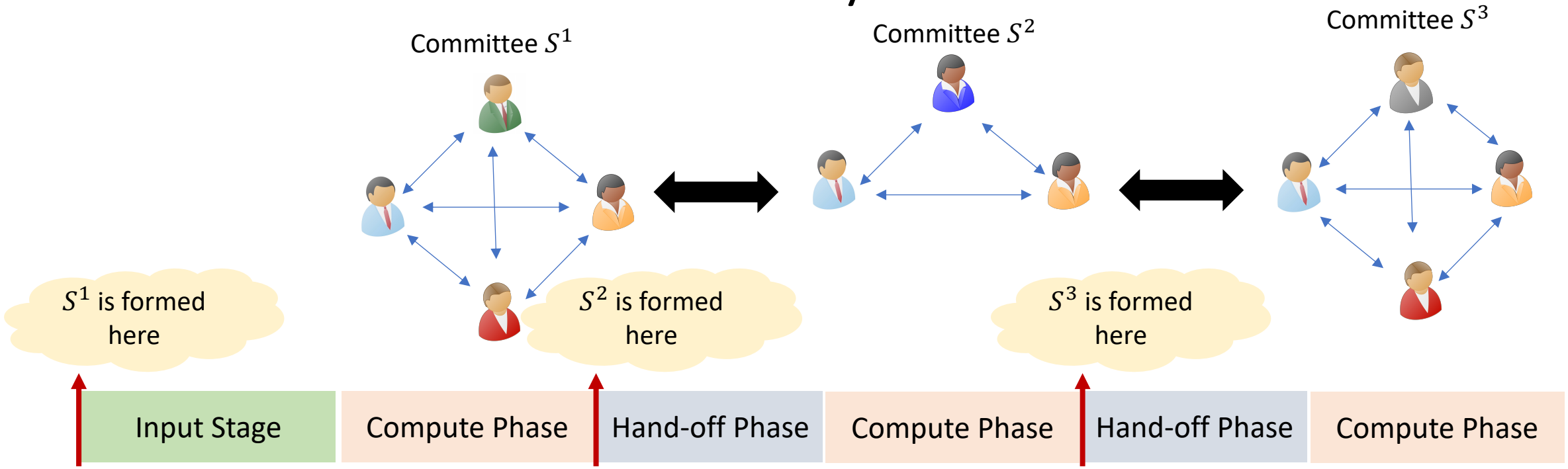
Committees: How are they formed?



On-the-fly Committee Formation:

Volunteer: Anyone who volunteers can join the computation (Corruption threshold is difficult to enforce)

Committees: How are they formed?

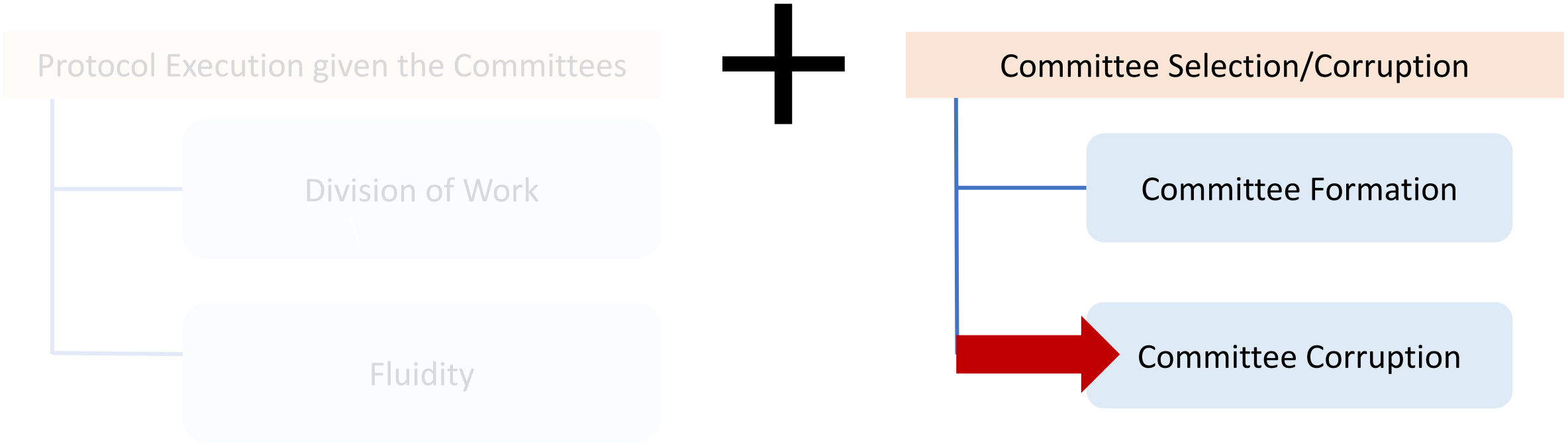


On-the-fly Committee Formation:

Volunteer: Anyone who volunteers can join the computation (Corruption threshold is difficult to enforce)

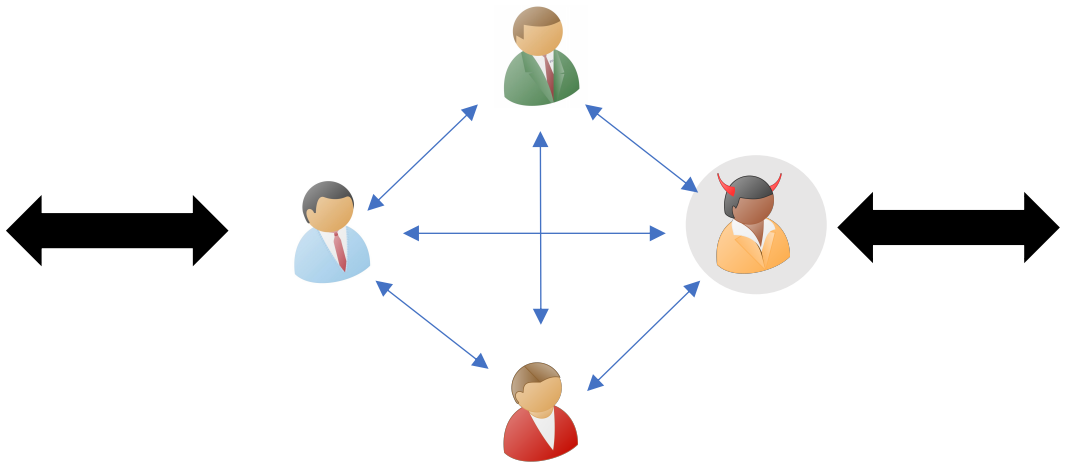
Elected: Anyone can nominate themself and an election process decides which nominees will participate (e.g., [BGGHKLRR20, GHMNY20] uses proof-of-stake blockchains)

Fluid MPC Protocol



Committee Corruption

When can a server be corrupted?

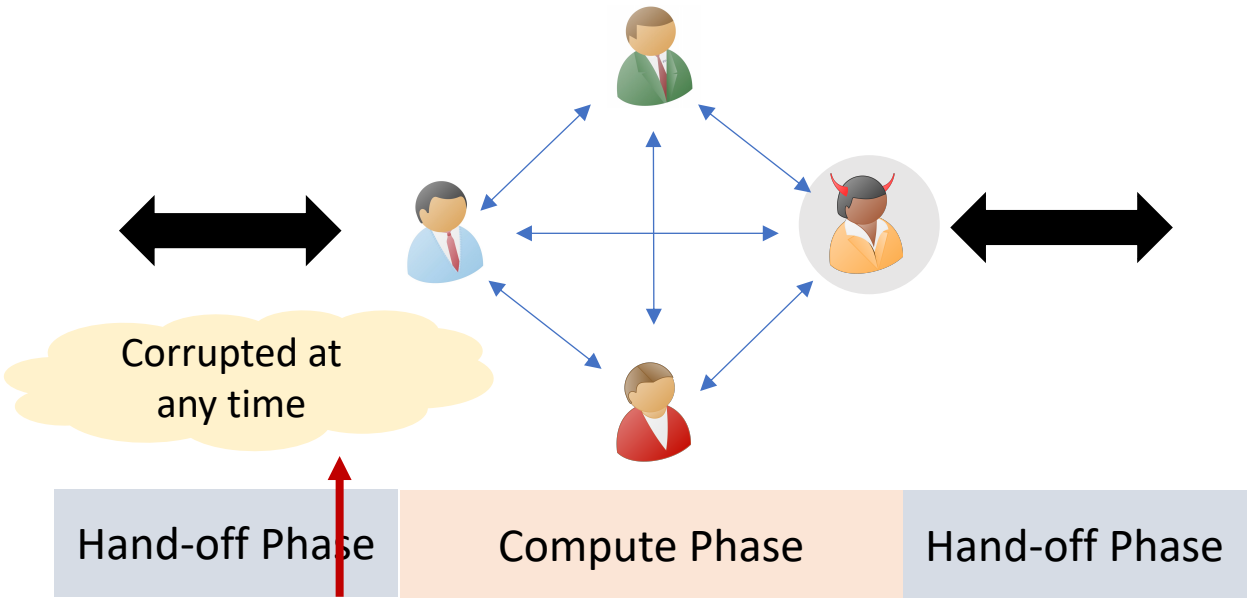


Hand-off Phase | Compute Phase | Hand-off Phase

Adaptive Corruption

Committee Corruption

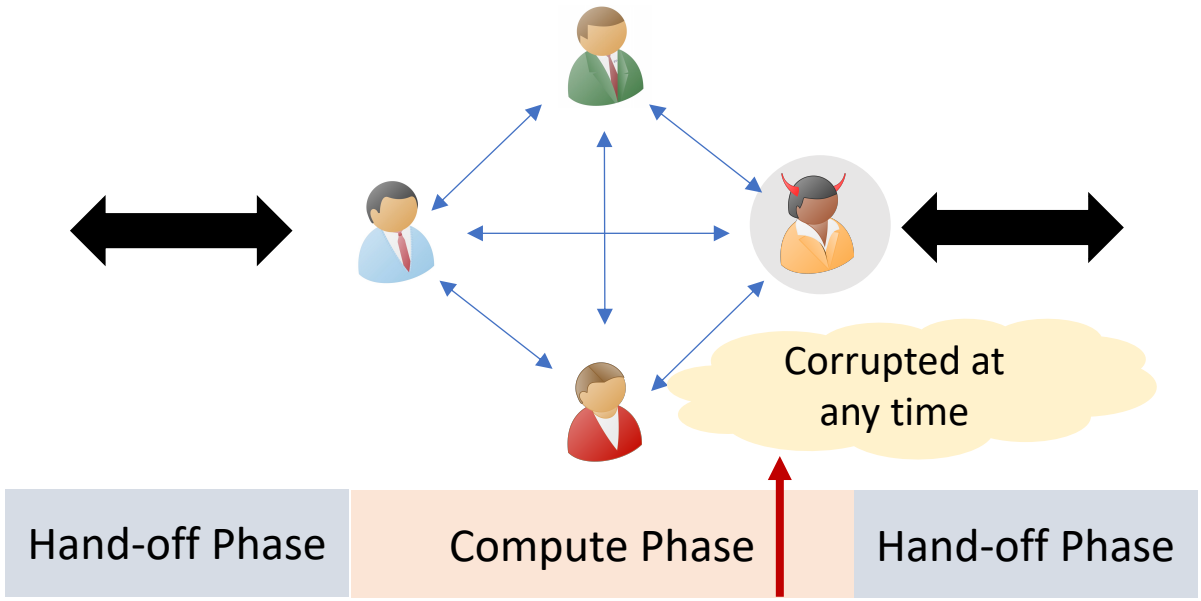
When can a server be corrupted?



