Perfectly-Secure Asynchronous MPC for General Adversaries

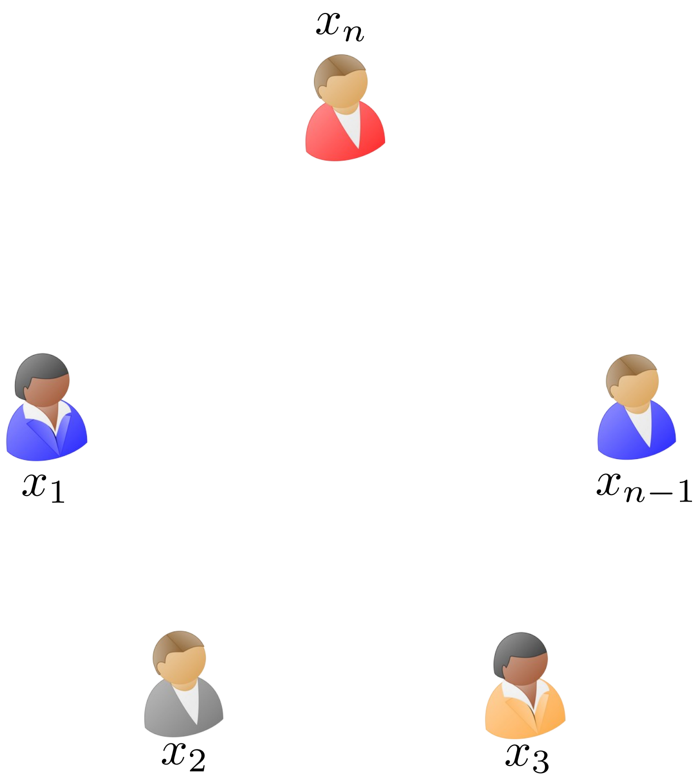
Ashish Choudhury, **Nikhil Pappu**

INDOCRYPT 2020

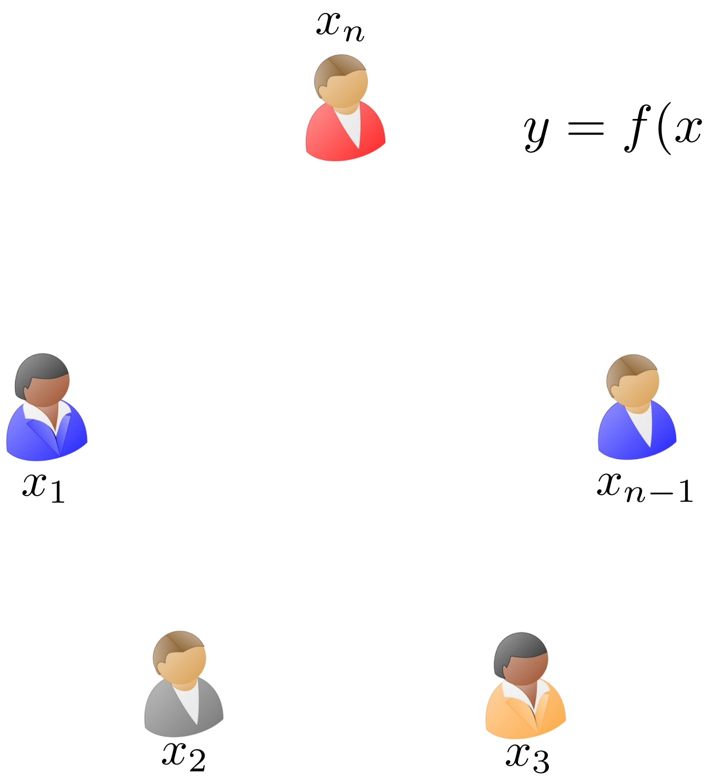
ज्ञानमुत्तमम्

Secure Multi-Party Computation (MPC)

Secure Multi-Party Computation (MPC)

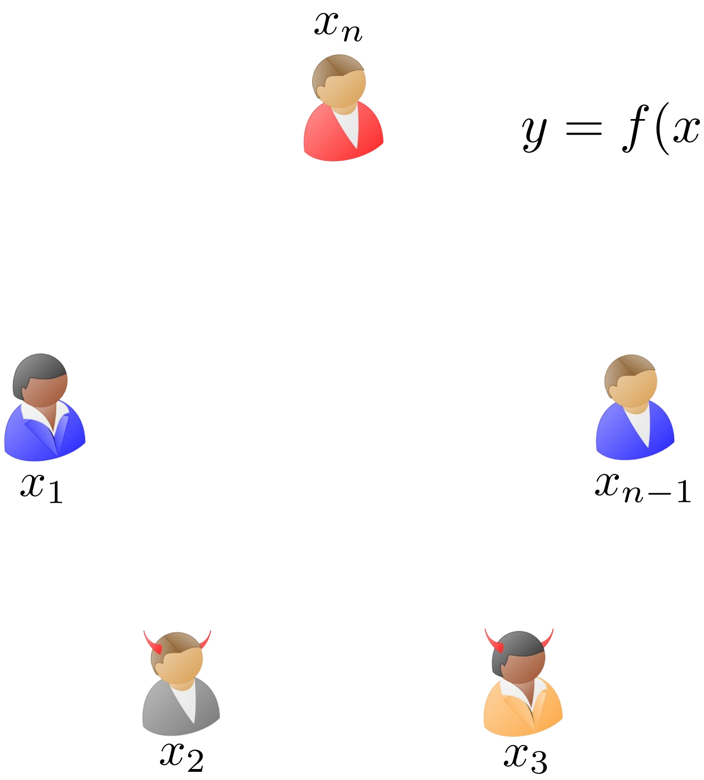


Secure Multi-Party Computation (MPC)



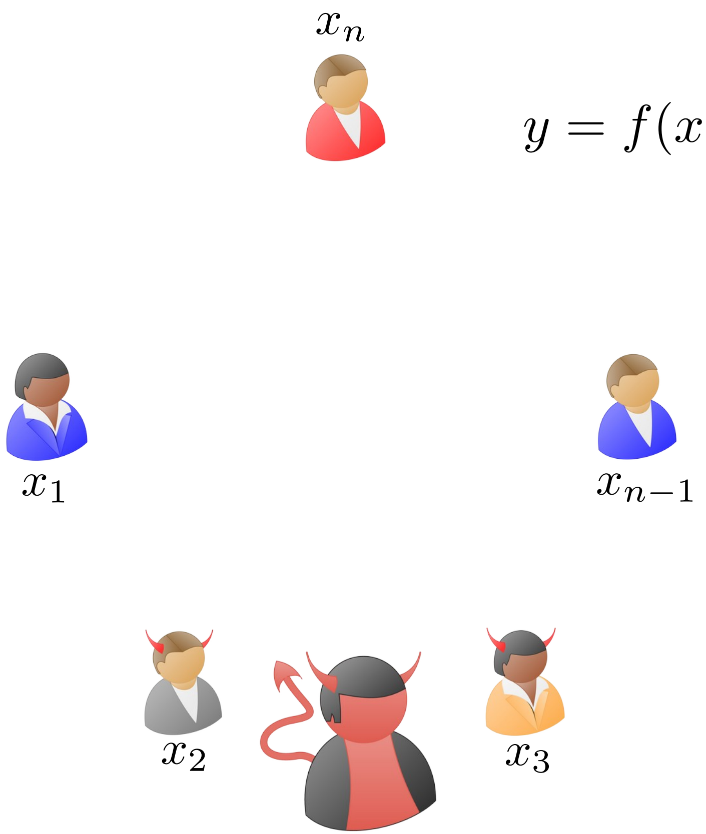
$$y = f(x_1, \ldots, x_n)$$

Secure Multi-Party Computation (MPC)



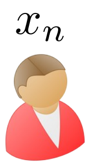
$$y = f(x_1, \ldots, x_n)$$

Secure Multi-Party Computation (MPC)



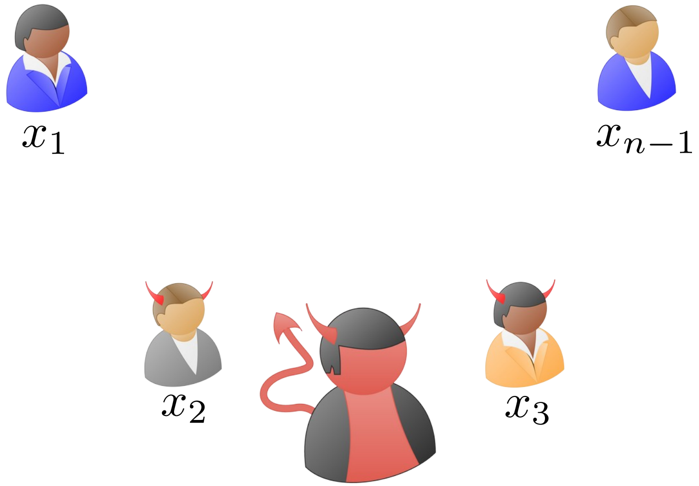
$$y = f(x_1, \ldots, x_n)$$

Secure Multi-Party Computation (MPC)

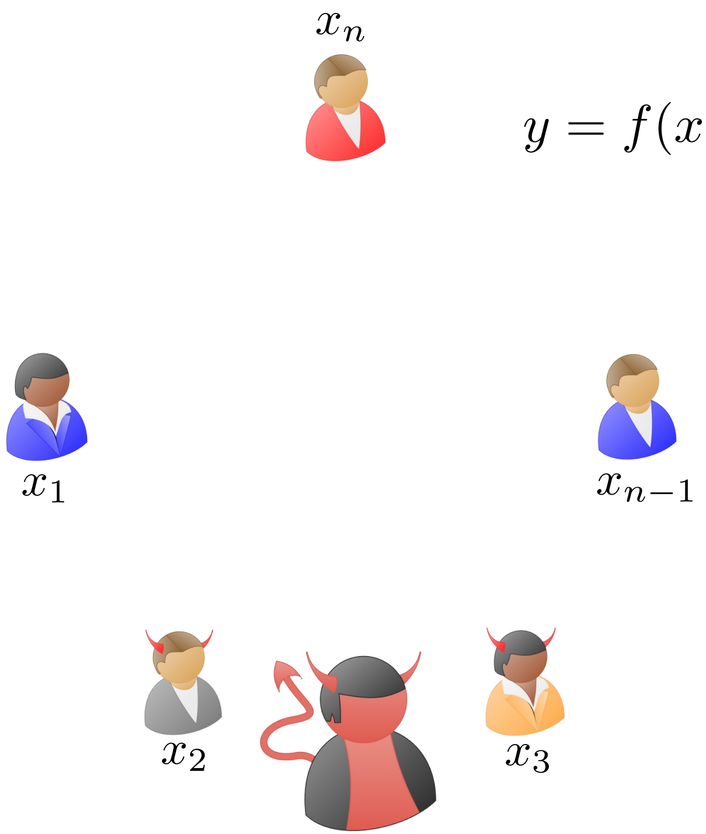


$$y = f(x_1, \ldots, x_n)$$

- Privacy



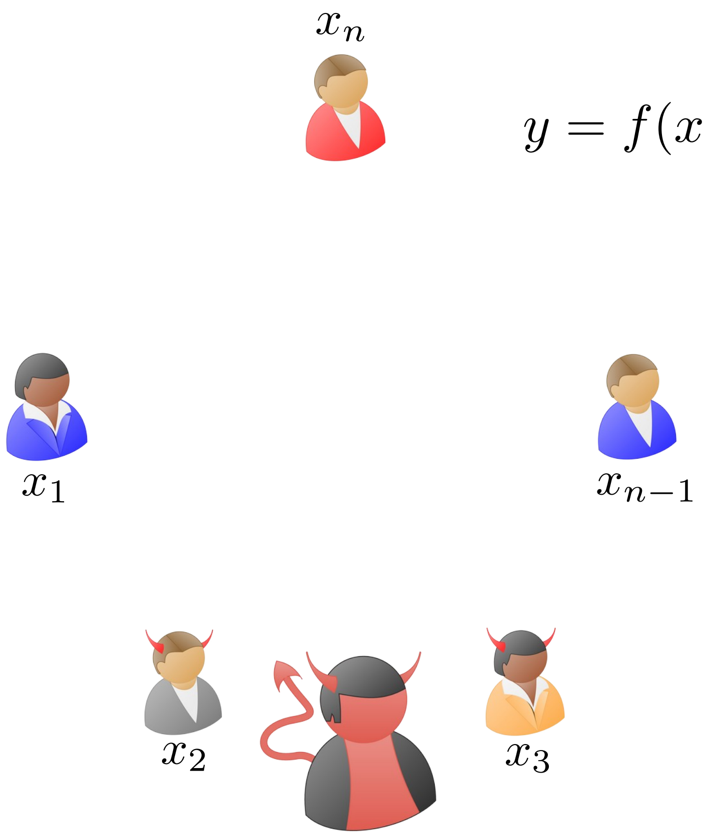
Secure Multi-Party Computation (MPC)



$$y = f(x_1, \ldots, x_n)$$

- Privacy
- Correctness

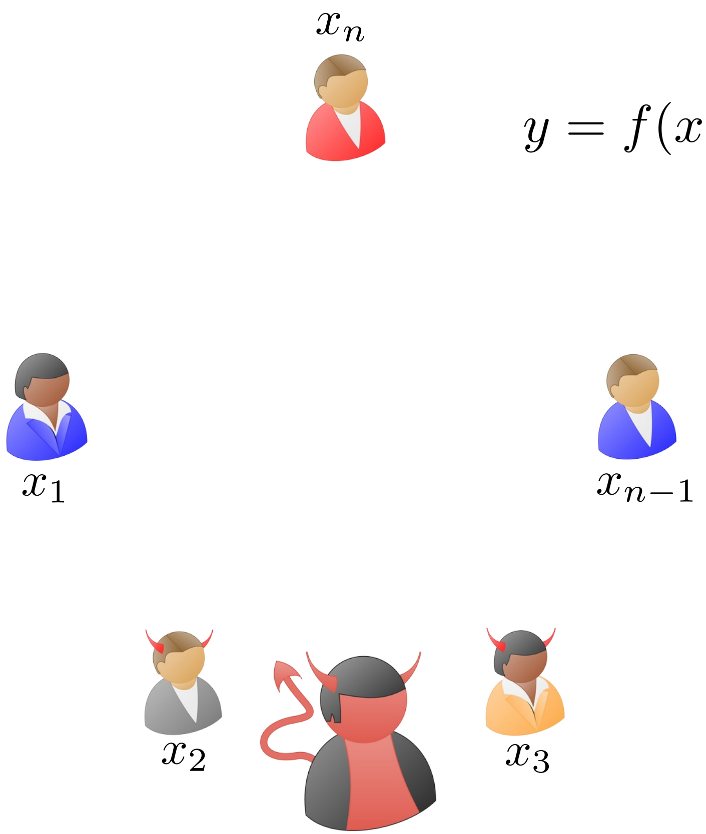
Secure Multi-Party Computation (MPC)