Adaptive Corruption

Committee Corruption

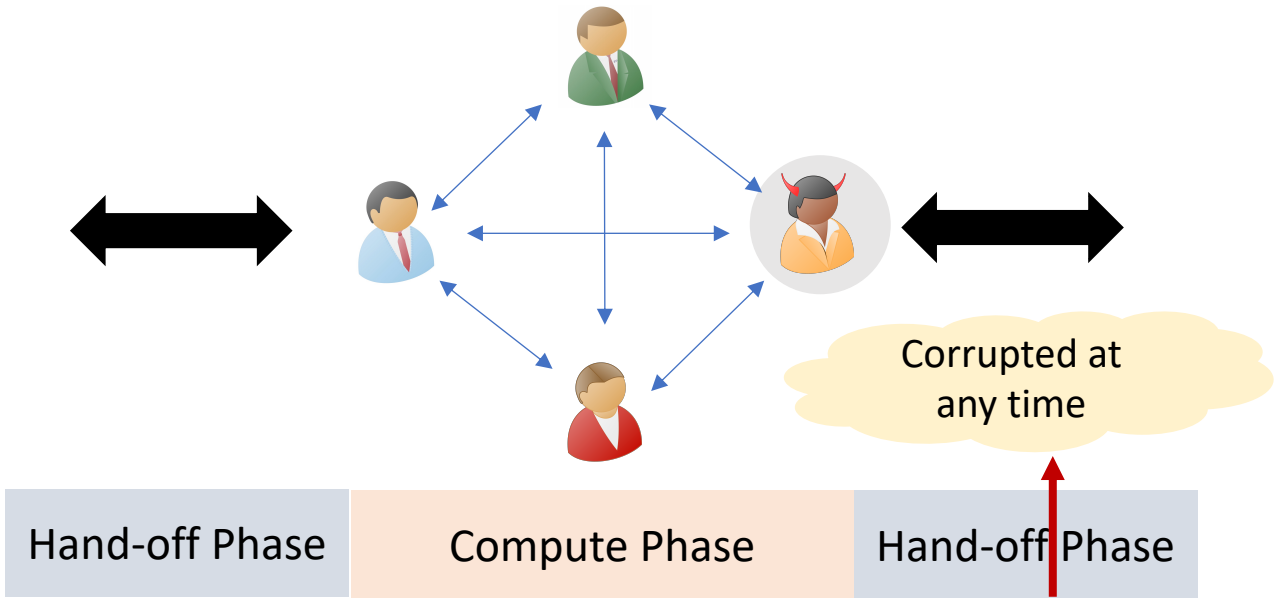
When can a server be corrupted?



Adaptive Corruption

Committee Corruption

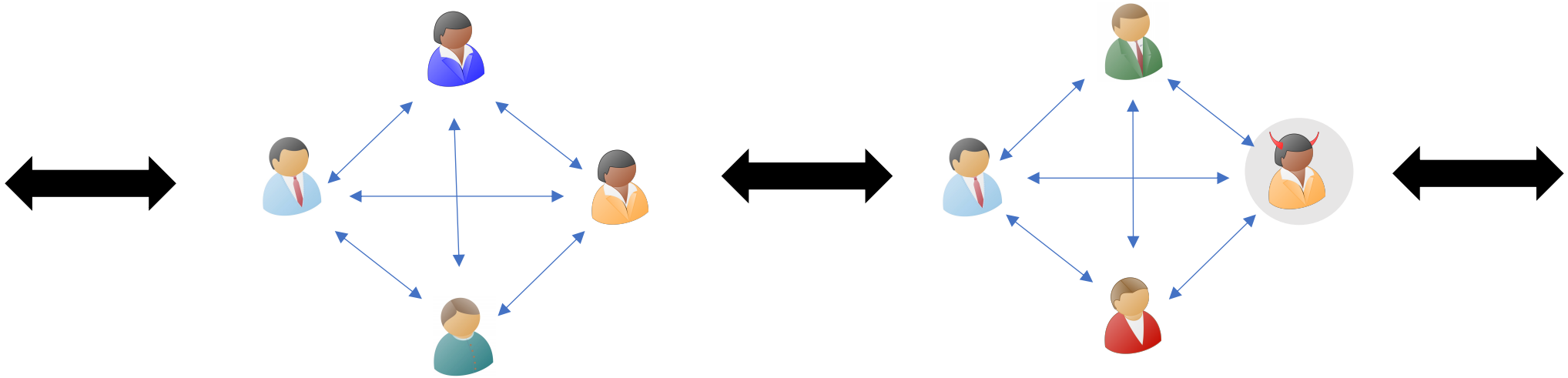
When can a server be corrupted?



Adaptive Corruption

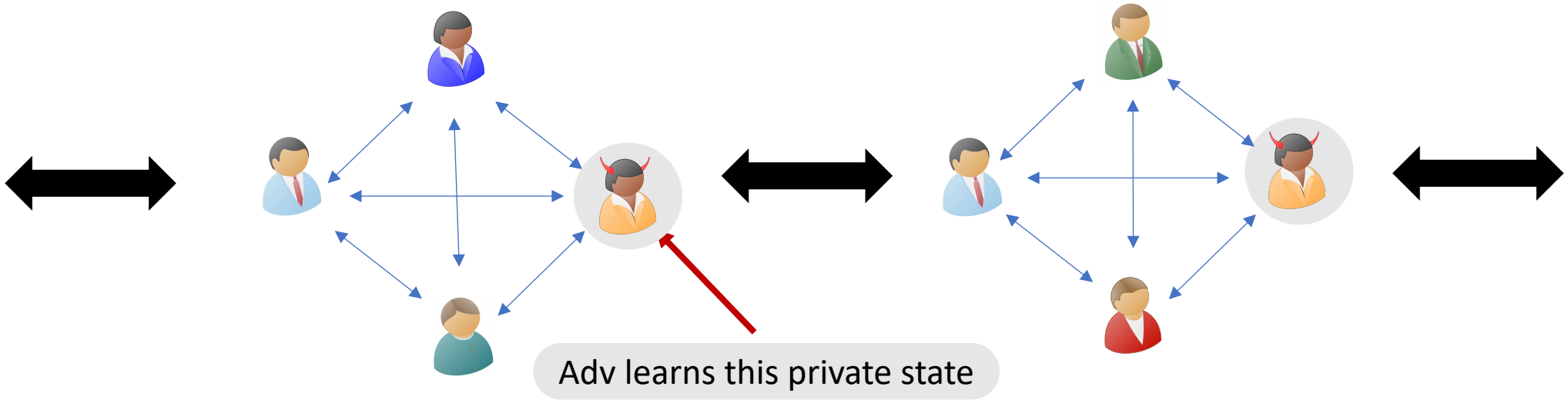
Effect of Committee Corruption on Prior Epochs

What effect does corrupting a server have on the prior epochs where it participated?



Effect of Committee Corruption on Prior Epochs

What effect does corrupting a server have on the prior epochs where it participated?



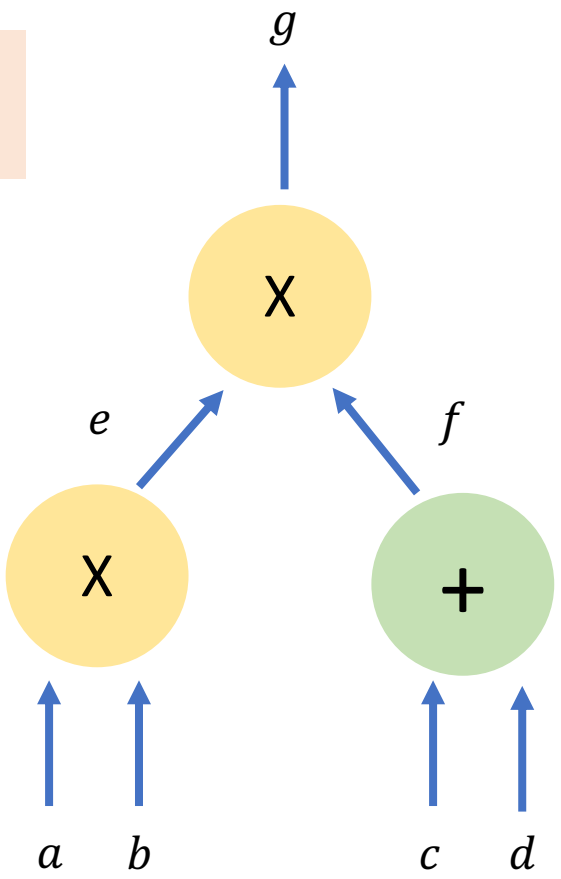
If there is overlap across committees, a server can only be corrupted if it does not violate the corruption threshold of prior epochs.

Fluid MPC Protocol (Semi-Honest)

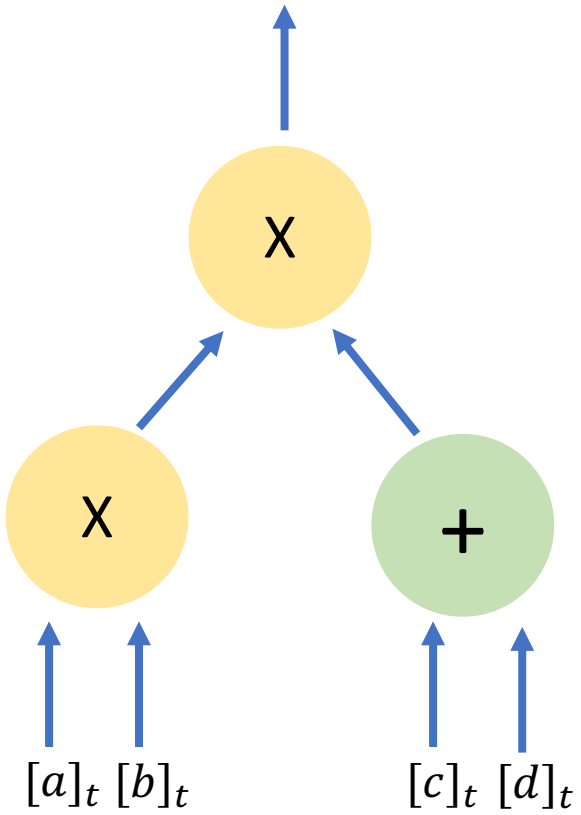
Semi-Honest BGW [GRR98] can be adapted to obtain a maximally Fluid semi-honest MPC

Semi-honest BGW [GRR98]

Gate-by-Gate evaluation on secret shared inputs



Semi-honest BGW [GRR98]



Input sharing: t-out-of-n shares of inputs

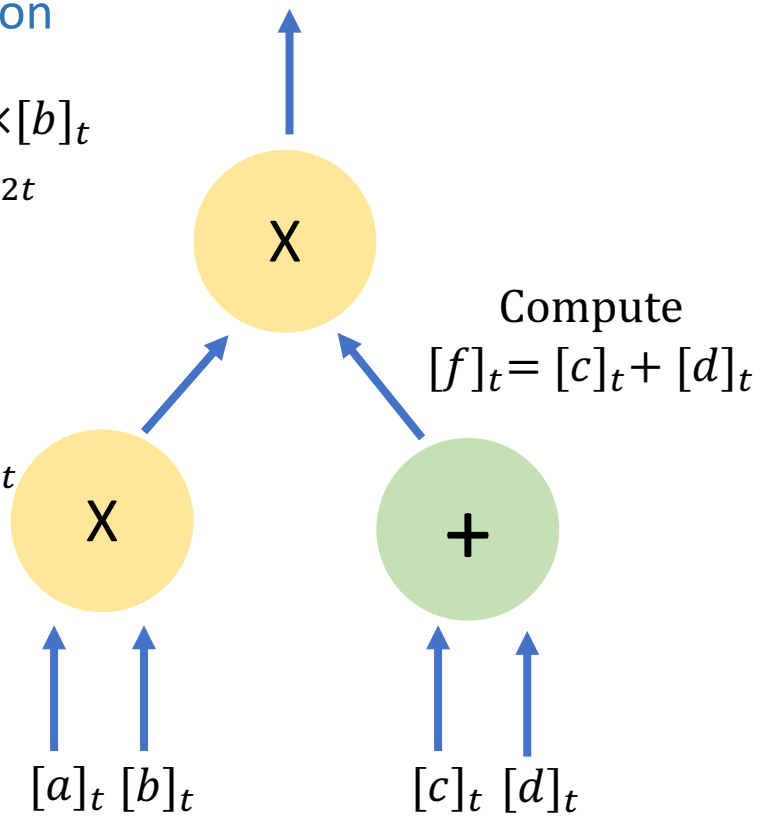
Semi-honest BGW [GRR98]

Gate-by-Gate Evaluation

Compute $[e]_{2t} = [a]_t \times [b]_t$
$[[e]_{2t}]_t \leftarrow [e]_{2t}$

Exchange $[[e]_{2t}]_t$
(Shares of Shares)

Compute $[e]_t \leftarrow [[e]_{2t}]_t$



Input sharing: t-out-of-n shares of inputs

Semi-honest BGW [GRR98]

Output Reconstruction

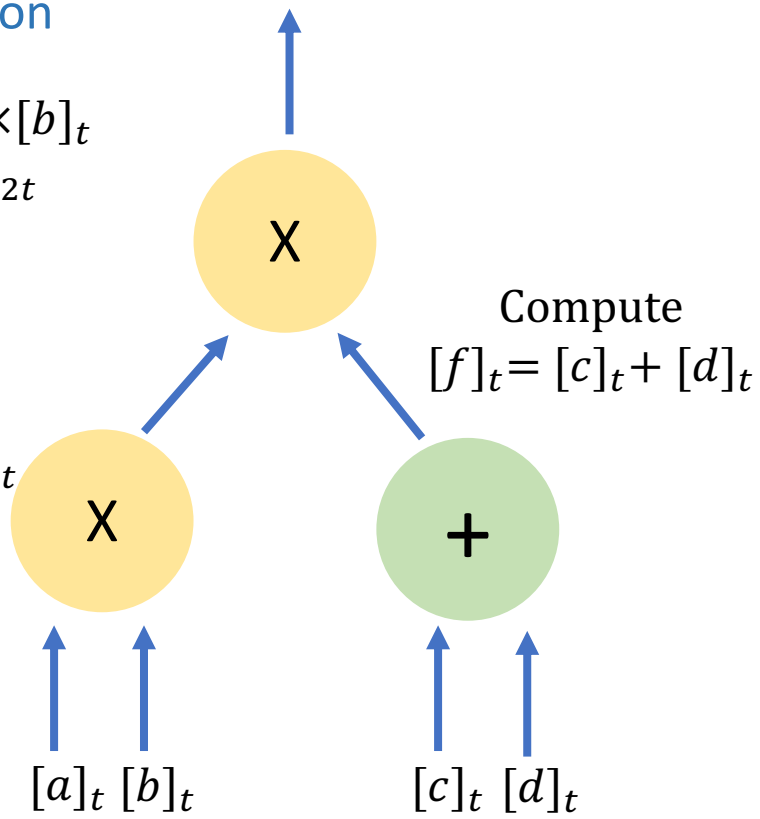
$g \leftarrow [g]_t$

Gate-by-Gate Evaluation

Compute $[e]_{2t} = [a]_t \times [b]_t$
$[[e]_{2t}]_t \leftarrow [e]_{2t}$

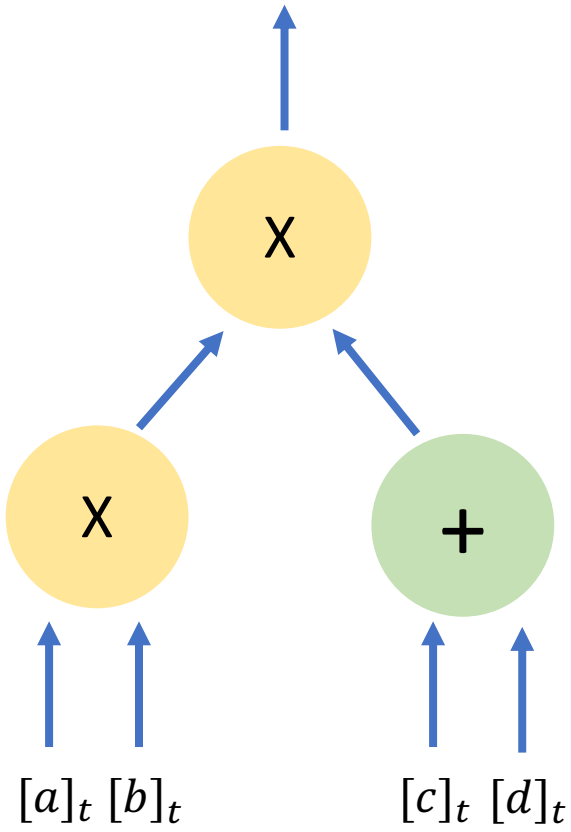
Exchange $[[e]_{2t}]_t$
(Shares of Shares)

Compute $[e]_t \leftarrow [[e]_{2t}]_t$



Input sharing: t-out-of-n shares of inputs

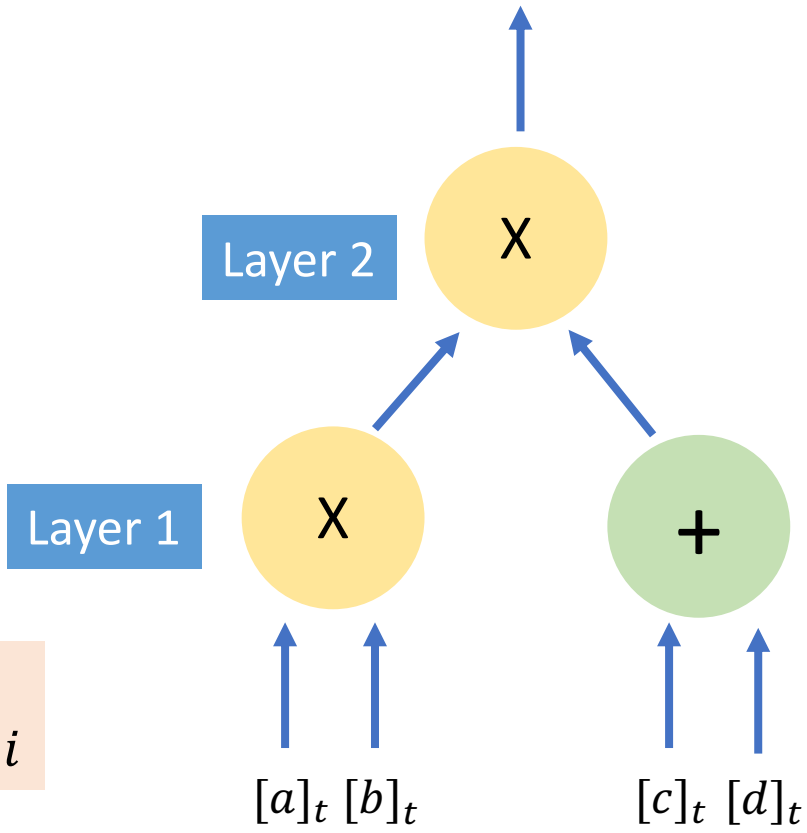
Semi-honest Fluid-BGW



Input Phase: Clients send t-out-of-n shares of inputs to the first committee

Semi-honest Fluid-BGW

Execution Stage



Layer-wise computations
Committee i computes layer i

Input Phase: Clients send t-out-of-n shares of inputs to the first committee

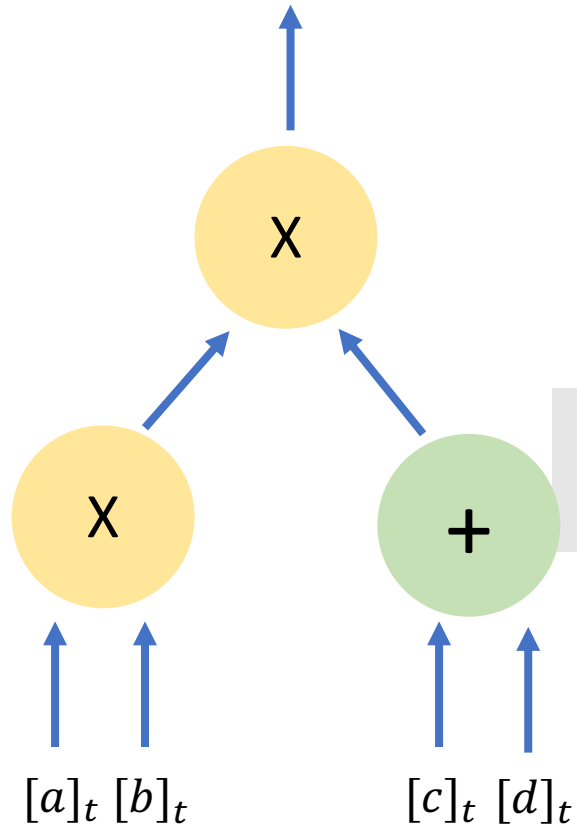
Semi-honest Fluid-BGW

Execution Stage

Computation Phase : $[e]_t \leftarrow [[e]_{2t}]_t$
of Epoch 2

Handoff Phase $[[e]_{2t}]_t$

Computation Phase : $[e]_{2t} = [a]_t \times [b]_t$
of Epoch 1 $[[e]_{2t}]_t \leftarrow [e]_{2t}$



Computation Phase : $[f]_t \leftarrow [[f]_t]_t$
of Epoch 2

Handoff Phase $[[f]_t]_t$

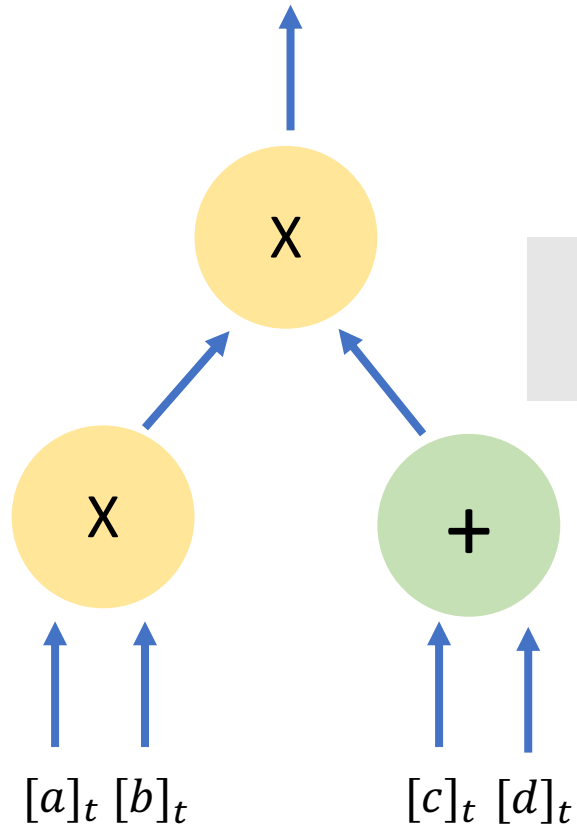
Computation Phase : $[f]_t = [c]_t + [d]_t$
of Epoch 1 $[[f]_t]_t \leftarrow [f]_t$

Input Phase: Clients send t-out-of-n shares of inputs to the first committee

Semi-honest Fluid-BGW

Execution Stage

Computation Phase : of Epoch 2	$[e]_t \leftarrow [[e]_{2t}]_t$
Handoff Phase	$[[e]_{2t}]_t$
Computation Phase : of Epoch 1	$[e]_{2t} = [a]_t \times [b]_t$ $[[e]_{2t}]_t \leftarrow [e]_{2t}$



Computation Phase : of Epoch 2	$[f]_t \leftarrow [[f]_t]_t$
Handoff Phase	$[[f]_t]_t$
Computation Phase : of Epoch 1	$[f]_t = [c]_t + [d]_t$ $[[f]_t]_t \leftarrow [f]_t$