$$y = f(x_1, \ldots, x_n)$$

- Privacy
- Correctness
- Independence of Inputs

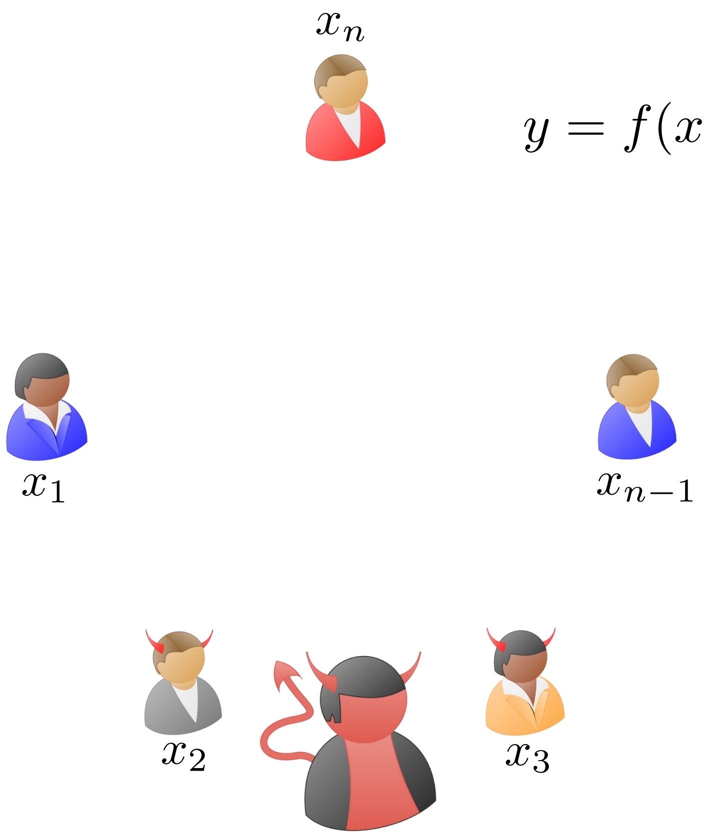
Secure Multi-Party Computation (MPC)



$$y = f(x_1, \ldots, x_n)$$

- Privacy
- Correctness
- Independence of Inputs
- Guaranteed Output Delivery

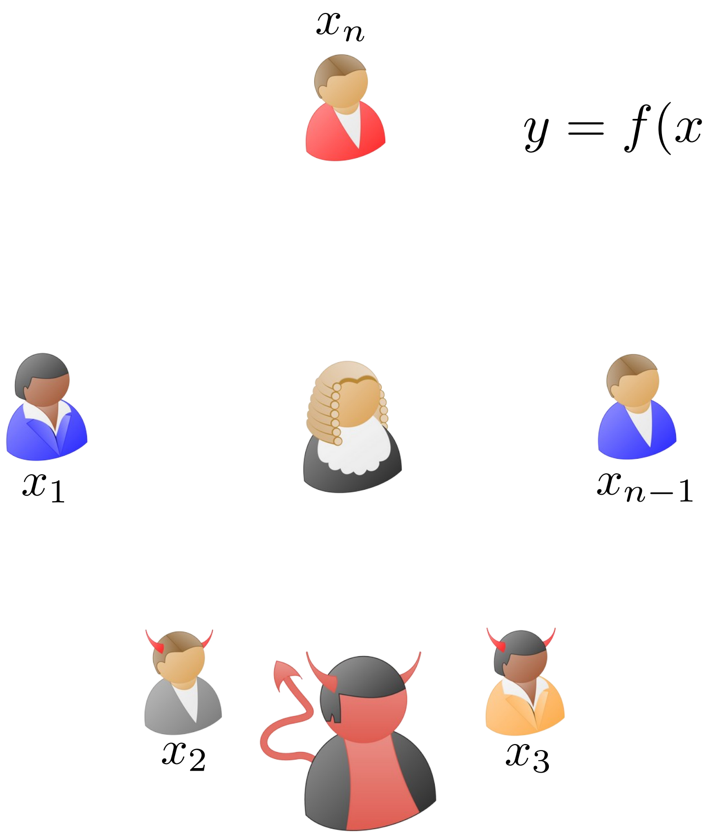
Secure Multi-Party Computation (MPC)



$$y = f(x_1, \ldots, x_n)$$

- Privacy
- Correctness
- Independence of Inputs
- Guaranteed Output Delivery
- ...

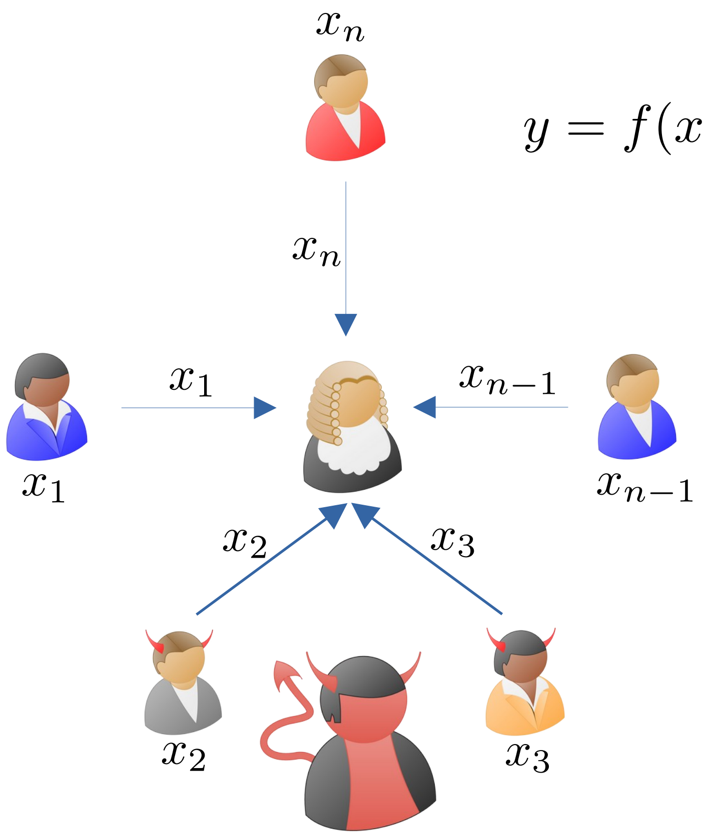
Secure Multi-Party Computation (MPC)



$$y = f(x_1, \ldots, x_n)$$

- Privacy
- Correctness
- Independence of Inputs
- Guaranteed Output Delivery
- ...

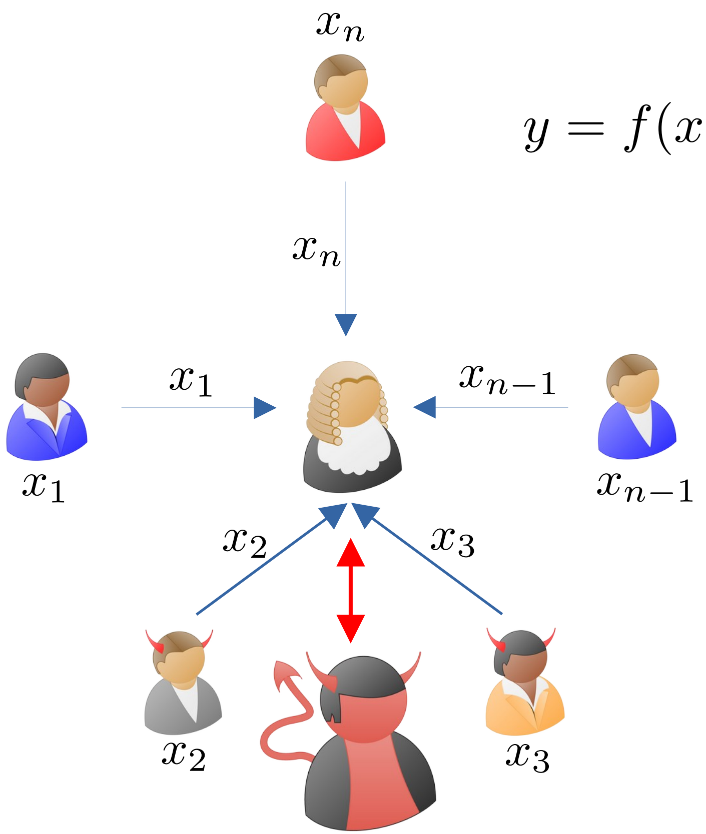
Secure Multi-Party Computation (MPC)



$$y = f(x_1, \ldots, x_n)$$

- Privacy
- Correctness
- Independence of Inputs
- Guaranteed Output Delivery
- ...

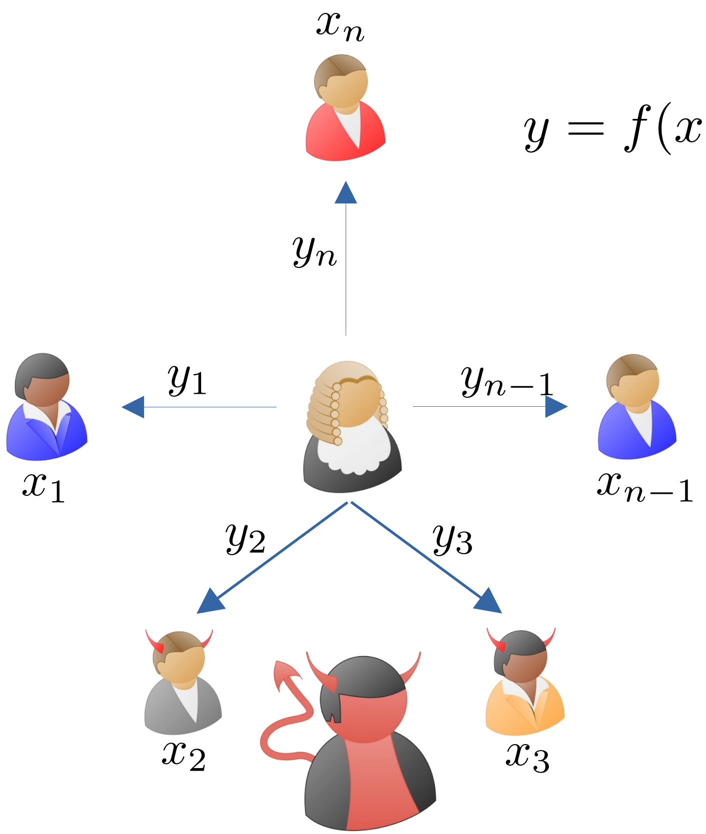
Secure Multi-Party Computation (MPC)



$$y = f(x_1, \ldots, x_n)$$

- Privacy
- Correctness
- Independence of Inputs
- Guaranteed Output Delivery
- ...

Secure Multi-Party Computation (MPC)



$$y = f(x_1, \ldots, x_n)$$

- Privacy
- Correctness
- Independence of Inputs
- Guaranteed Output Delivery
- ...