Input Phase: Clients send t-out-of-n shares of inputs to the first committee

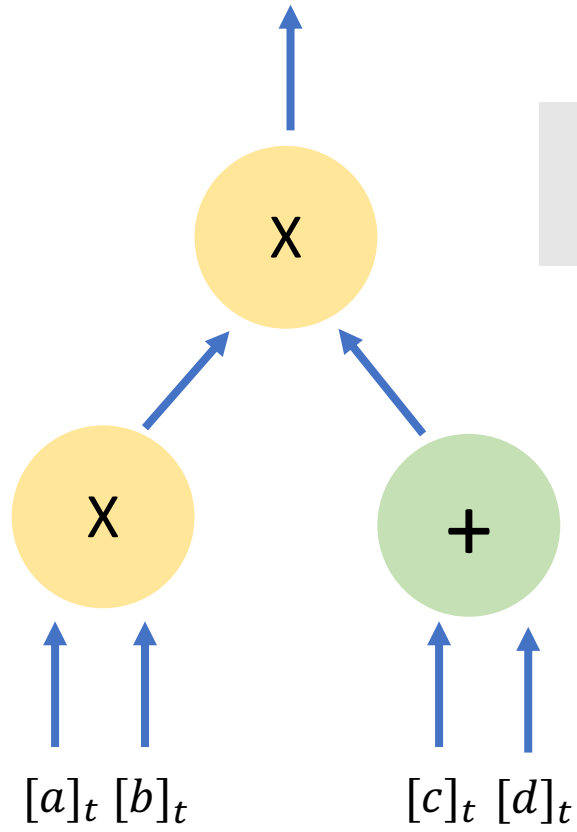
Semi-honest Fluid-BGW

Execution Stage

Computation Phase : $[e]_t \leftarrow [[e]_{2t}]_t$
of Epoch 2

Handoff Phase $[[e]_{2t}]_t$

Computation Phase : $[e]_{2t} = [a]_t \times [b]_t$
of Epoch 1 $[[e]_{2t}]_t \leftarrow [e]_{2t}$



Computation Phase : $[f]_t \leftarrow [[f]_t]_t$
of Epoch 2

Handoff Phase $[[f]_t]_t$

Computation Phase : $[f]_t = [c]_t + [d]_t$
of Epoch 1 $[[f]_t]_t \leftarrow [f]_t$

Input Phase: Clients send t-out-of-n shares of inputs to the first committee

Semi-honest Fluid-BGW

Output Phase

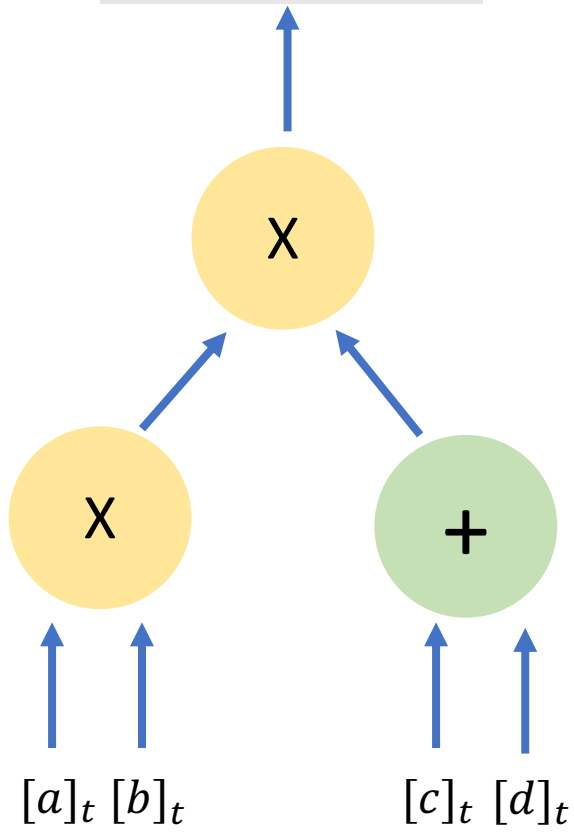
$g \leftarrow [g]_t$

Execution Stage

Computation Phase : $[e]_t \leftarrow [[e]_{2t}]_t$
of Epoch 2

Handoff Phase $[[e]_{2t}]_t$

Computation Phase : $[e]_{2t} = [a]_t \times [b]_t$
of Epoch 1 $[[e]_{2t}]_t \leftarrow [e]_{2t}$



Computation Phase : $[f]_t \leftarrow [[f]_t]_t$
of Epoch 2

Handoff Phase $[[f]_t]_t$

Computation Phase : $[f]_t = [c]_t + [d]_t$
of Epoch 1 $[[f]_t]_t \leftarrow [f]_t$

Input Phase: Clients send t-out-of-n shares of inputs to the first committee

Semi-honest Fluid-BGW

- ☑ Division of Work
- ☑ Maximal Fluidity

Output Phase

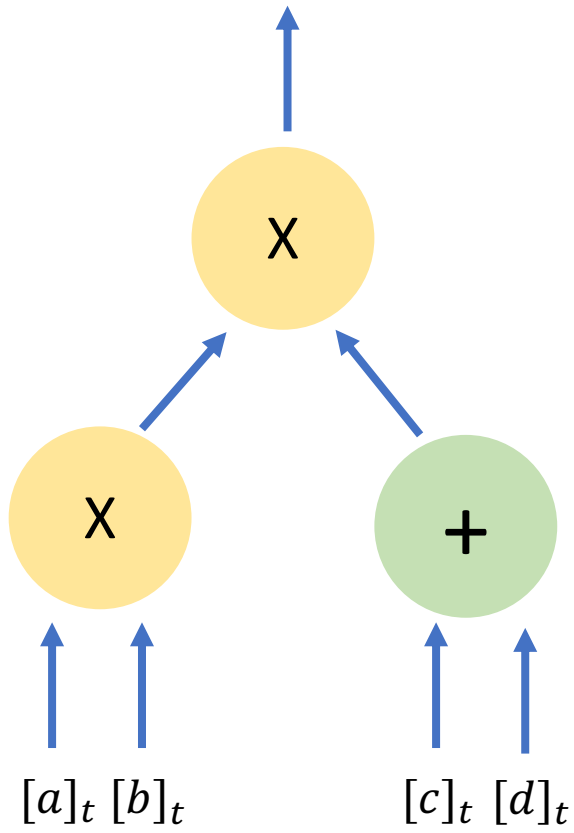
$g \leftarrow [g]_t$

Execution Stage

Computation Phase : $[e]_t \leftarrow [[e]_{2t}]_t$
of Epoch 2

Handoff Phase $[[e]_{2t}]_t$

Computation Phase : $[e]_{2t} = [a]_t \times [b]_t$
of Epoch 1 $[[e]_{2t}]_t \leftarrow [e]_{2t}$



Computation Phase : $[f]_t \leftarrow [[f]_t]_t$
of Epoch 2

Handoff Phase $[[f]_t]_t$

Computation Phase : $[f]_t = [c]_t + [d]_t$
of Epoch 1 $[[f]_t]_t \leftarrow [f]_t$

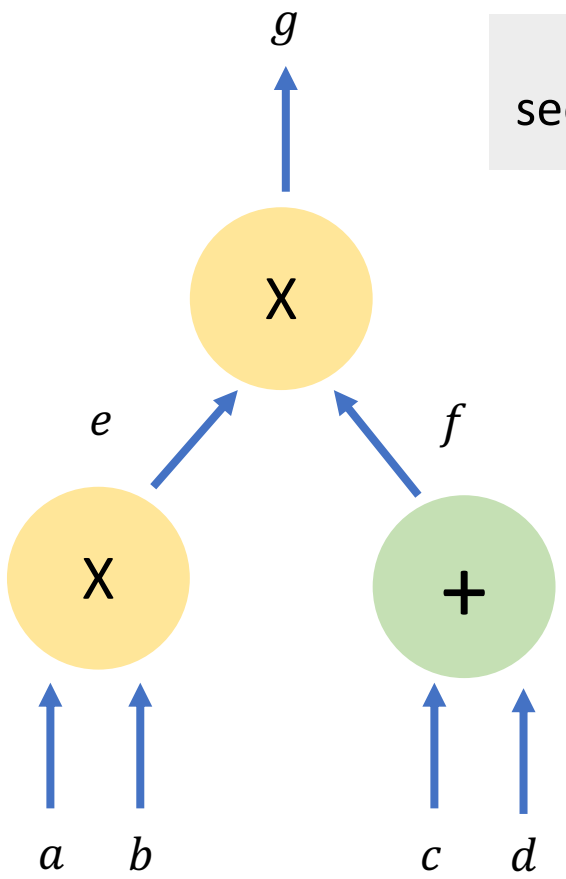
Input Phase: Clients send t-out-of-n shares of inputs to the first committee

Fluid MPC Protocol (Malicious)

1. A compiler that that transforms “certain” semi-honest Fluid MPC protocols into maliciously secure protocols:
   - security with abort
   - $4 \times$ communication complexity
   - Preserves fluidity

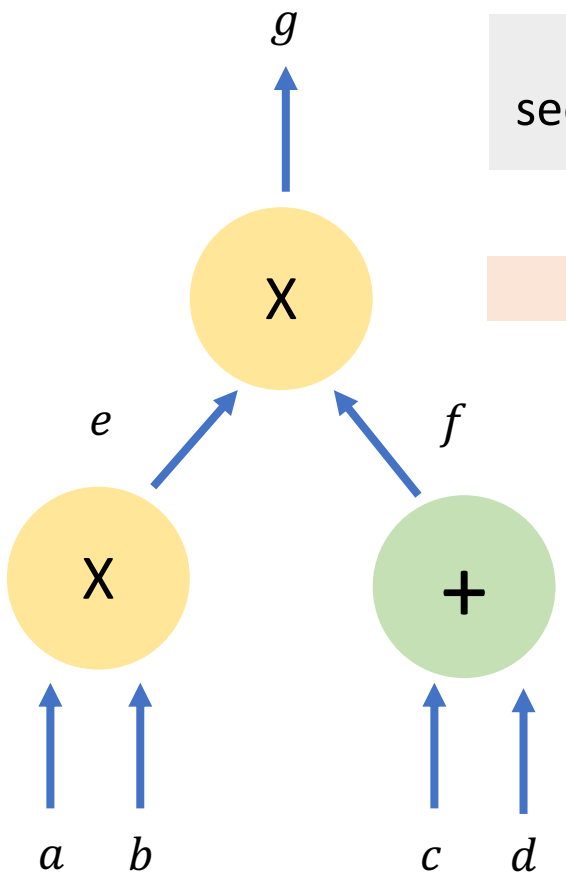
2. Provide Implementation of our protocol

Additive Attack Paradigm [GIPST14]



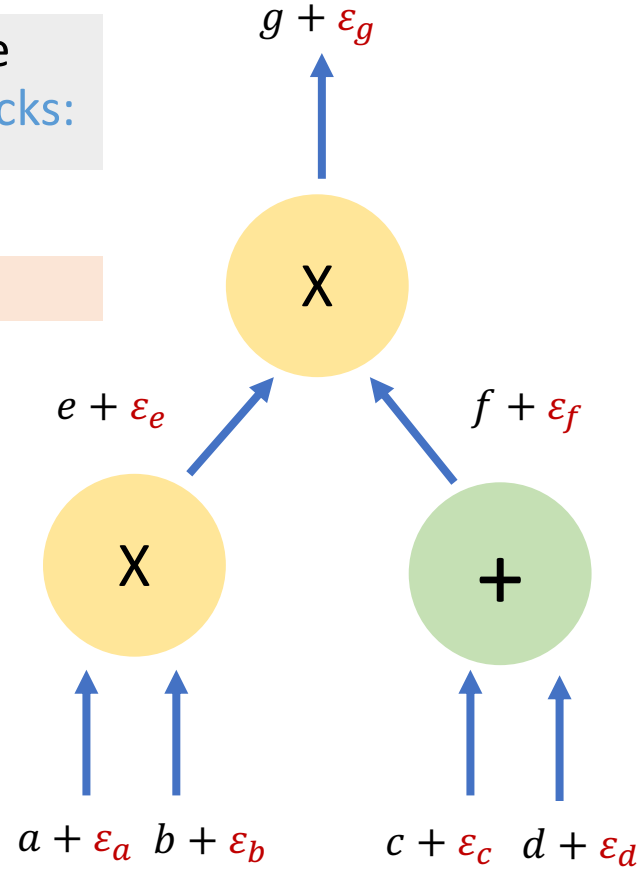
Most secret sharing based semi-honest protocols are secure against malicious adversaries up to additive attacks:

Additive Attack Paradigm [GIPST14]



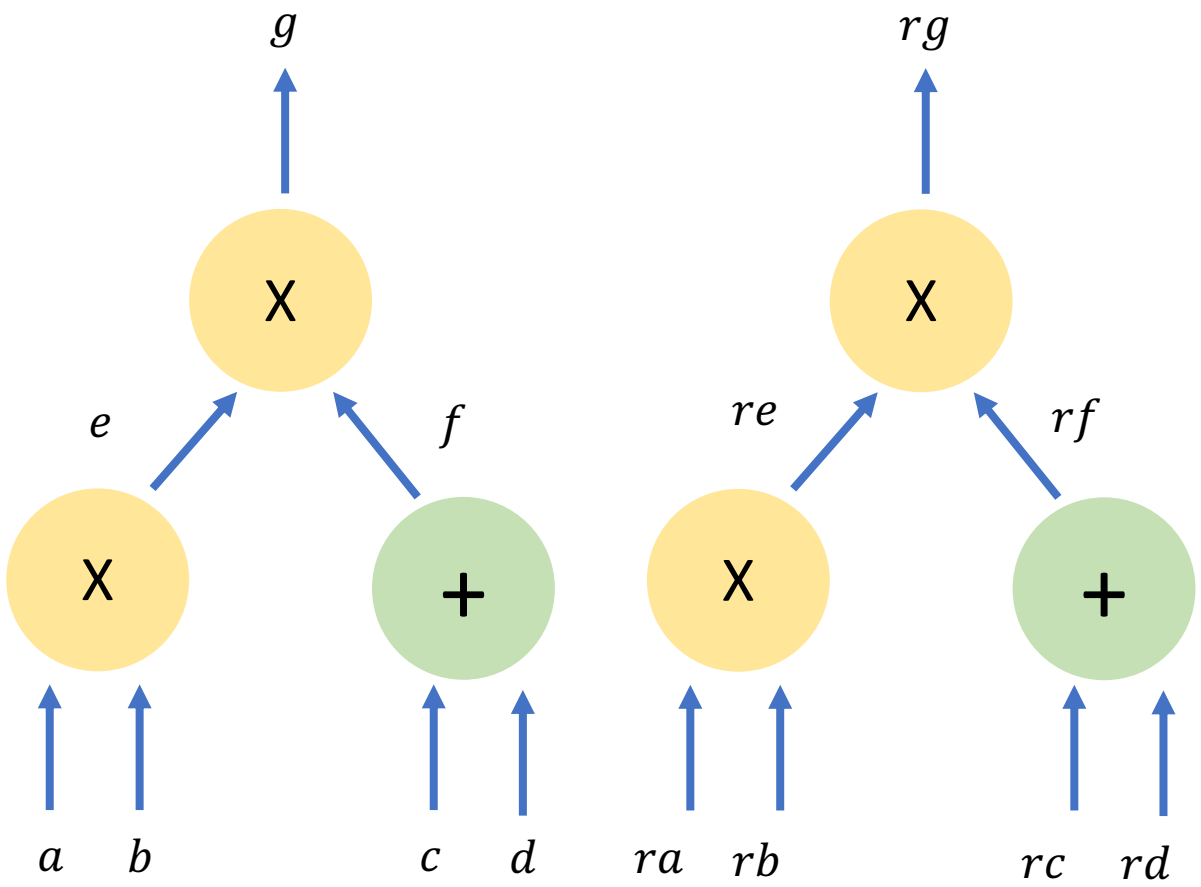
Most secret sharing based semi-honest protocols are secure against malicious adversaries up to additive attacks:

ε values are independent of the actual wire values



Efficient Maliciously Secure Protocols [DPSZ12,CGHIKLN18]

Modern efficient maliciously secure protocols rely on this additive attack paradigm.



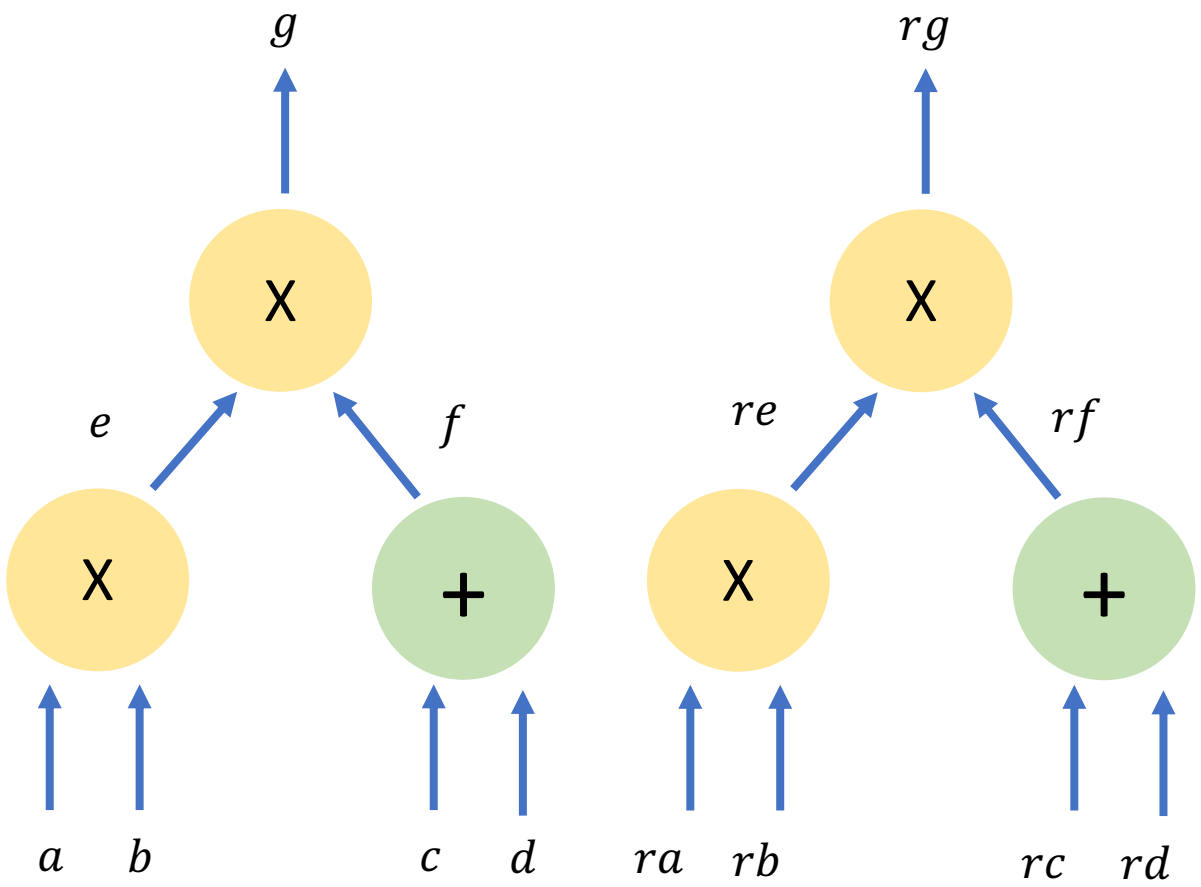
Semi-honest execution

Semi-honest execution

Dual execution: On actual inputs and randomized inputs.

Efficient Maliciously Secure Protocols [DPSZ12,CGHIKLN18]

Modern efficient maliciously secure protocols rely on this additive attack paradigm.



Semi-honest execution

Semi-honest execution

Dual execution: On actual inputs and randomized inputs.

Check for correctness by comparing a random linear combination of all the intermediate values at the end.

$$r(\alpha_1 a + \alpha_2 b + \cdots + \alpha_7 g)$$
$$=?=$$
$$\alpha_1 ra + \alpha_2 rb + \cdots + \alpha_7 rg$$

Maliciously secure Fluid MPC

Additive Attack Paradigm?

Semi-honest Fluid BGW  Maliciously secure Fluid MPC

Maliciously secure Fluid MPC

Additive Attack Paradigm?

Semi-honest Fluid BGW  Maliciously secure Fluid MPC

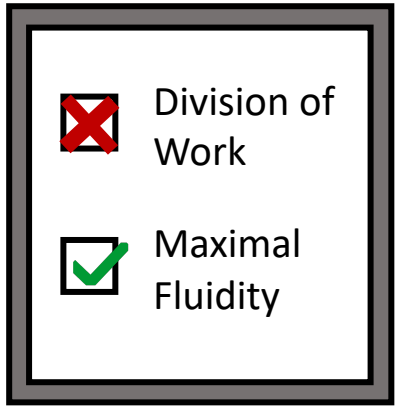
We Show: Additive Attack Paradigm extends to the Fluid MPC setting

Maliciously secure Fluid MPC

Can we use known techniques in the additive attack paradigm?

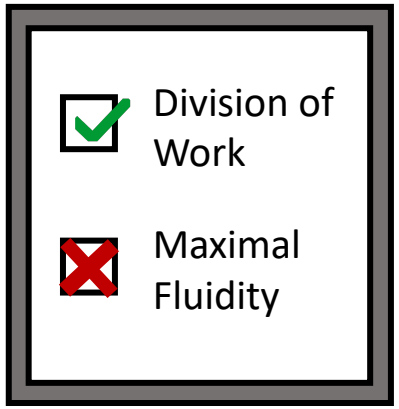
If the linear combination is computed at the end

All intermediate values must be passed along till the end of the protocol.