Communication Models

Communication Models

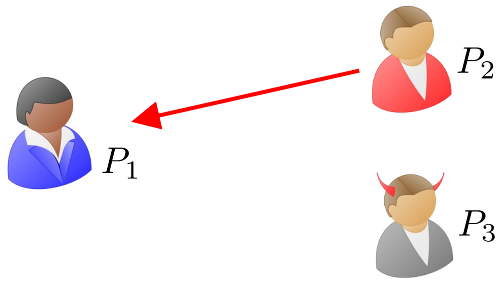
Synchronous Model

Communication Models

Synchronous Model

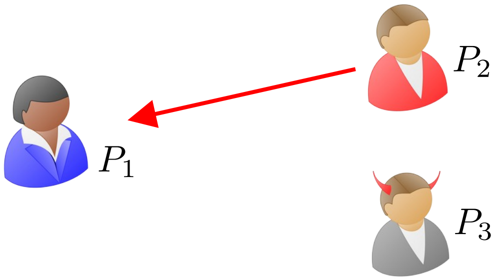
Communication Models

Synchronous Model



Communication Models

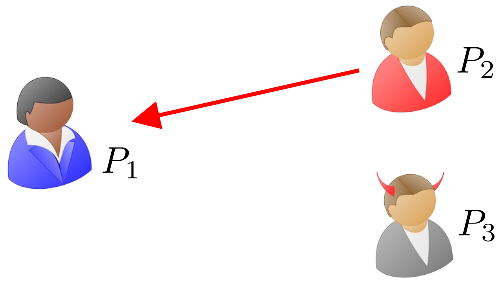
Synchronous Model



- Message Delays $< \Delta$

Communication Models

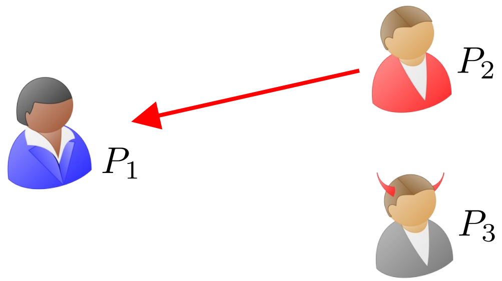
Synchronous Model



- Message Delays $< \Delta$
- Synchronized Clocks

Communication Models

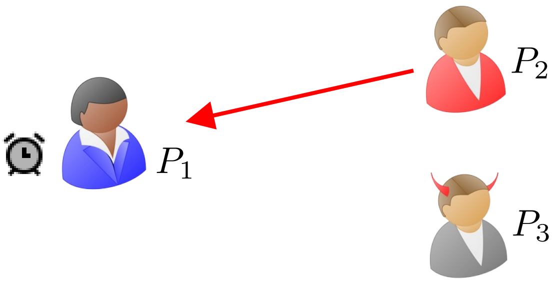
Synchronous Model



- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

Communication Models

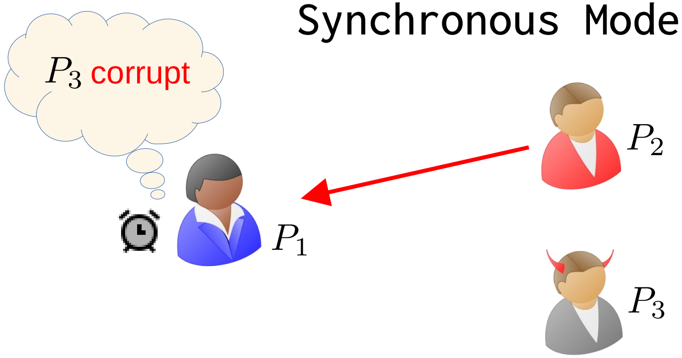
Synchronous Model



- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

Communication Models

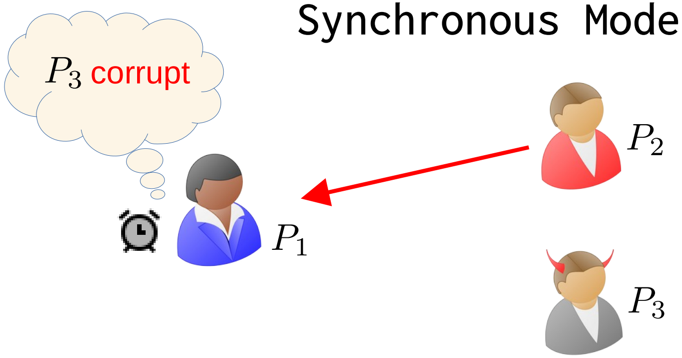
Synchronous Model



- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

Communication Models

Synchronous Model

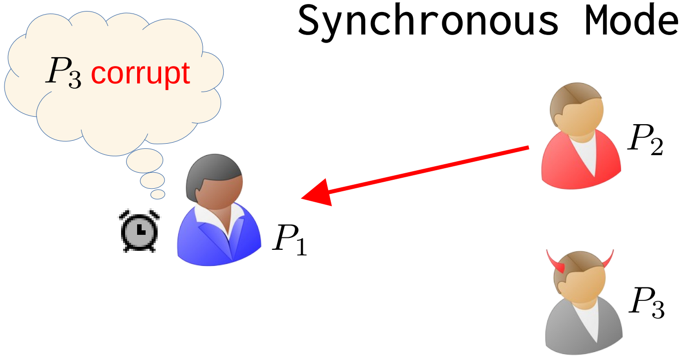


- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

Asynchronous Model [BCG93]

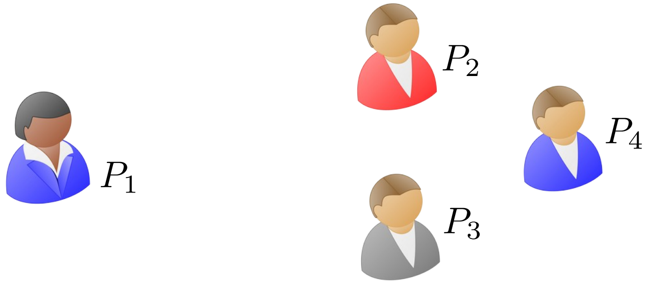
Communication Models

Synchronous Model



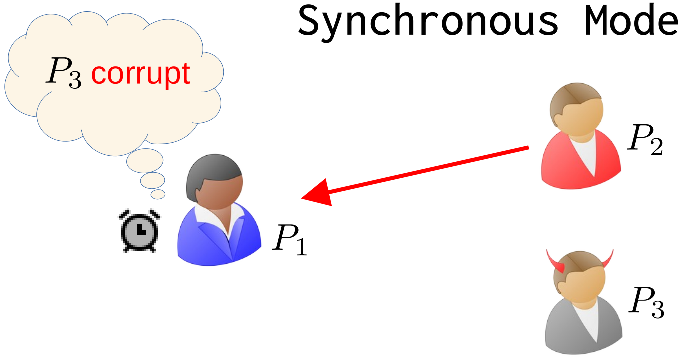
- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

Asynchronous Model [BCG93]

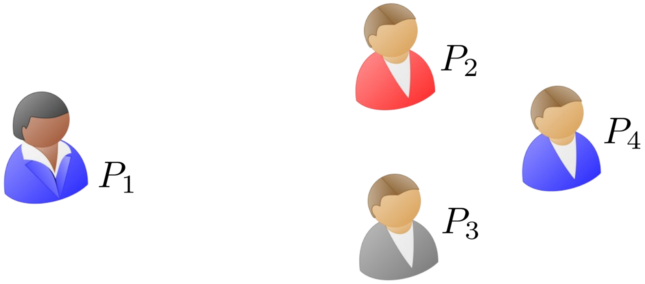


Communication Models

Synchronous Model



Asynchronous Model [BCG93]

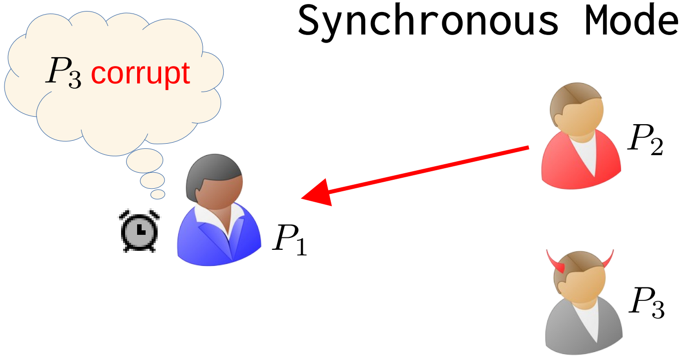


Unbounded
(finite) Delays

- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

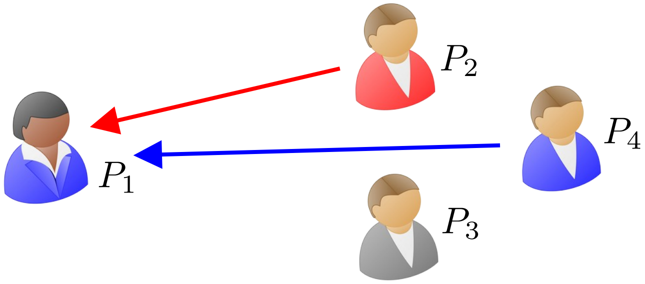
Communication Models

Synchronous Model



- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

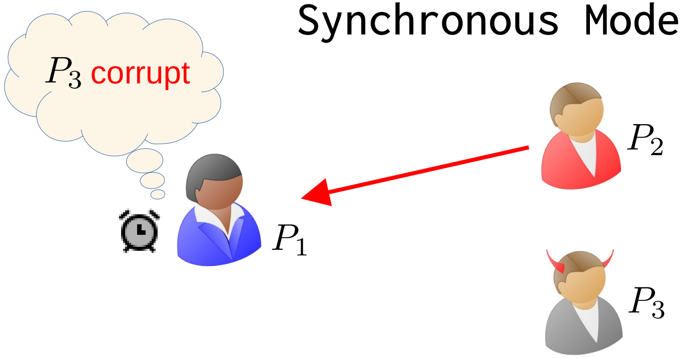
Asynchronous Model [BCG93]



Unbounded
(finite) Delays

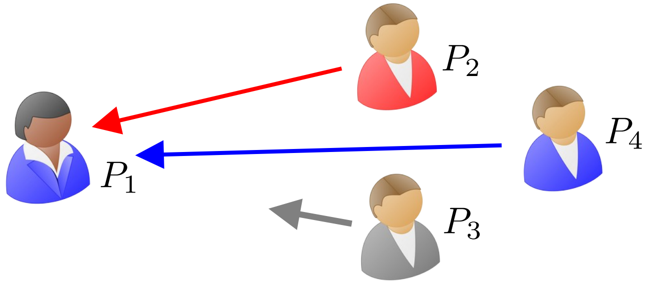
Communication Models

Synchronous Model



- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

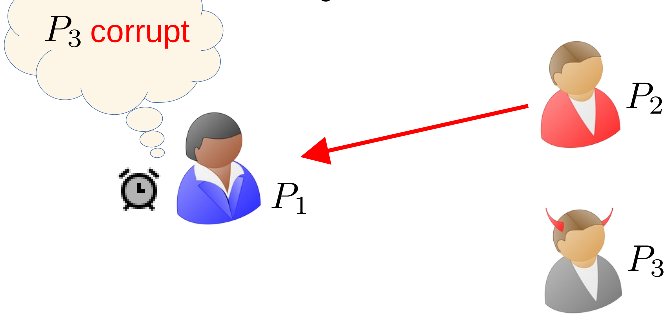
Asynchronous Model [BCG93]



Unbounded (finite) Delays

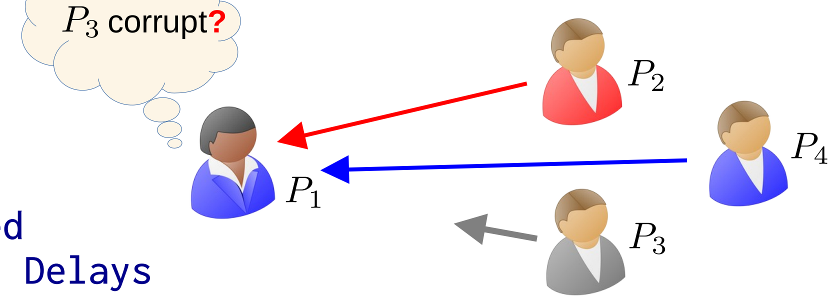
Communication Models

Synchronous Model



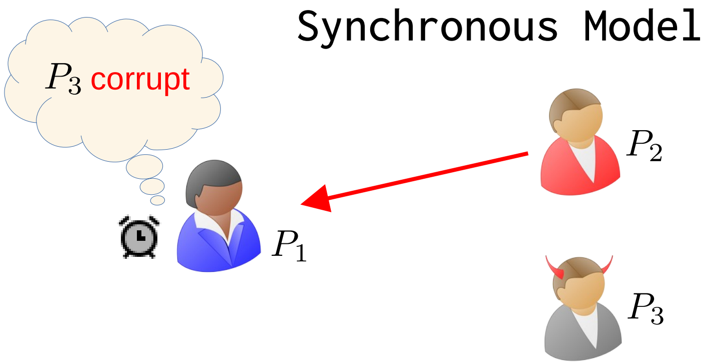
- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

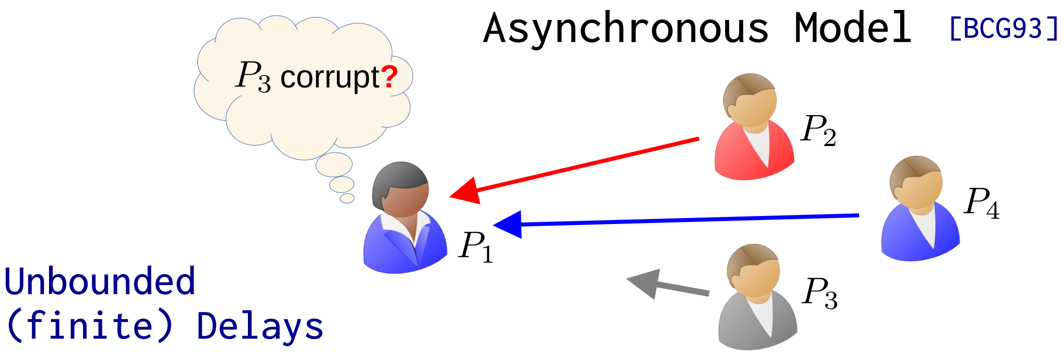
Asynchronous Model [BCG93]



Unbounded (finite) Delays

Communication Models



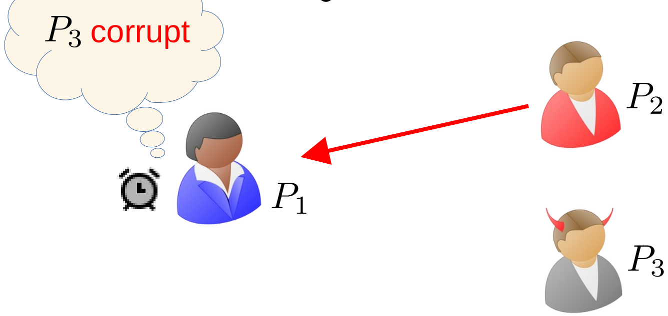


- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

- No Input Provision

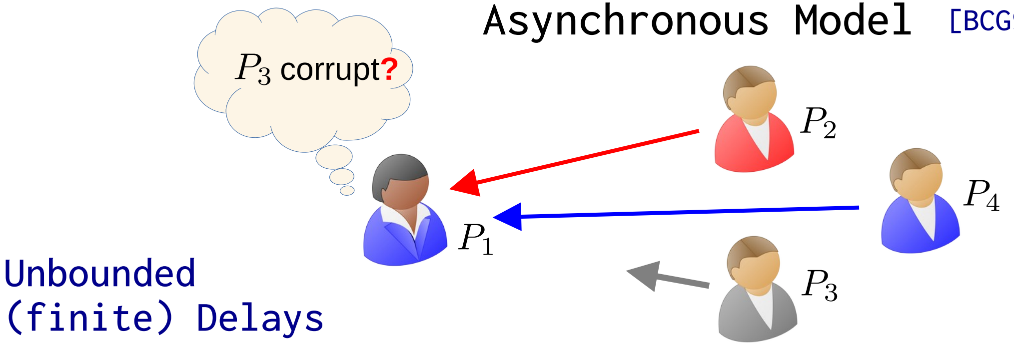
Communication Models

Synchronous Model



- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

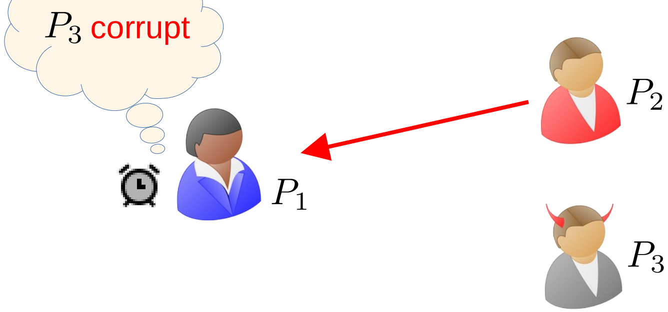
Asynchronous Model [BCG93]



- No Input Provision $f(x_1, x_2, \cdot, x_4)$

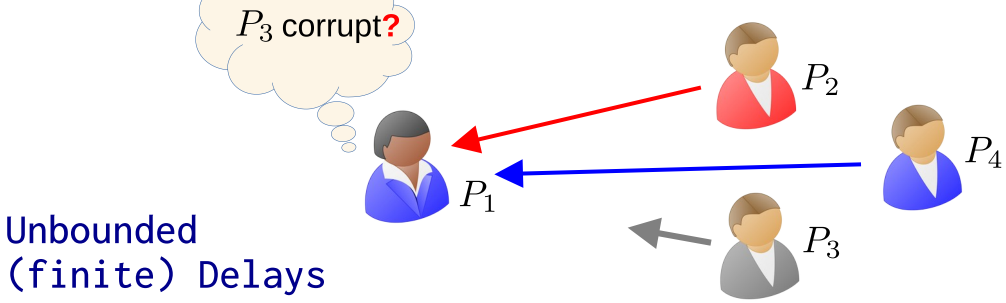
Communication Models

Synchronous Model



- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

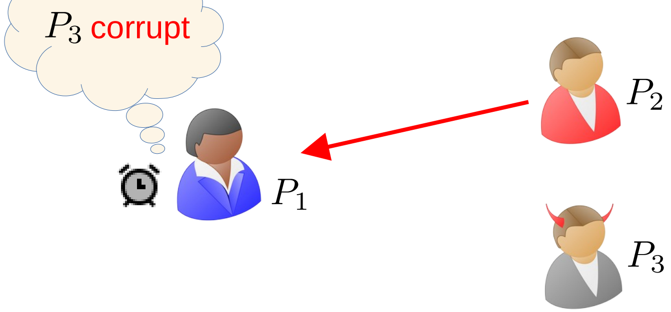
Asynchronous Model [BCG93]



- No Input Provision $f(x_1, x_2, \cdot, x_4)$
- Worse Resilience

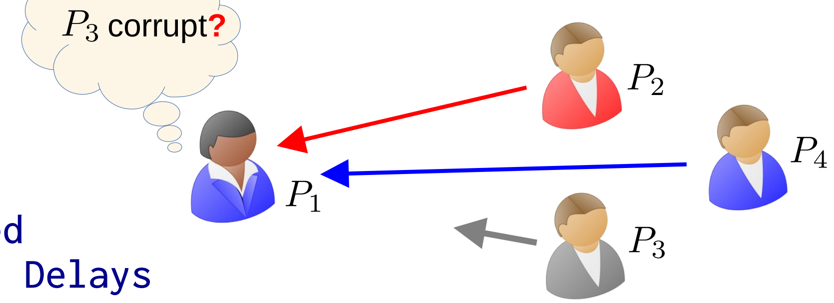
Communication Models

Synchronous Model



- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

Asynchronous Model [BCG93]

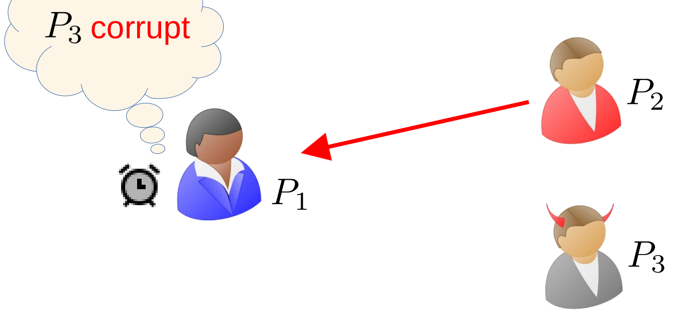


Unbounded (finite) Delays

- No Input Provision $f(x_1, x_2, \cdot, x_4)$
- Worse Resilience
- Worse Communication and Computation (Known Protocols)

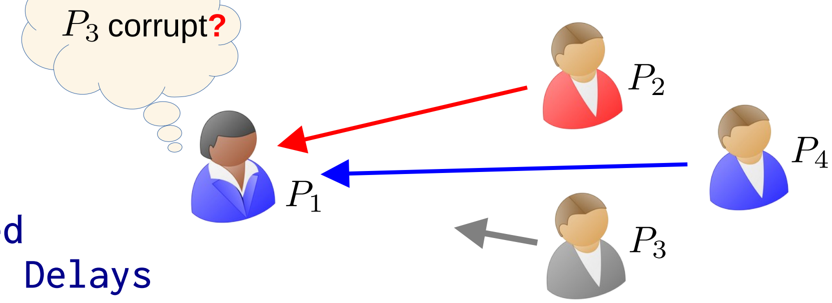
Communication Models

Synchronous Model



- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

Asynchronous Model [BCG93]

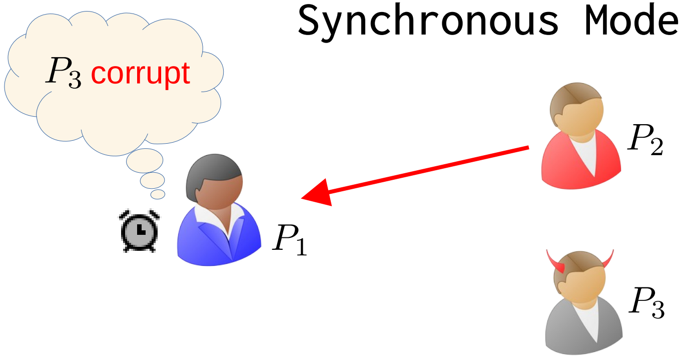


Unbounded
(finite) Delays

- No Input Provision $f(x_1, x_2, \cdot, x_4)$
- Worse Resilience
- Worse Communication and Computation (Known Protocols)
- Real-World Networks

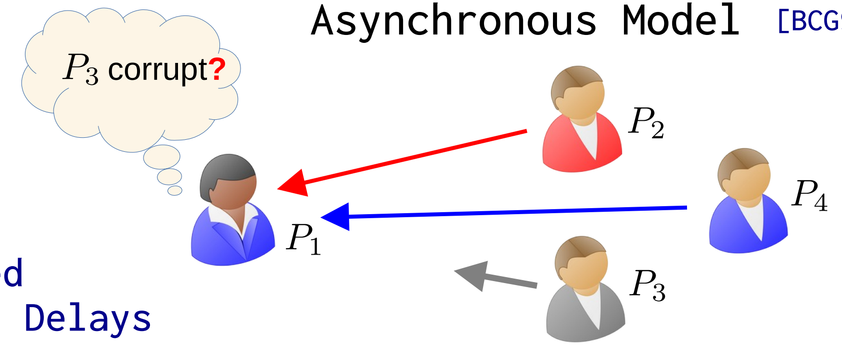
Communication Models

Synchronous Model



- Message Delays $< \Delta$
- Synchronized Clocks
- Computation in Rounds

Asynchronous Model [BCG93]



Unbounded (finite) Delays

- No Input Provision $f(x_1, x_2, \cdot, x_4)$
- Worse Resilience
- Worse Communication and Computation (Known Protocols)
- Real-World Networks 
- Responsiveness 

General Adversaries

General Adversaries

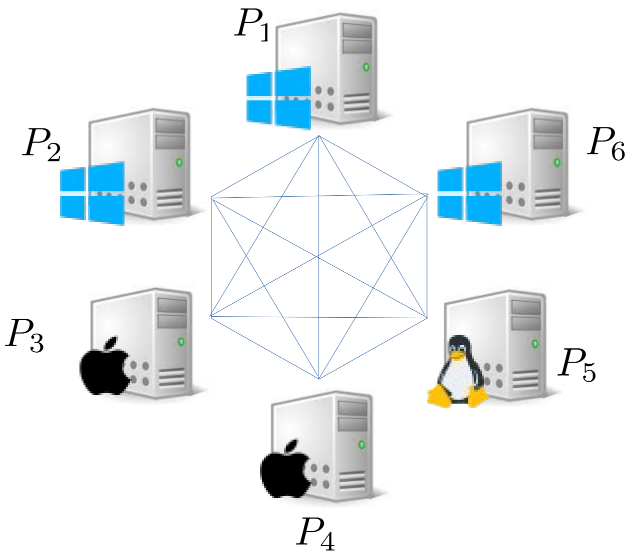
Most MPC protocols: $t < \frac{n}{k}$

General Adversaries

Most MPC protocols: $t < \frac{n}{k}$ Can be limiting...

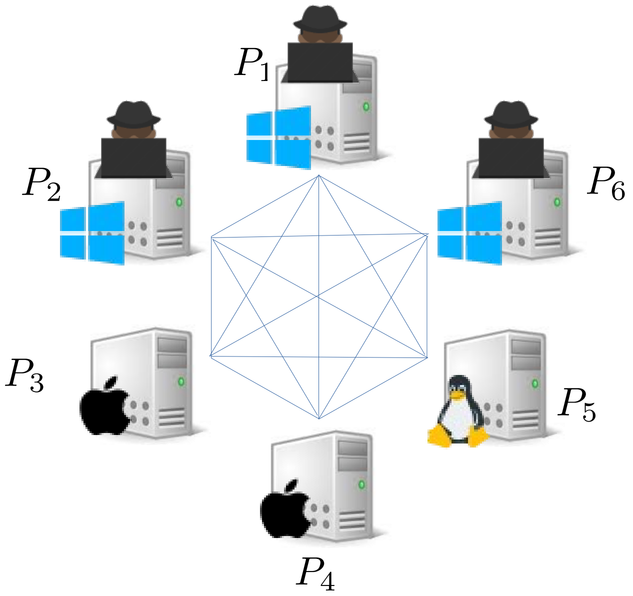
General Adversaries

Most MPC protocols: $t < \frac{n}{k}$ Can be limiting...



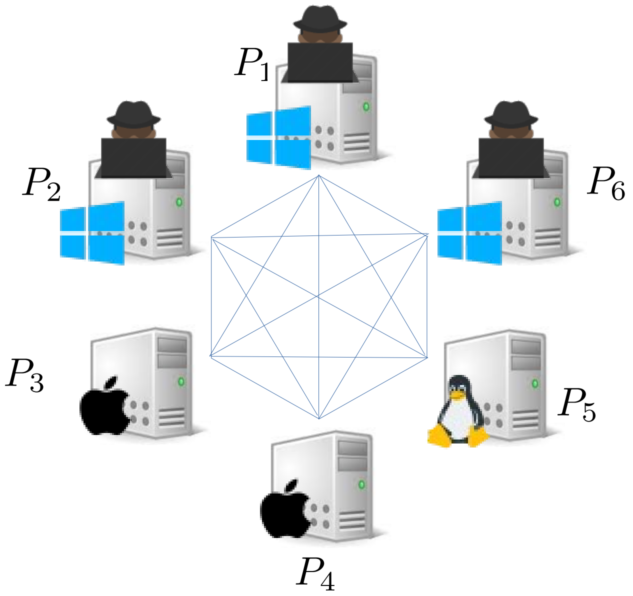
General Adversaries

Most MPC protocols: $t < \frac{n}{k}$ Can be limiting...



General Adversaries

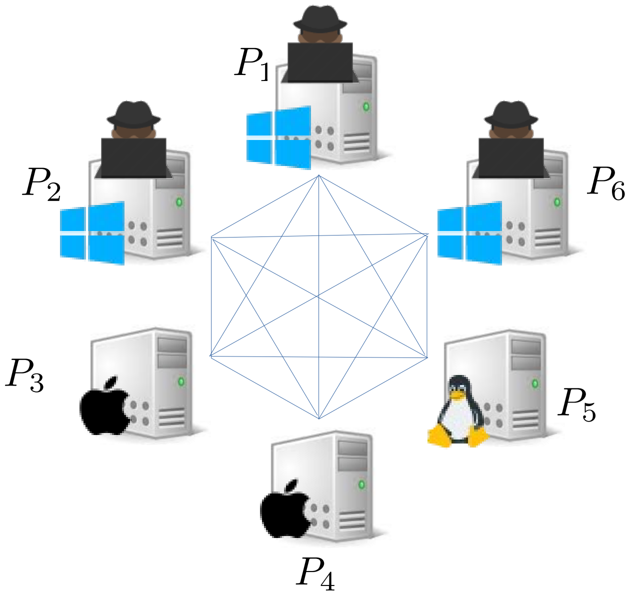
Most MPC protocols: $t < \frac{n}{k}$ Can be limiting...



- Computational-Security

General Adversaries

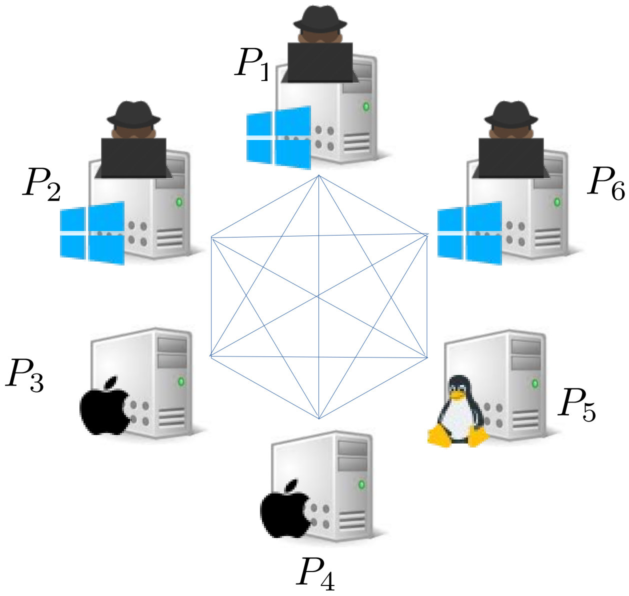
Most MPC protocols: $t < \frac{n}{k}$ Can be limiting...