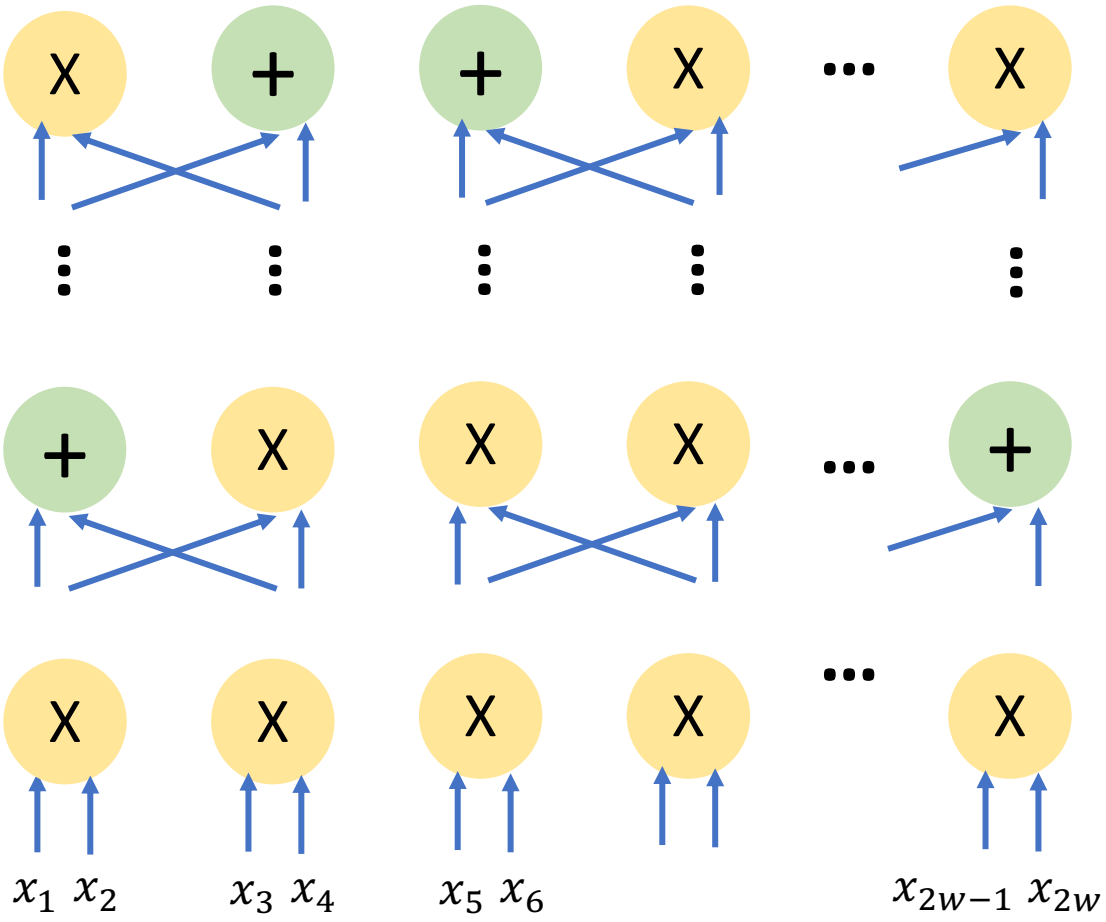


If the linear combination is computed incrementally layer-by-layer

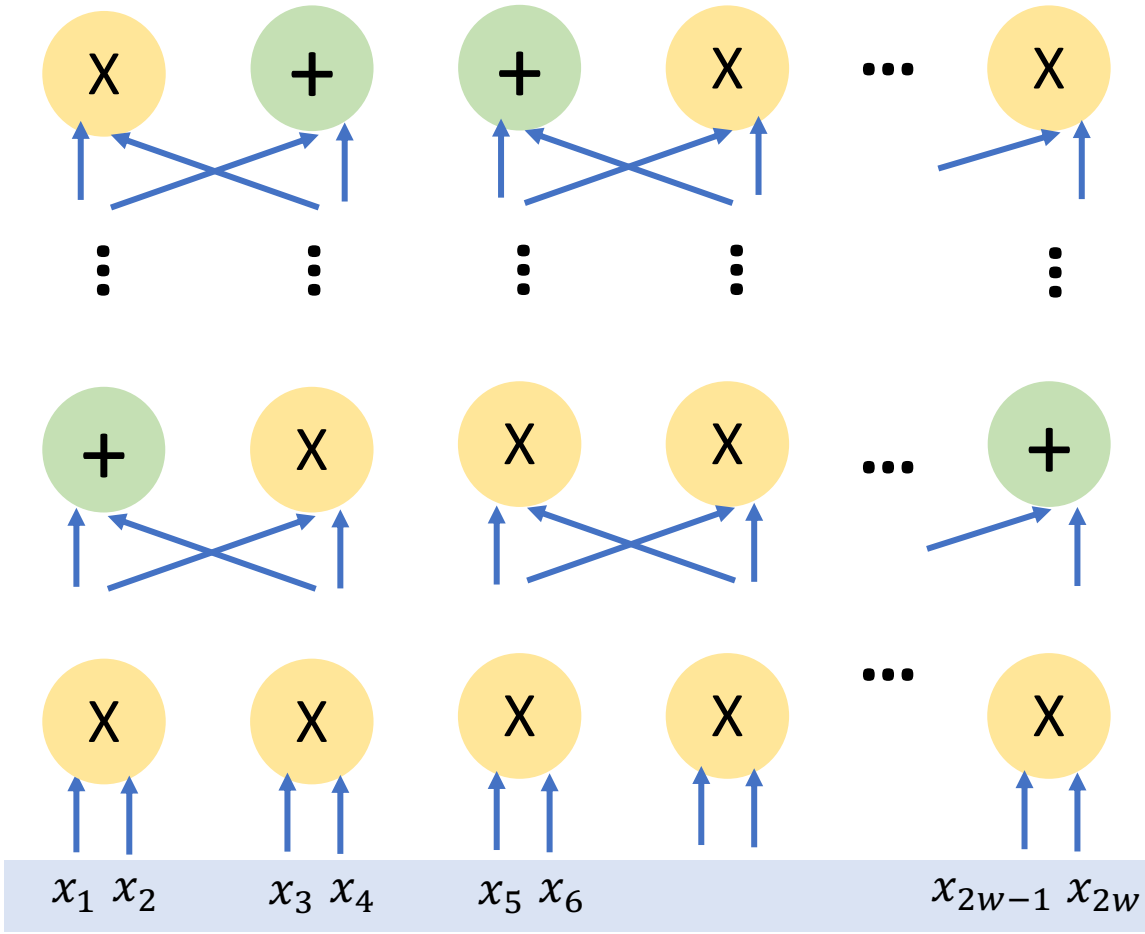
Random α values used in the linear combination will have to be generated on the fly, which may take many rounds.