- Computational-Security
- Guaranteed Output Delivery

General Adversaries

Most MPC protocols: $t < \frac{n}{k}$ Can be limiting...

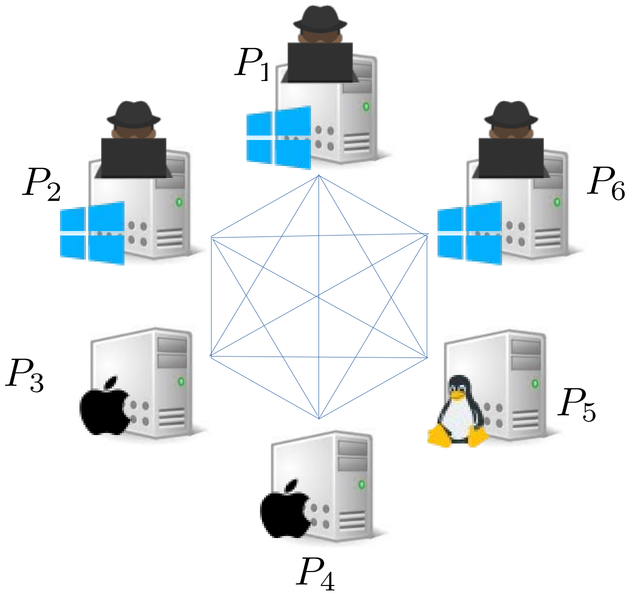


- Computational-Security
- Guaranteed Output Delivery

$$t < 6/2 \implies t \leq 2$$

General Adversaries

Most MPC protocols: $t < \frac{n}{k}$ Can be limiting...



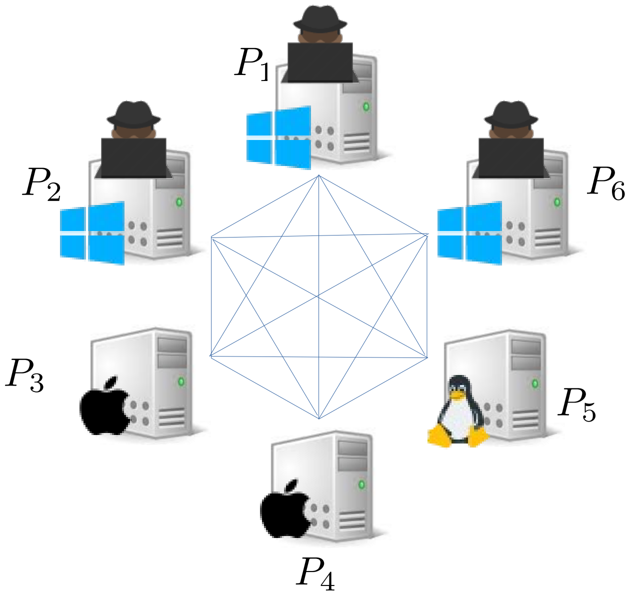
$$\mathcal{Z} = \{\{P_1, P_2, P_6\}, \{P_3, P_4\}, \{P_5\}\}$$ [HM97]

- Computational-Security
- Guaranteed Output Delivery

$$t < 6/2 \implies t \leq 2$$

General Adversaries

Most MPC protocols: $t < \frac{n}{k}$ Can be limiting...



$$\mathcal{Z} = \{\{P_1, P_2, P_6\}, \{P_3, P_4\}, \{P_5\}\}$$ [HM97]

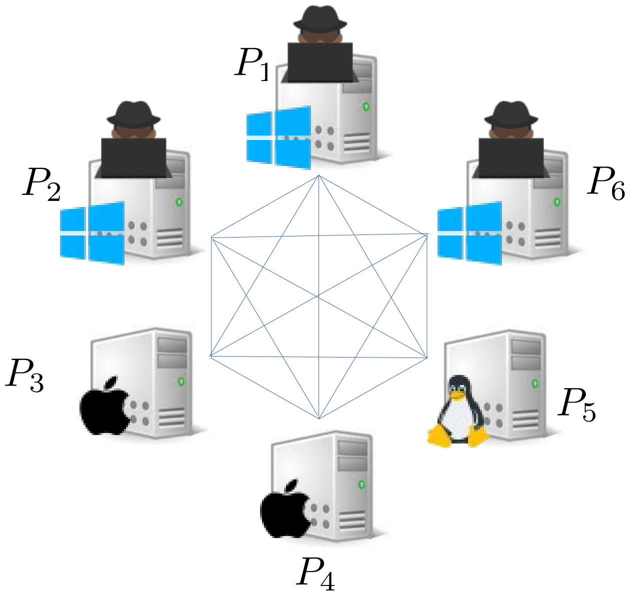
- monotone, maximal

- Computational-Security
- Guaranteed Output Delivery

$$t < 6/2 \implies t \leq 2$$

General Adversaries

Most MPC protocols: $t < \frac{n}{k}$ Can be limiting...



$$\mathcal{Z} = \{\{P_1, P_2, P_6\}, \{P_3, P_4\}, \{P_5\}\}$$ [HM97]

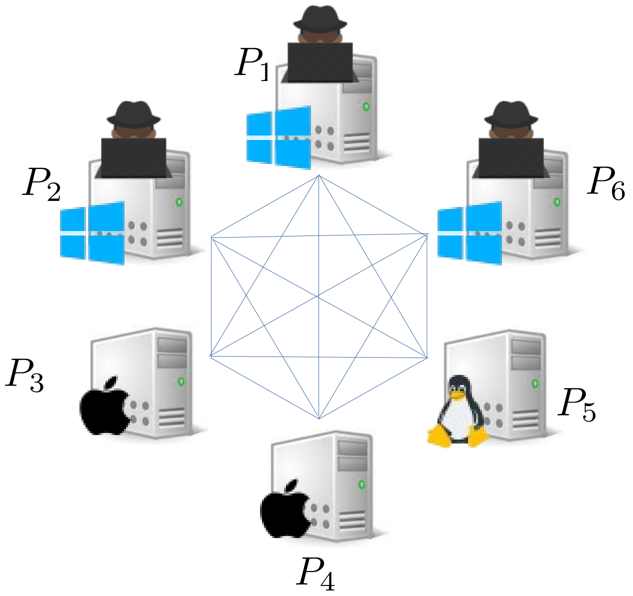
- monotone, maximal
- Size possibly exp in n

- Computational-Security
- Guaranteed Output Delivery

$t < 6/2 \implies t \leq 2$

General Adversaries

Most MPC protocols: $t < \frac{n}{k}$ Can be limiting...



$$\mathcal{Z} = \{\{P_1, P_2, P_6\}, \{P_3, P_4\}, \{P_5\}\}$$ [HM97]

- monotone, maximal
- Size possibly exp in n

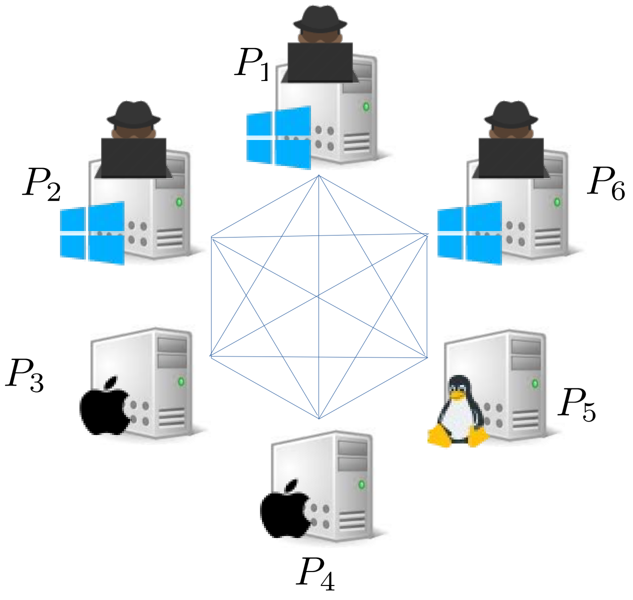
- Increased flexibility

- Computational-Security
- Guaranteed Output Delivery

$t < 6/2 \implies t \leq 2$

General Adversaries

Most MPC protocols: $t < \frac{n}{k}$ Can be limiting...



$$\mathcal{Z} = \{\{P_1, P_2, P_6\}, \{P_3, P_4\}, \{P_5\}\}$$ [HM97]

- monotone, maximal
- Size possibly exp in n

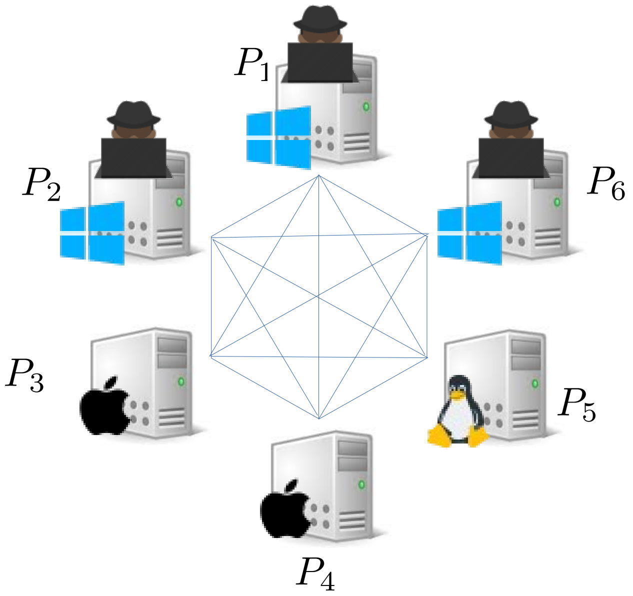
- Increased flexibility
- Communication Complexity $|\mathcal{Z}|^{\mathcal{O}(1)}$ (Known Protocols)

- Computational-Security
- Guaranteed Output Delivery

$t < 6/2 \implies t \leq 2$

General Adversaries

Most MPC protocols: $t < \frac{n}{k}$ Can be limiting...



$$\mathcal{Z} = \{\{P_1, P_2, P_6\}, \{P_3, P_4\}, \{P_5\}\}$$ [HM97]

- monotone, maximal
- Size possibly exp in n

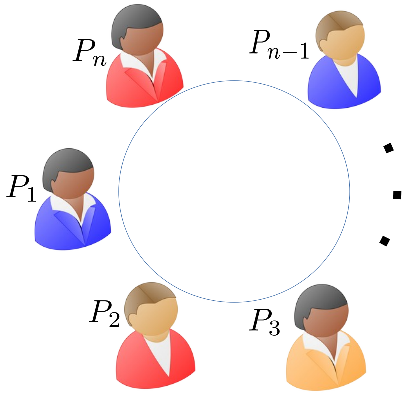
- Computational-Security
- Guaranteed Output Delivery

$$t < 6/2 \implies t \leq 2$$

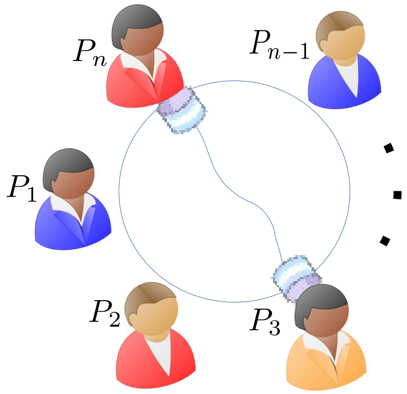
- Increased flexibility
- Communication Complexity $|\mathcal{Z}|^{\mathcal{O}(1)}$ (Known Protocols)
- Computational Complexity Lower Bound $\Omega(|\mathcal{Z}|)$ [HM00]

Setting

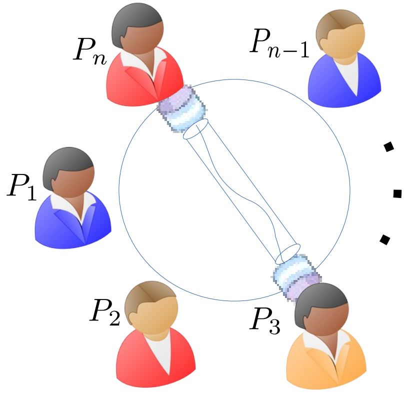
Setting



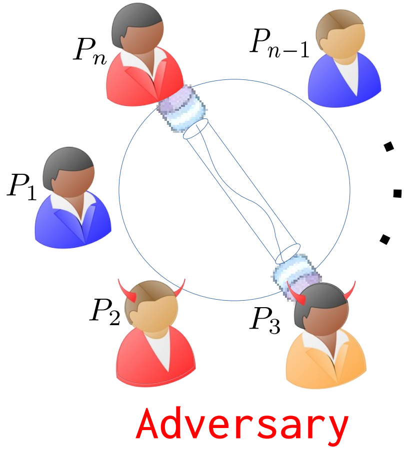
Setting



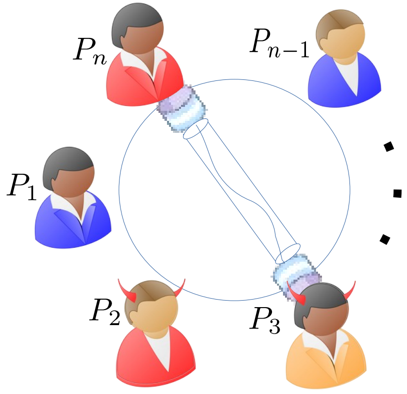
Setting



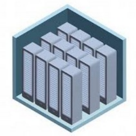
Setting



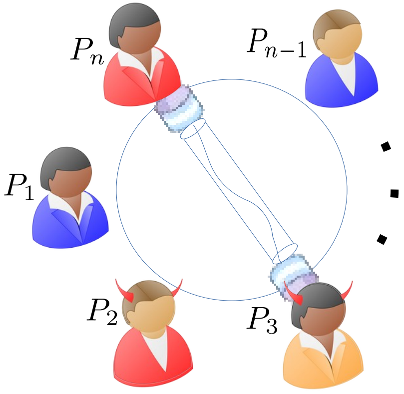
Setting



Adversary

- Computationally-Unbounded 

Setting

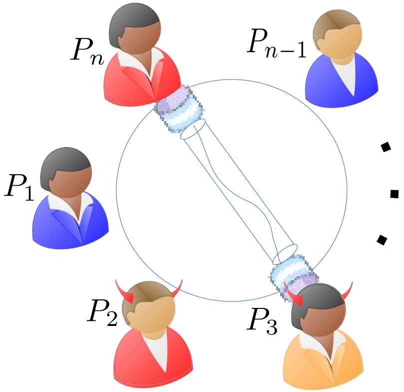


Adversary

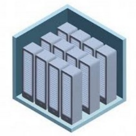
- Computationally-Unbounded 

  Perfect-Security 0%

Setting



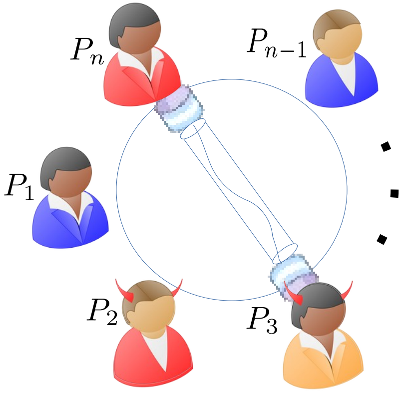
Adversary

- Computationally-Unbounded 

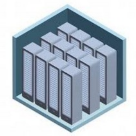
  Perfect-Security 0%

- Malicious (Byzantine)

Setting



Adversary

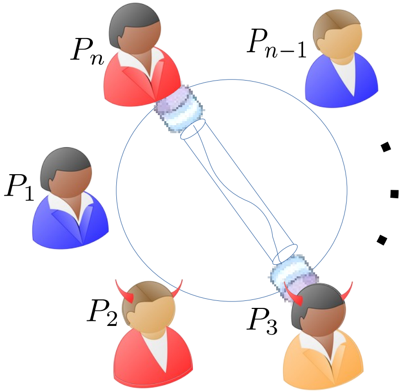
- Computationally-Unbounded 

  Perfect-Security 0% 

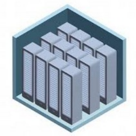
- Malicious (Byzantine)  

- Message Scheduler 

Setting



Adversary

- Computationally-Unbounded 

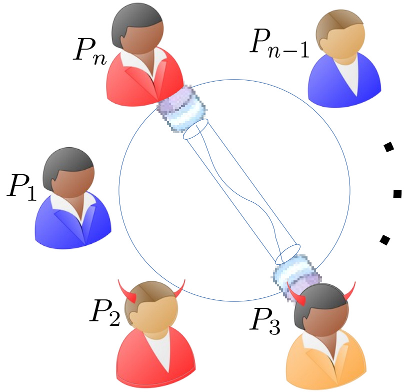
  Perfect-Security 0% 

- Malicious (Byzantine)  

- Message Scheduler 

Adversary Structure $\mathcal{Z} = \{\ldots, Z_i, \ldots\}$

Setting



Adversary

- Computationally-Unbounded 

  Perfect-Security 0% 

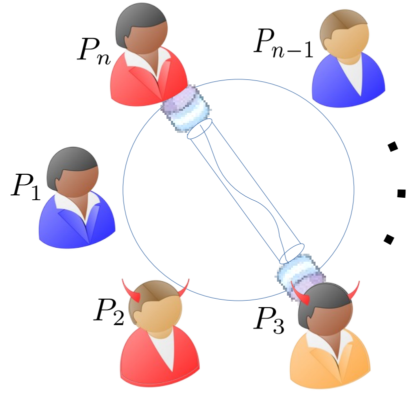
- Malicious (Byzantine)  

- Message Scheduler 

Adversary Structure $\mathcal{Z} = \{\ldots, Z_i, \ldots\}$

Requires $\mathcal{Q}^{(4)}$
[KSR02]

Setting



Adversary

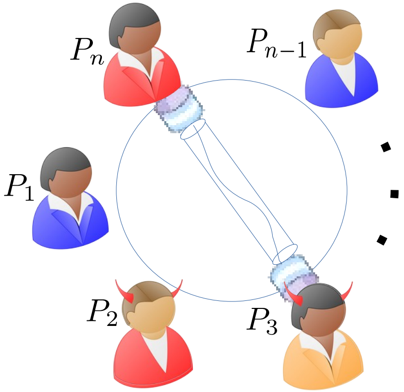
- Computationally-Unbounded
  Perfect-Security 0%
- Malicious (Byzantine)
- Message Scheduler

Adversary Structure $\mathcal{Z} = \{\ldots, Z_i, \ldots\}$

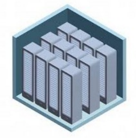
Requires $\mathcal{Q}^{(4)}$
[KSR02]

Partyset $\mathcal{P}$

Setting



Adversary

- Computationally-Unbounded 

  Perfect-Security 0% 

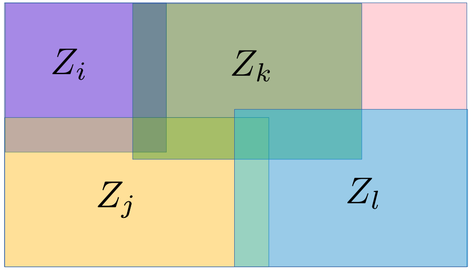
- Malicious (Byzantine)  

- Message Scheduler 

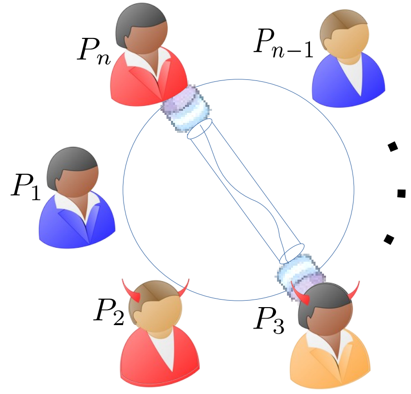
Adversary Structure $\mathcal{Z} = \{\ldots, Z_i, \ldots\}$

Requires $\mathcal{Q}^{(4)}$
[KSR02]

Partyset $\mathcal{P}$

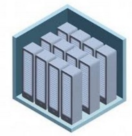


Setting



Adversary

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

- Computationally-Unbounded 

  Perfect-Security 0% ⚠

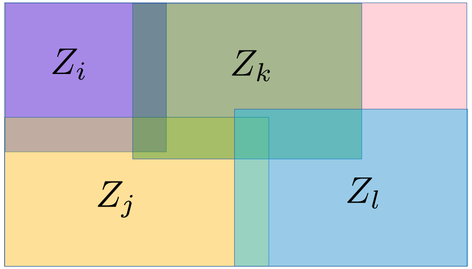
- Malicious (Byzantine)  

- Message Scheduler 

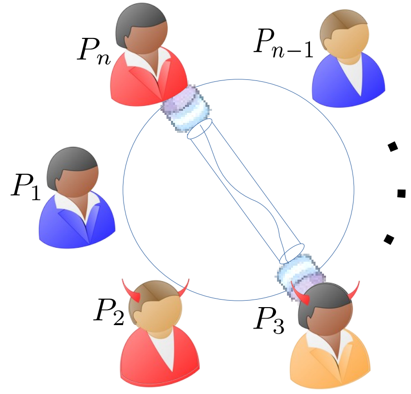
Adversary Structure $\mathcal{Z} = \{\ldots, Z_i, \ldots\}$

Requires $\mathcal{Q}^{(4)}$
[KSR02]

Partyset $\mathcal{P}$

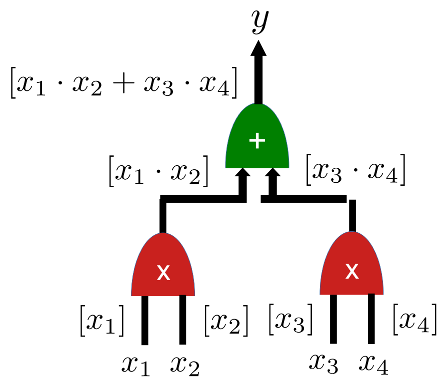


Setting



Adversary

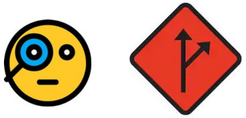
$f(x_1, x_2, x_3, x_4)$



Arithmetic Circuit over Field/Ring

- Computationally-Unbounded 

  Perfect-Security 0%

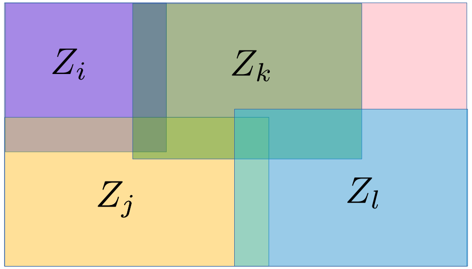
- Malicious (Byzantine) 

- Message Scheduler 

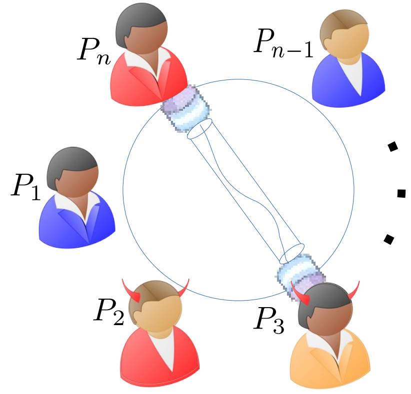
Adversary Structure $\mathcal{Z} = \{\ldots, Z_i, \ldots\}$

Requires $\mathcal{Q}^{(4)}$ [KSR02]

Partyset $\mathcal{P}$

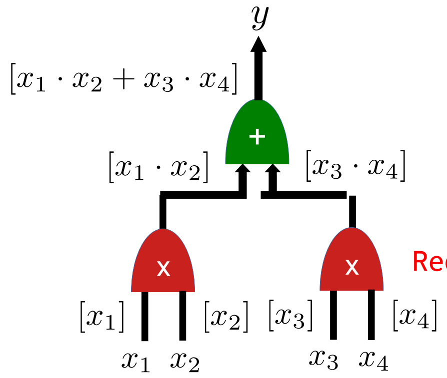


Setting



Adversary

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



Requires Interaction

Arithmetic Circuit over Field/Ring

- Computationally-Unbounded 

  Perfect-Security 0% 

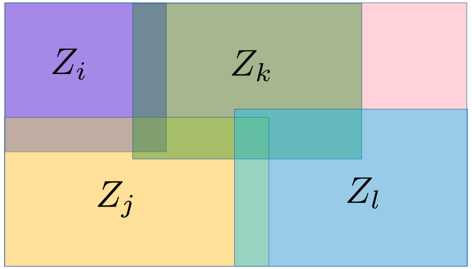
- Malicious (Byzantine)  

- Message Scheduler 

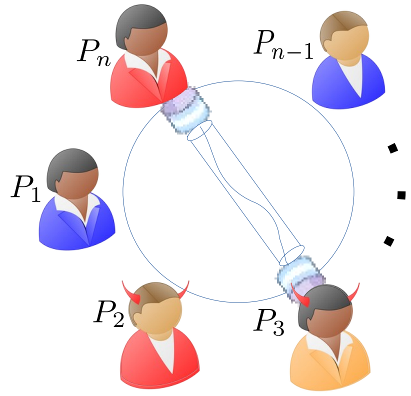
Adversary Structure $\mathcal{Z} = \{\ldots, Z_i, \ldots\}$

Requires $\mathcal{Q}^{(4)}$ [KSR02]

Partyset $\mathcal{P}$

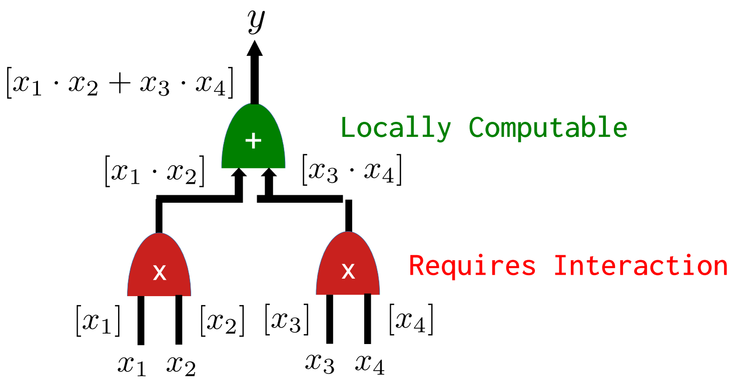


Setting



Adversary

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



Arithmetic Circuit over Field/Ring

- Computationally-Unbounded 

  Perfect-Security 0% 

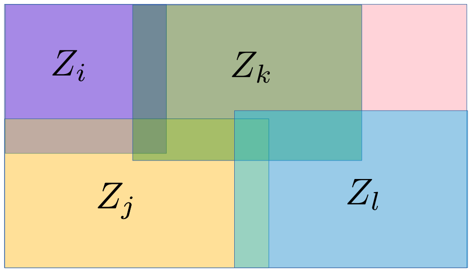
- Malicious (Byzantine)  

- Message Scheduler 

Adversary Structure $\mathcal{Z} = \{\ldots, Z_i, \ldots\}$

Requires $\mathcal{Q}^{(4)}$ [KSR02]

Partyset $\mathcal{P}$



Work on General Adversaries

Work on General Adversaries

Synchronous Model

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results

- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results

- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities

- [HT13, LO13]
  Improved Efficiency

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results
- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities
- [HT13, LO13]
  Improved Efficiency
- Others…

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results
- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities
- [HT13, LO13]
  Improved Efficiency
- Others…
  - Byzantine Agreement [FM98, AFM03]

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results
- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities
- [HT13, LO13]
  Improved Efficiency
- Others…
  - Byzantine Agreement [FM98, AFM03]
  - Mixed Model [BFH+08, HMZ08]

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results
- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities
- [HT13, LO13]
  Improved Efficiency
- Others…
  - Byzantine Agreement [FM98, AFM03]
  - Mixed Model [BFH+08, HMZ08]
  - Cryptographic Setting [KRS+18, SW19]

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results

- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities

- [HT13, LO13]
  Improved Efficiency

- Others…
  - Byzantine Agreement [FM98, AFM03]
  - Mixed Model [BFH+08, HMZ08]
  - Cryptographic Setting [KRS+18, SW19]

  etc...