Maliciously Secure Fluid MPC: Our Idea

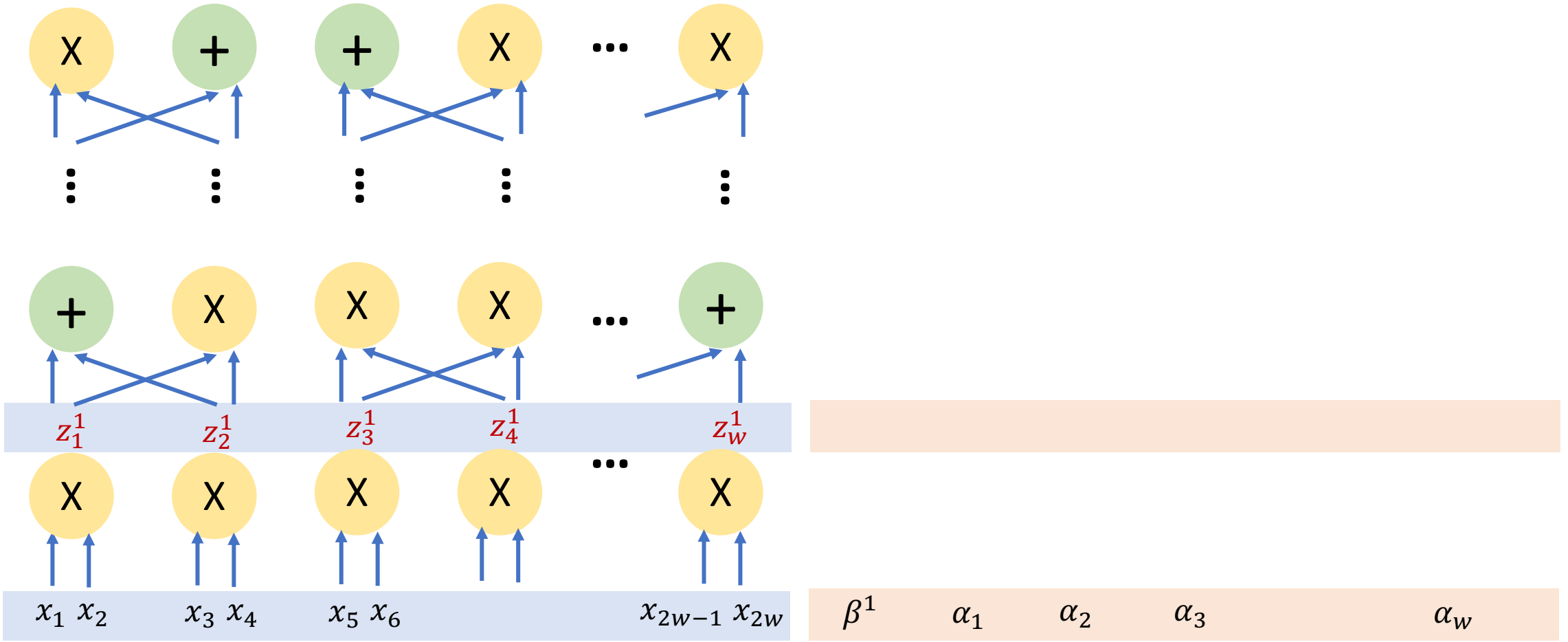


Maliciously Secure Fluid MPC: Our Idea

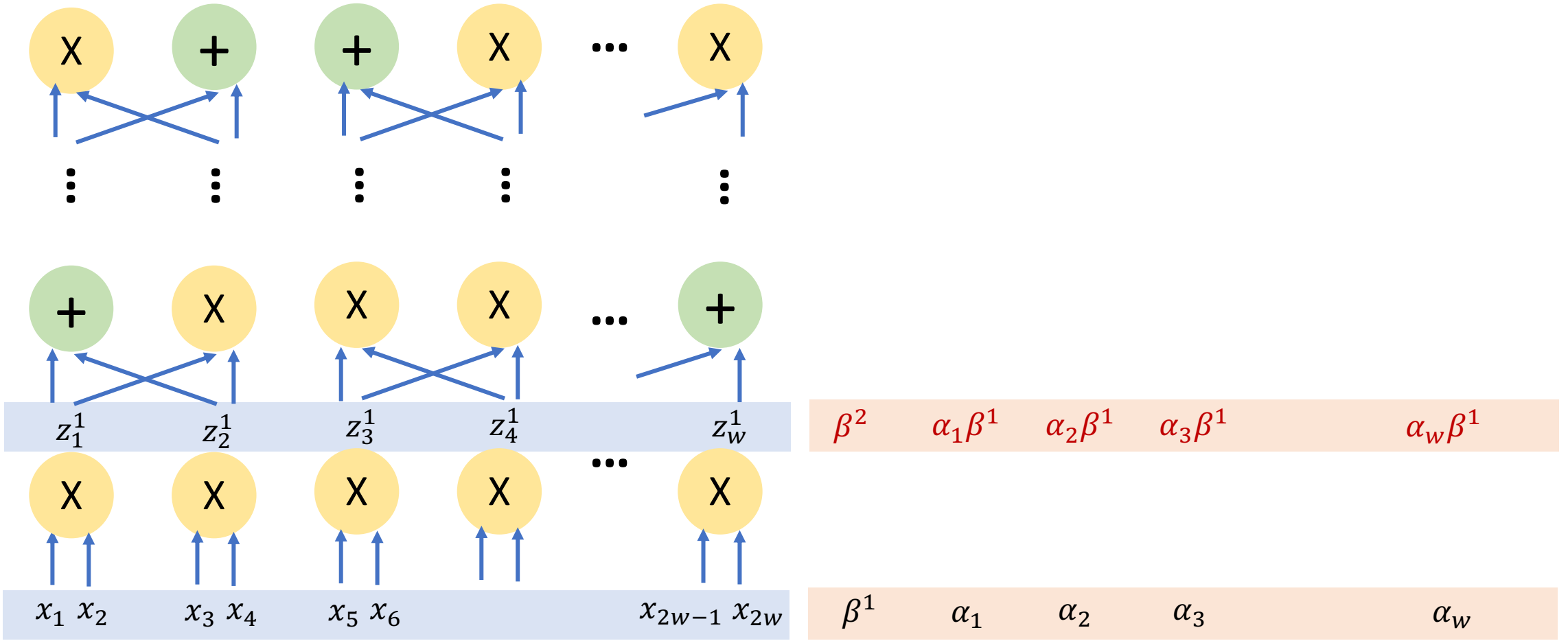


β^1 α_1 α_2 α_3 α_w

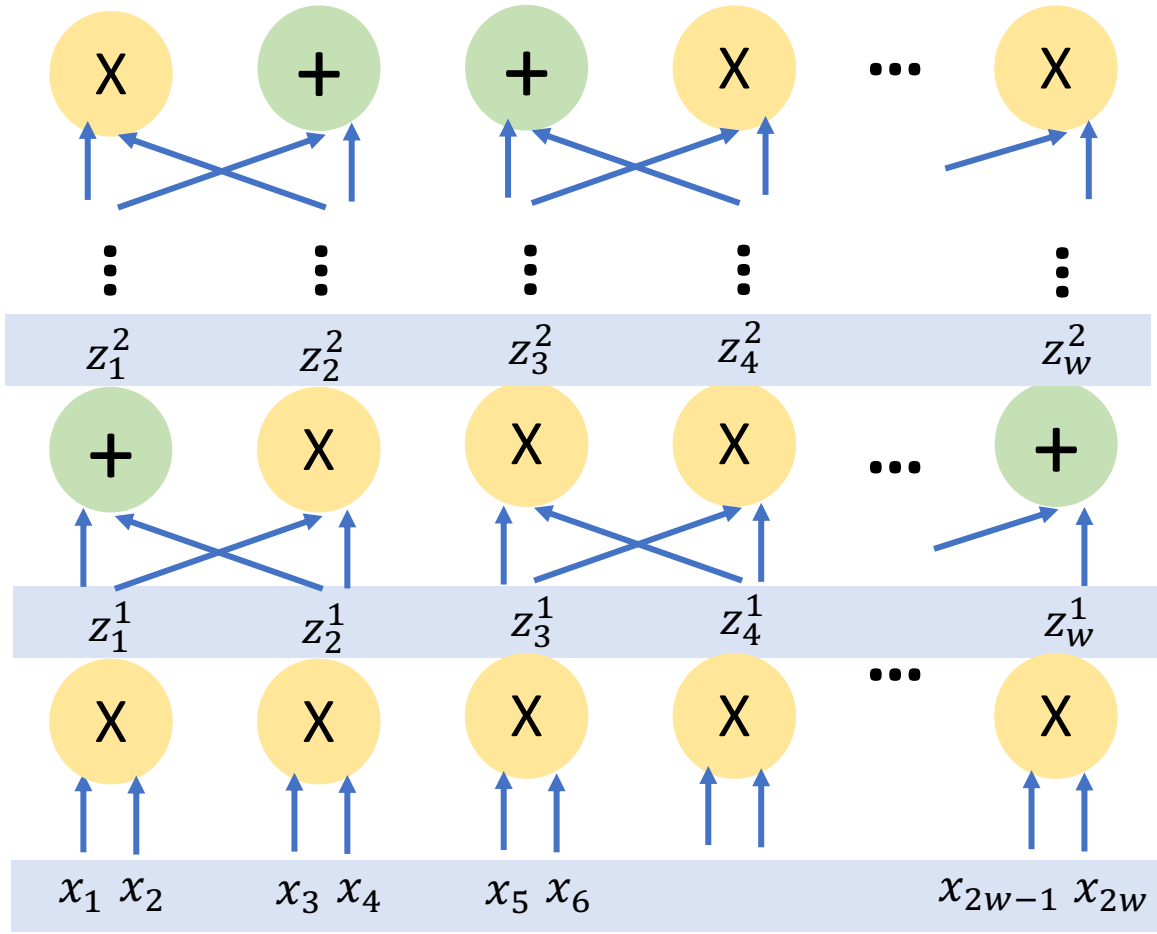
Maliciously Secure Fluid MPC: Our Idea



Maliciously Secure Fluid MPC: Our Idea



Maliciously Secure Fluid MPC: Our Idea

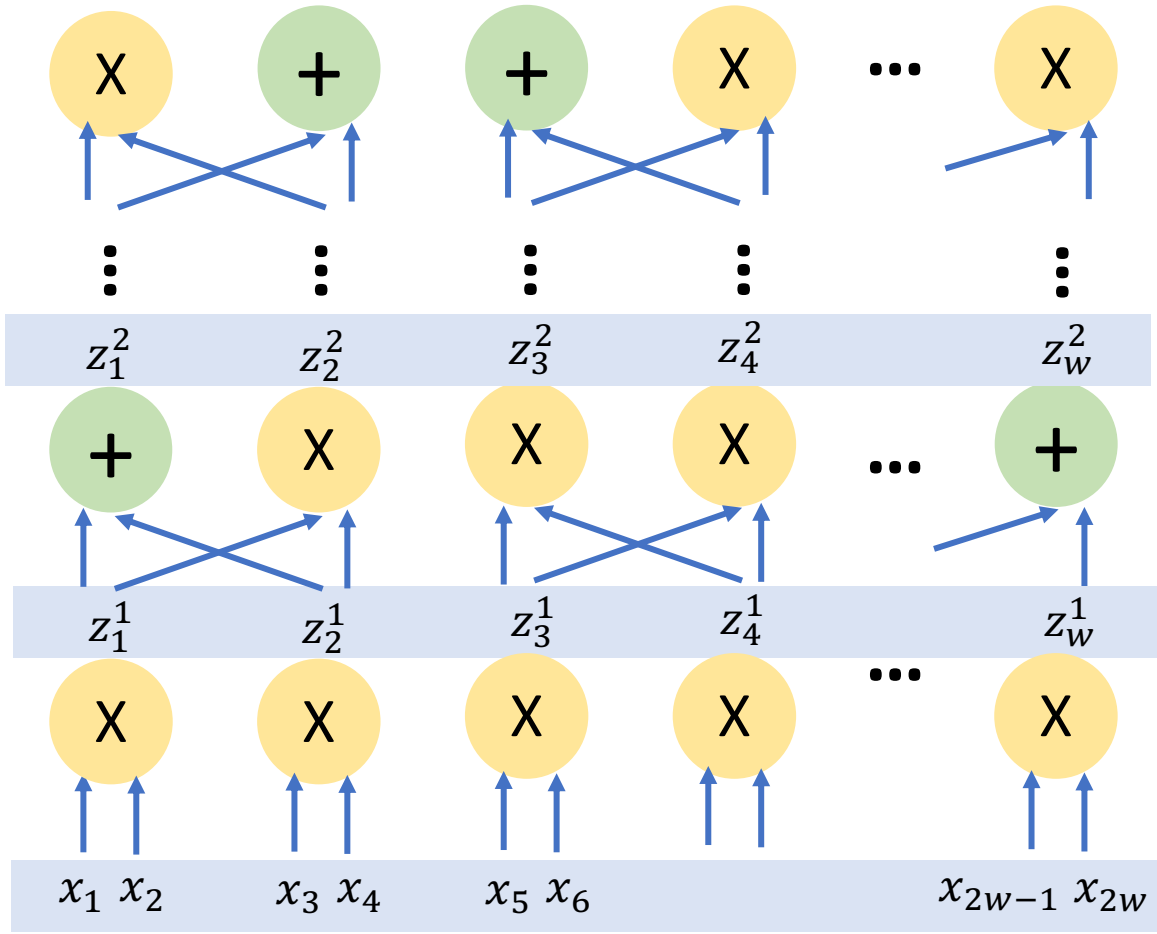


β^3 $\alpha_1\beta^2$ $\alpha_2\beta^2$ $\alpha_3\beta^2$ $\alpha_w\beta^2$

β^2 $\alpha_1\beta^1$ $\alpha_2\beta^1$ $\alpha_3\beta^1$ $\alpha_w\beta^1$

β^1 α_1 α_2 α_3 α_w

Maliciously Secure Fluid MPC: Our Idea



β^3 $\alpha_1\beta^2$ $\alpha_2\beta^2$ $\alpha_3\beta^2$ $\alpha_w\beta^2$

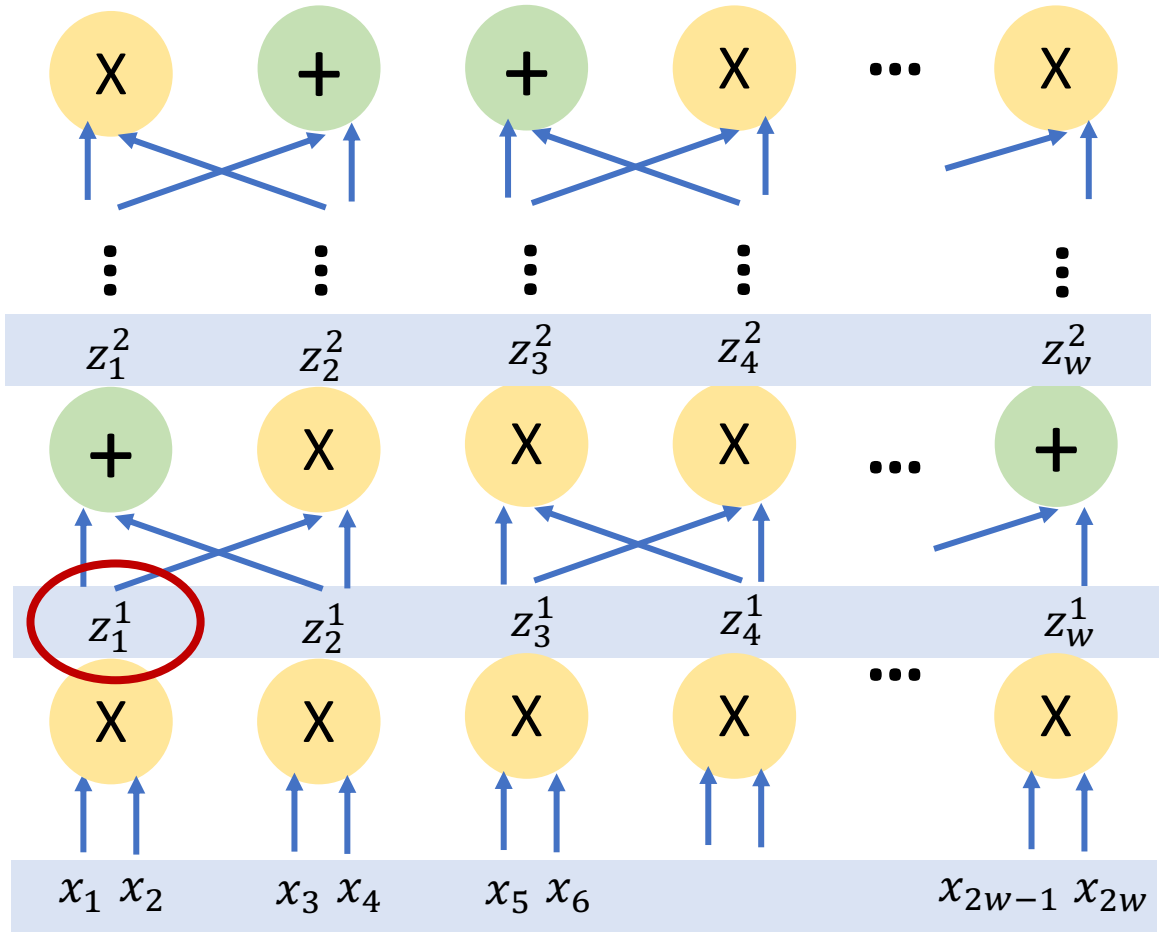
$$u_1 = u_0 + \alpha_1\beta^1 z_1^1 + \alpha_2\beta^1 z_2^1 + \cdots + \alpha_w\beta^1 z_w^1$$