Work on General Adversaries

Synchronous Model

Asynchronous Model

- [HM97, HM00]
  Feasibility Results

- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities

- [HT13, LO13]
  Improved Efficiency

- Others…
  - Byzantine Agreement [FM98, AFM03]
  - Mixed Model [BFH+08, HMZ08]
  - Cryptographic Setting [KRS+18, SW19]
    etc...

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results

- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities

- [HT13, LO13]
  Improved Efficiency

- Others…
  - Byzantine Agreement [FM98, AFM03]
  - Mixed Model [BFH+08, HMZ08]
  - Cryptographic Setting [KRS+18, SW19]

  etc...

Asynchronous Model

- [KSR02]

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results
- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities
- [HT13, LO13]
  Improved Efficiency
- Others…
  - Byzantine Agreement [FM98, AFM03]
  - Mixed Model [BFH+08, HMZ08]
  - Cryptographic Setting [KRS+18, SW19]
    etc...

Asynchronous Model

- [KSR02]
  - Perfect-Security Setting

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results
- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities
- [HT13, LO13]
  Improved Efficiency
- Others…
  - Byzantine Agreement [FM98, AFM03]
  - Mixed Model [BFH+08, HMZ08]
  - Cryptographic Setting [KRS+18, SW19]
    etc...

Asynchronous Model

- [KSR02]
  - Perfect-Security Setting
  - MSP-based AVSS Protocol

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results

- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities

- [HT13, LO13]
  Improved Efficiency

- Others…
  - Byzantine Agreement [FM98, AFM03]
  - Mixed Model [BFH+08, HMZ08]
  - Cryptographic Setting [KRS+18, SW19]
    etc...

Asynchronous Model

- [KSR02]
  - Perfect-Security Setting
  - MSP-based AVSS Protocol
  - AMPC Protocol ⚠️

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results
- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities
- [HT13, LO13]
  Improved Efficiency
- Others…
  - Byzantine Agreement [FM98, AFM03]
  - Mixed Model [BFH+08, HMZ08]
  - Cryptographic Setting [KRS+18, SW19]

  etc...

Asynchronous Model

- [KSR02]
  - Perfect-Security Setting
  - MSP-based AVSS Protocol
  - AMPC Protocol
- Our Work

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results
- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities
- [HT13, LO13]
  Improved Efficiency
- Others…
  - Byzantine Agreement [FM98, AFM03]
  - Mixed Model [BFH+08, HMZ08]
  - Cryptographic Setting [KRS+18, SW19]

  etc...

Asynchronous Model

- [KSR02]
  - Perfect-Security Setting
  - MSP-based AVSS Protocol
  - AMPC Protocol
- Our Work
  - Perfectly-Secure Additive SS-based ([Mau02]) AVSS Protocol

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results

- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities

- [HT13, LO13]
  Improved Efficiency

- Others…
  - Byzantine Agreement [FM98, AFM03]
  - Mixed Model [BFH+08, HMZ08]
  - Cryptographic Setting [KRS+18, SW19]
  etc...

Asynchronous Model

- [KSR02]
  - Perfect-Security Setting
  - MSP-based AVSS Protocol
  - AMPC Protocol ⚠

- Our Work
  - Perfectly-Secure Additive SS-based ([Mau02]) AVSS Protocol
  - Perfectly-Secure AMPC Protocol

Work on General Adversaries

Synchronous Model

- [HM97, HM00]
  Feasibility Results

- [CDD+99, CDM00, FHM99, Mau02, SS99]
  Polynomial (in $|\mathcal{Z}|$) complexities

- [HT13, LO13]
  Improved Efficiency

- Others…
  - Byzantine Agreement [FM98, AFM03]
  - Mixed Model [BFH+08, HMZ08]
  - Cryptographic Setting [KRS+18, SW19]

  etc...

Asynchronous Model

- [KSR02]
  - Perfect-Security Setting
  - MSP-based AVSS Protocol
  - AMPC Protocol

- Our Work
  - Perfectly-Secure Additive SS-based ([Mau02]) AVSS Protocol
  - Perfectly-Secure AMPC Protocol
  - ABA Protocol (Generalization of [CR93])

Flaw in [KSR02]

Flaw in [KSR02]

Player Elimination Framework [HMP00]

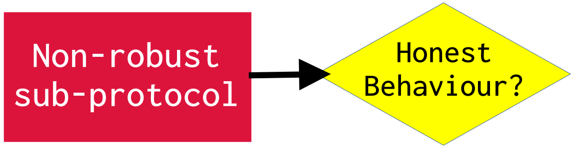
Flaw in [KSR02]

Player Elimination Framework [HMP00]

Non-robust sub-protocol

Flaw in [KSR02]

Player Elimination Framework [HMP00]

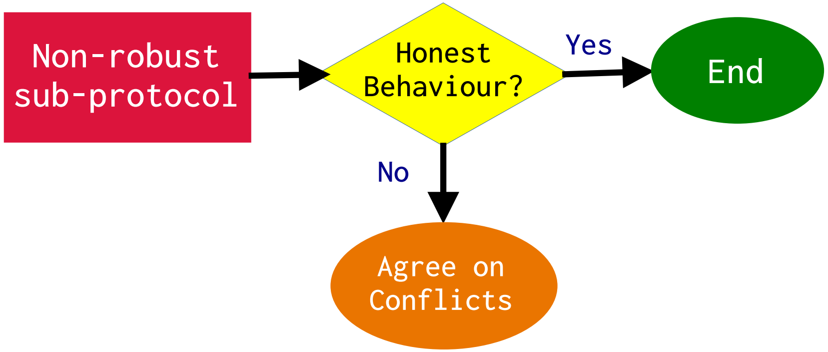


Flaw in [KSR02]

Player Elimination Framework [HMP00]

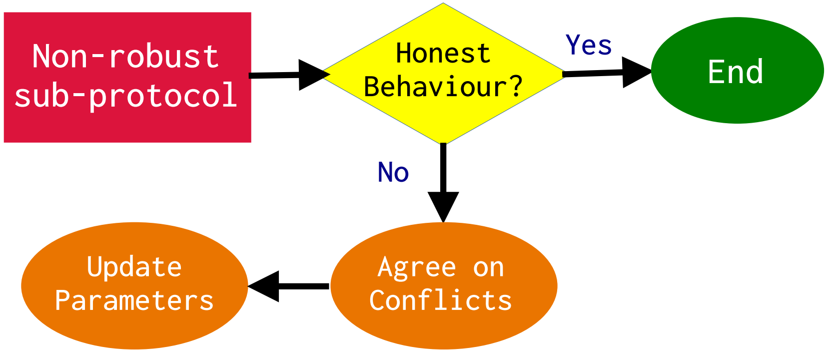
Flaw in [KSR02]

Player Elimination Framework [HMP00]



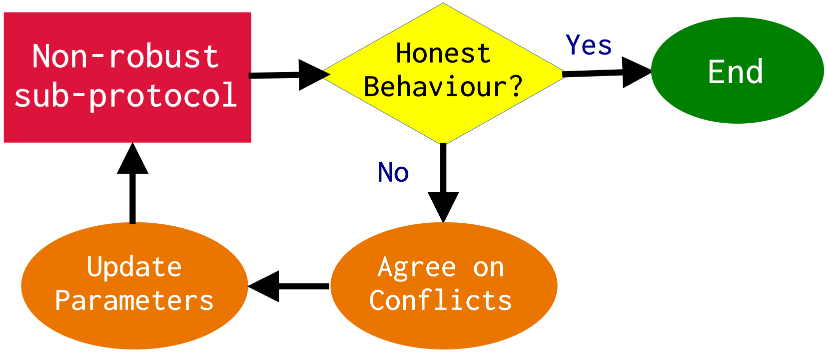
Flaw in [KSR02]

Player Elimination Framework [HMP00]



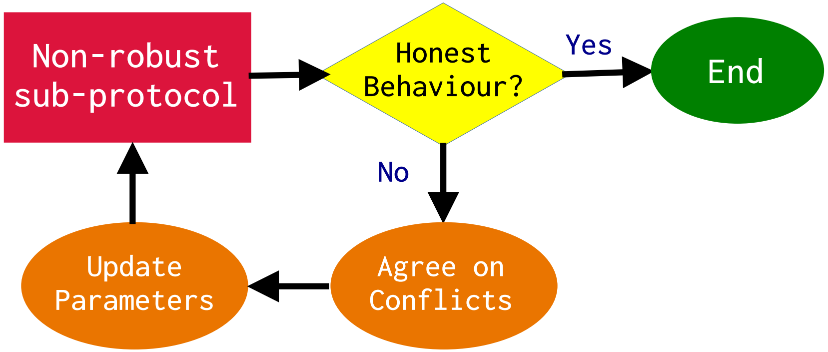
Flaw in [KSR02]

Player Elimination Framework [HMP00]



Flaw in [KSR02]

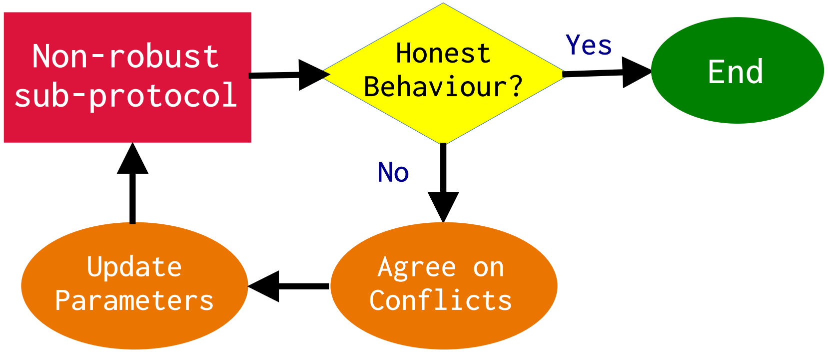
Player Elimination Framework [HMP00]



Example Execution

Flaw in [KSR02]

Player Elimination Framework [HMP00]

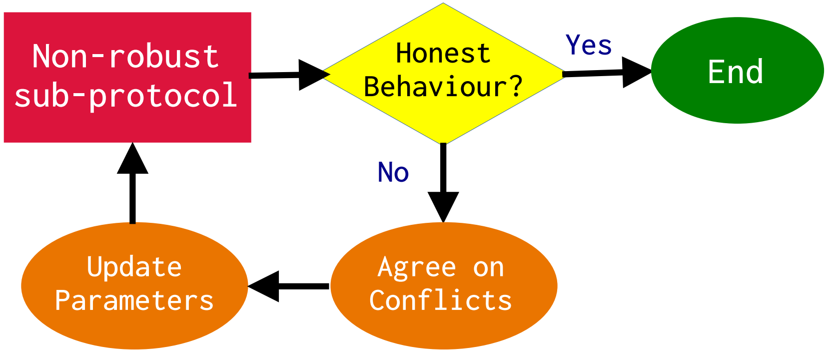


Example Execution

Partyset $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$

Flaw in [KSR02]

Player Elimination Framework [HMP00]



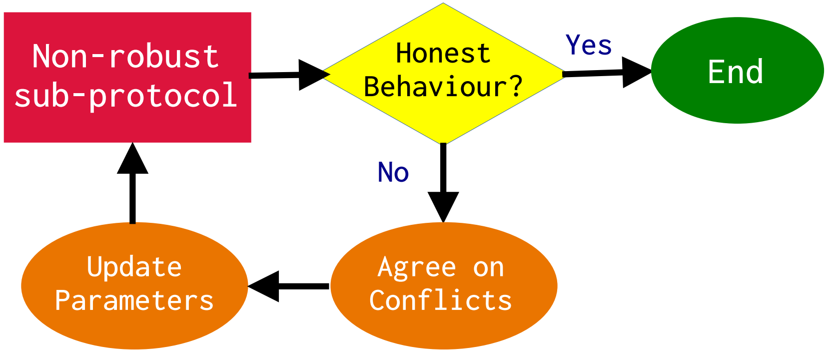
Example Execution

Partyset $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$

Adversary Structure satisfying $\mathcal{Q}^{(4)}$

Flaw in [KSR02]

Player Elimination Framework [HMP00]



Example Execution

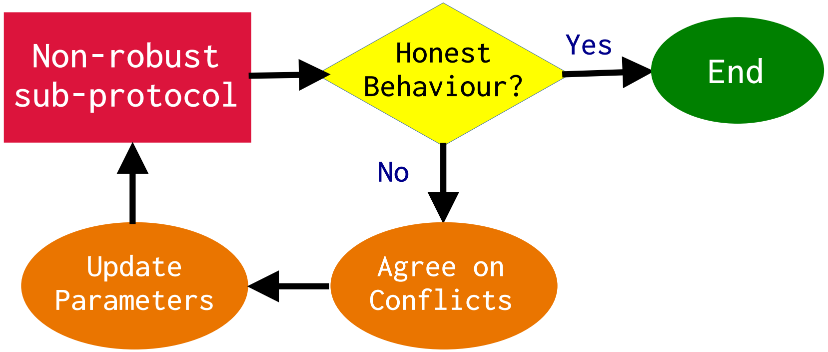
Partyset $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$

Adversary Structure satisfying $\mathcal{Q}^{(4)}$

$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

Flaw in [KSR02]

Player Elimination Framework [HMP00]