β^2 $\alpha_1\beta^1$ $\alpha_2\beta^1$ $\alpha_3\beta^1$ $\alpha_w\beta^1$

$$u_0 = 0$$

β^1 α_1 α_2 α_3 α_w

Maliciously Secure Fluid MPC: Our Idea



β^3 $\alpha_1\beta^2$ $\alpha_2\beta^2$ $\alpha_3\beta^2$ $\alpha_w\beta^2$

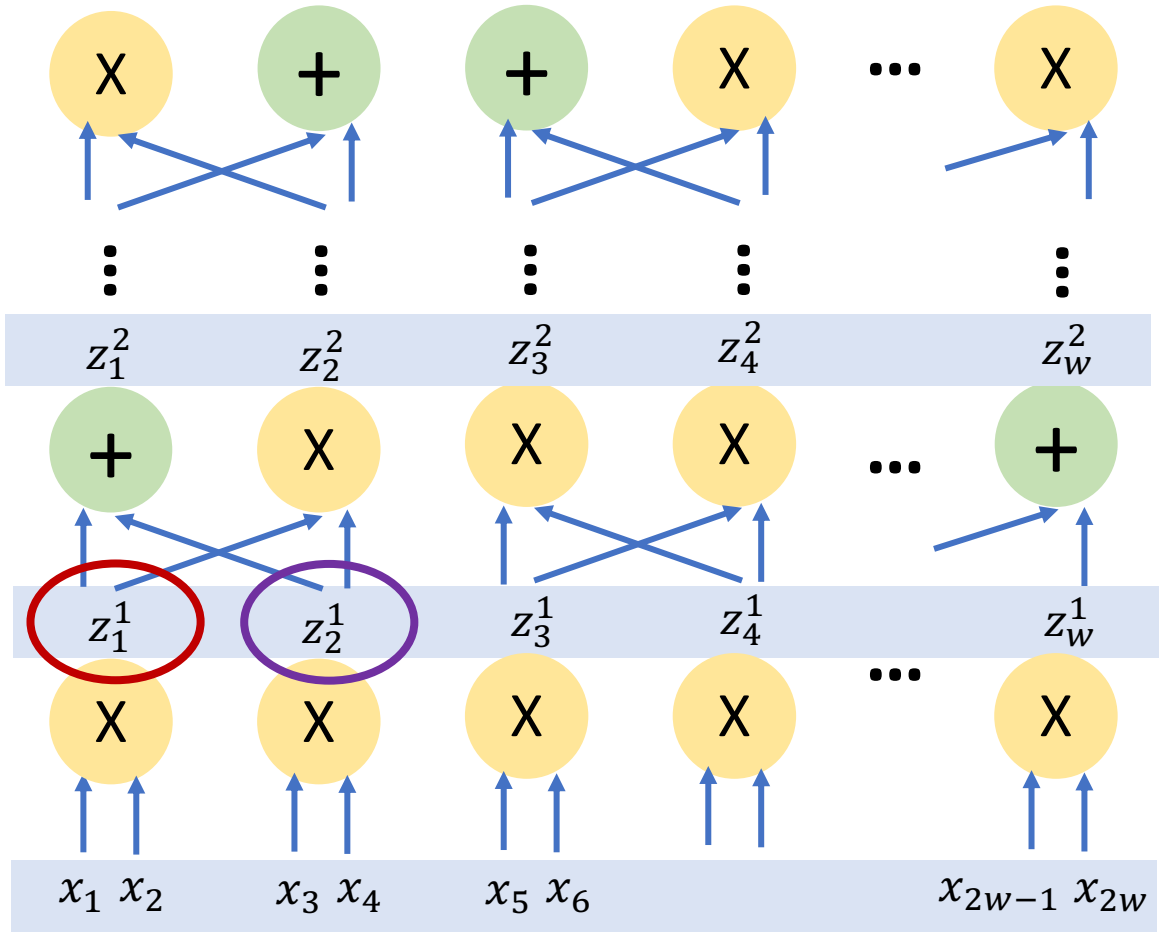
$$u_1 = u_0 + \alpha_1\beta^1 z_1^1 + \alpha_2\beta^1 z_2^1 + \cdots + \alpha_w\beta^1 z_w^1$$

β^2 $\alpha_1\beta^1$ $\alpha_2\beta^1$ $\alpha_3\beta^1$ $\alpha_w\beta^1$

$$u_0 = 0$$

β^1 α_1 α_2 α_3 α_w

Maliciously Secure Fluid MPC: Our Idea



β^3 $\alpha_1\beta^2$ $\alpha_2\beta^2$ $\alpha_3\beta^2$ $\alpha_w\beta^2$

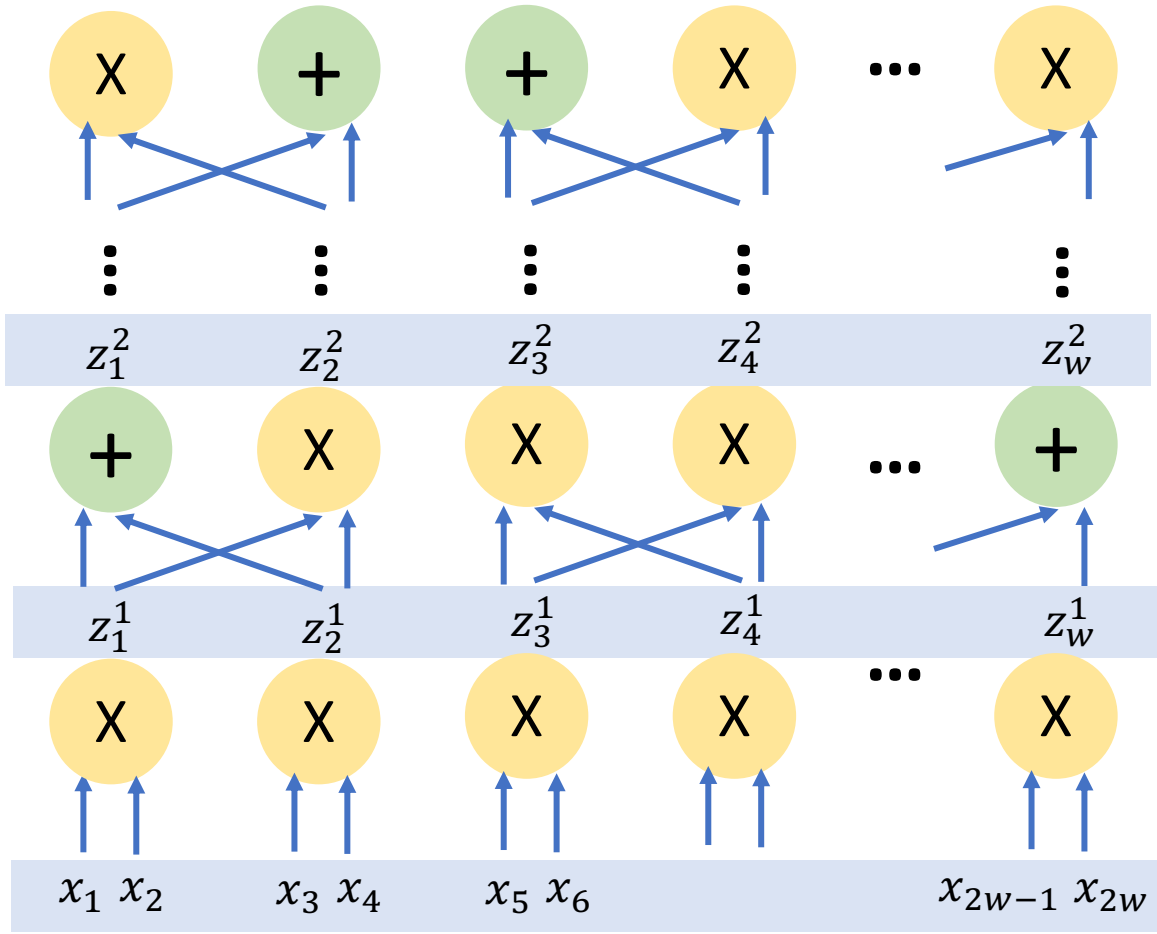
$$u_1 = u_0 + \alpha_1\beta^1 z_1^1 + \alpha_2\beta^1 z_2^1 + \cdots + \alpha_w\beta^1 z_w^1$$

β^2 $\alpha_1\beta^1$ $\alpha_2\beta^1$ $\alpha_3\beta^1$ $\alpha_w\beta^1$

$$u_0 = 0$$

β^1 α_1 α_2 α_3 α_w

Maliciously Secure Fluid MPC: Our Idea



β^3 $\alpha_1\beta^2$ $\alpha_2\beta^2$ $\alpha_3\beta^2$ $\alpha_w\beta^2$

Epoch 2

$$u_1 = u_0 + \alpha_1\beta^1 z_1^1 + \alpha_2\beta^1 z_2^1 + \cdots + \alpha_w\beta^1 z_w^1$$

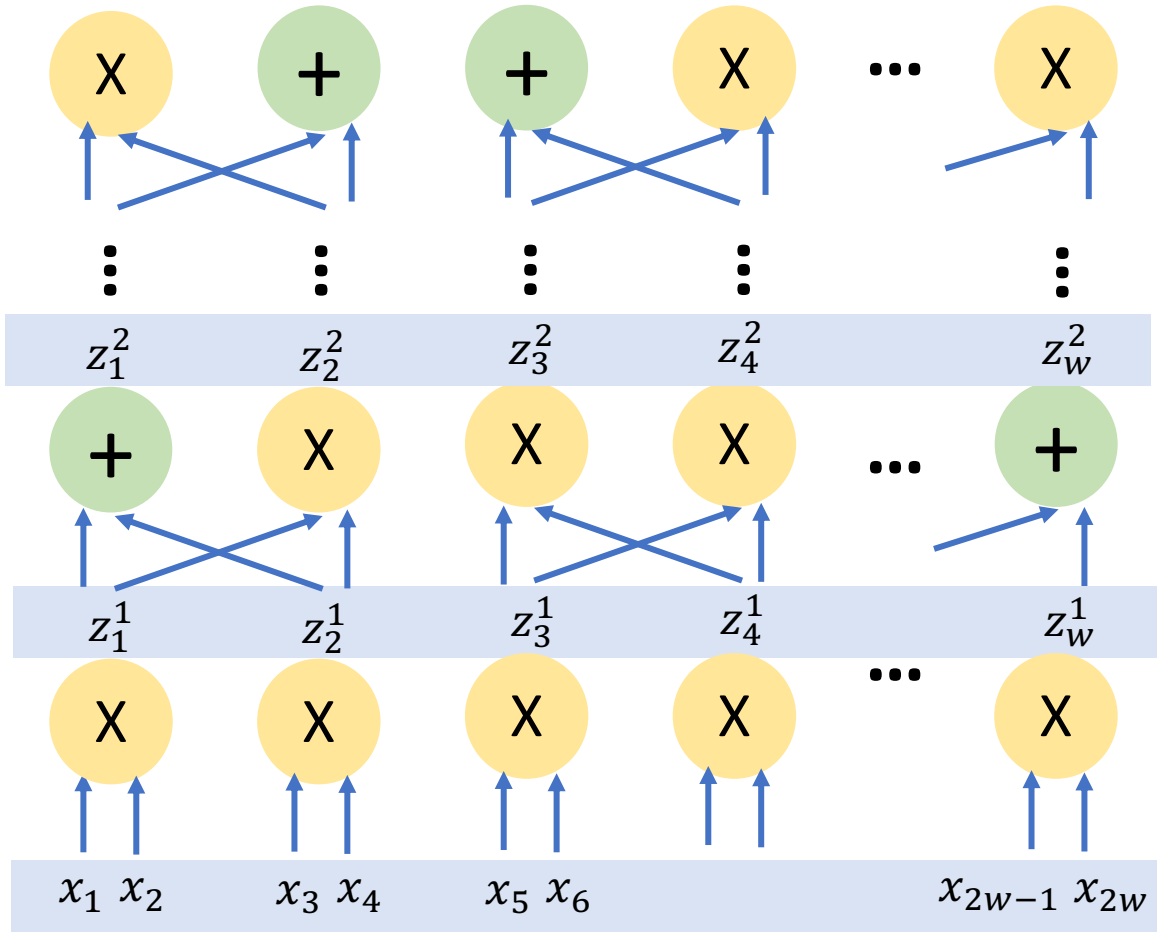
β^2 $\alpha_1\beta^1$ $\alpha_2\beta^1$ $\alpha_3\beta^1$ $\alpha_w\beta^1$

Epoch 1

$$u_0 = 0$$

β^1 α_1 α_2 α_3 α_w

Maliciously Secure Fluid MPC: Our Idea



- ☑ Division of Work
- ☑ Maximal Fluidity

β^3 $\alpha_1\beta^2$ $\alpha_2\beta^2$ $\alpha_3\beta^2$ $\alpha_w\beta^2$

Epoch 2

$$u_1 = u_0 + \alpha_1\beta^1 z_1^1 + \alpha_2\beta^1 z_2^1 + \cdots + \alpha_w\beta^1 z_w^1$$

β^2 $\alpha_1\beta^1$ $\alpha_2\beta^1$ $\alpha_3\beta^1$ $\alpha_w\beta^1$

Epoch 1

$$u_0 = 0$$

β^1 α_1 α_2 α_3 α_w

Summary

Fluid MPC: A formal model for MPC with dynamic participants.

Construct semi-honest and malicious Fluid MPC protocols that have maximum fluidity.

Provide an implementation of our protocol.

Thank You!