Example Execution

Partyset $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$

Adversary Structure satisfying $\mathcal{Q}^{(4)}$

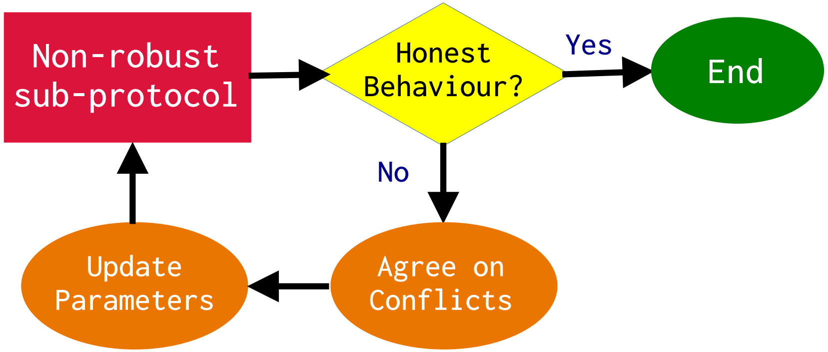
$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

Conflict Set

$\{P_1, P_2, P_7\}$

Flaw in [KSR02]

Player Elimination Framework [HMP00]



Example Execution

Partyset $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$

Adversary Structure satisfying $\mathcal{Q}^{(4)}$

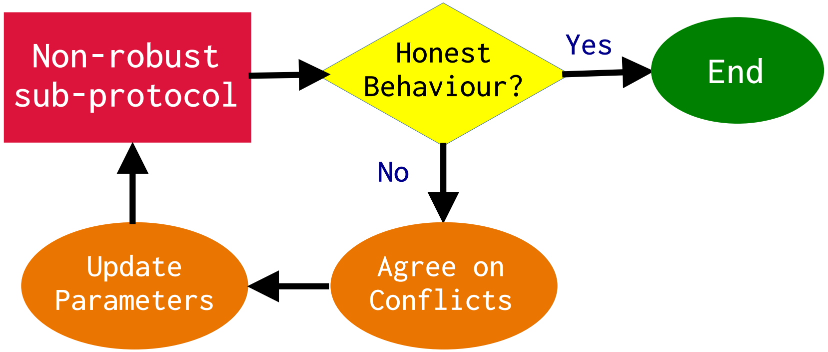
$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

Conflict Set

$\{P_1, P_2, P_7\}$ Choice of Adversary

Flaw in [KSR02]

Player Elimination Framework [HMP00]



Example Execution

Partyset $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$

Adversary Structure satisfying $\mathcal{Q}^{(4)}$

$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

Conflict Set

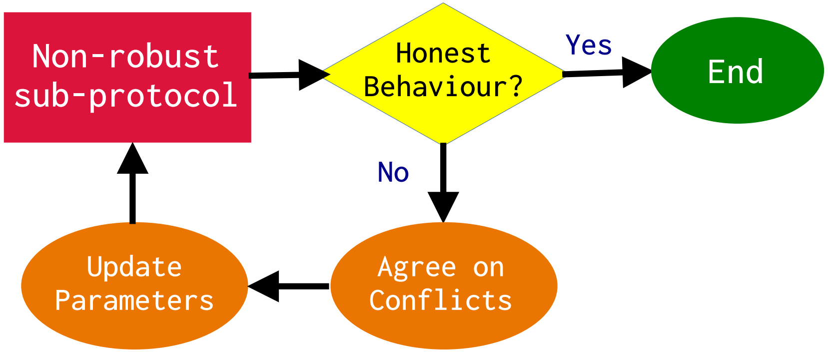
$\{P_1, P_2, P_7\}$ Choice of Adversary

Updated Parameters

$\mathcal{P} = \{P_3, P_4, P_5, P_6\}$

Flaw in [KSR02]

Player Elimination Framework [HMP00]



Example Execution

Partyset $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$

Adversary Structure satisfying $\mathcal{Q}^{(4)}$

$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

Conflict Set

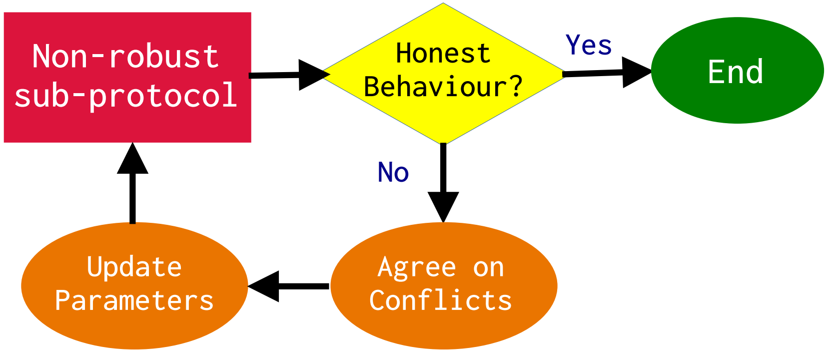
$\{P_1, P_2, P_7\}$ Choice of Adversary

Updated Parameters

$\mathcal{P} = \{P_3, P_4, P_5, P_6\}$ $\mathcal{Z}$ remains same

Flaw in [KSR02]

Player Elimination Framework [HMP00]



Example Execution

Partyset $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$

Adversary Structure satisfying $\mathcal{Q}^{(4)}$

$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

Conflict Set

$\{P_1, P_2, P_7\}$ Choice of Adversary

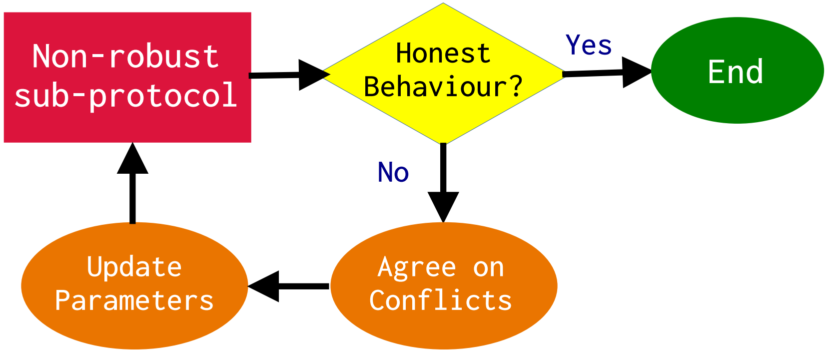
Updated Parameters

$\mathcal{P} = \{P_3, P_4, P_5, P_6\}$ $\mathcal{Z}$ remains same

$$\mathcal{P} \subseteq \{P_1, P_3\} \cup \{P_1, P_4\} \cup \{P_1, P_5, P_6\}$$

Flaw in [KSR02]

Player Elimination Framework [HMP00]



Example Execution

Partyset $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$

Adversary Structure satisfying $\mathcal{Q}^{(4)}$

$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

Conflict Set

$\{P_1, P_2, P_7\}$ Choice of Adversary

Updated Parameters

$\mathcal{P} = \{P_3, P_4, P_5, P_6\}$ $\mathcal{Z}$ remains same

$\mathcal{P} \subseteq \{P_1, P_3\} \cup \{P_1, P_4\} \cup \{P_1, P_5, P_6\}$ $\mathcal{Q}^{(3)}$ Fails

Verifiable Secret-Sharing

Verifiable Secret-Sharing

Dealer

Verifiable Secret-Sharing

Dealer 

Secret s

Verifiable Secret-Sharing

Dealer 

Secret $\boxed{s}$

$\downarrow$

$\boxed{s^{(1)}}$, $\cdots$, $\boxed{s^{(q)}}$ $\quad q = |\mathcal{Z}|$

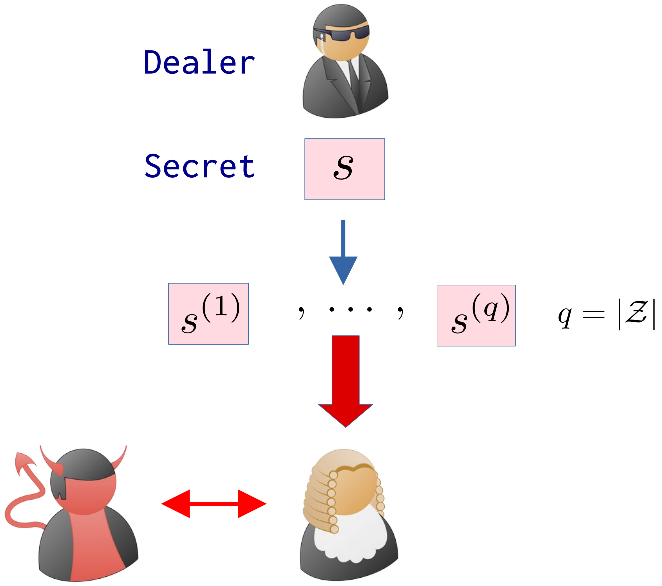
Verifiable Secret-Sharing

Dealer 

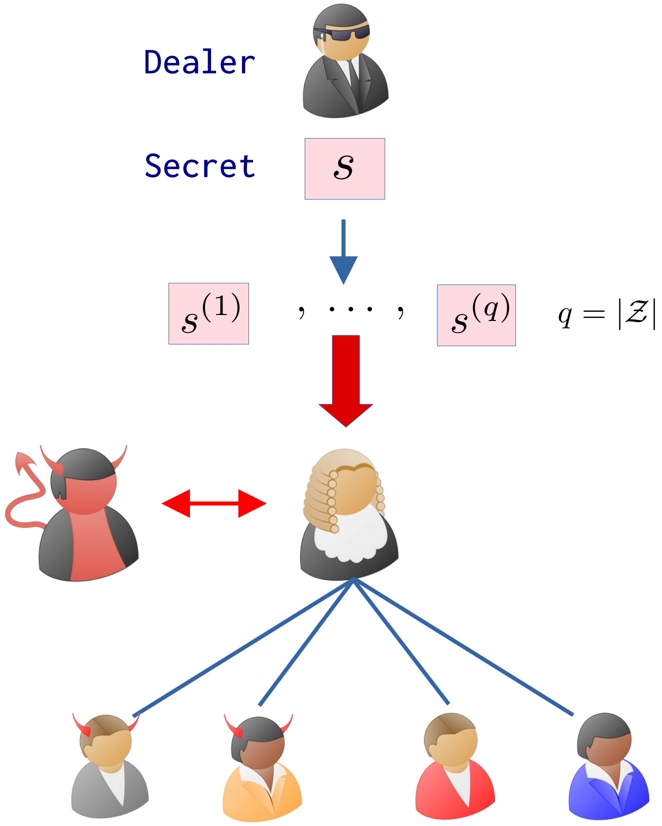
Secret $\boxed{s}$

$$\boxed{s^{(1)}}\;, \cdots,\; \boxed{s^{(q)}} \qquad q = |\mathcal{Z}|$$

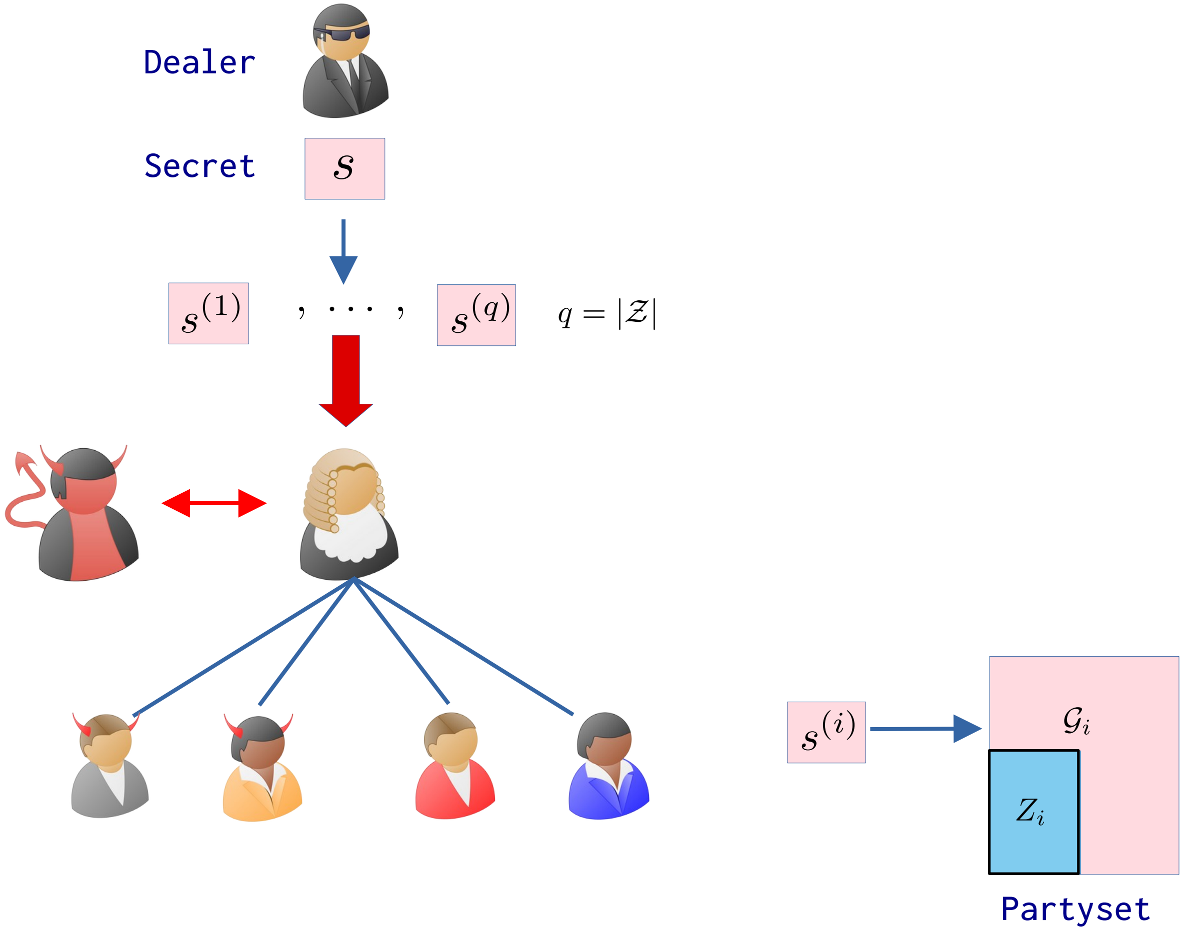
Verifiable Secret-Sharing



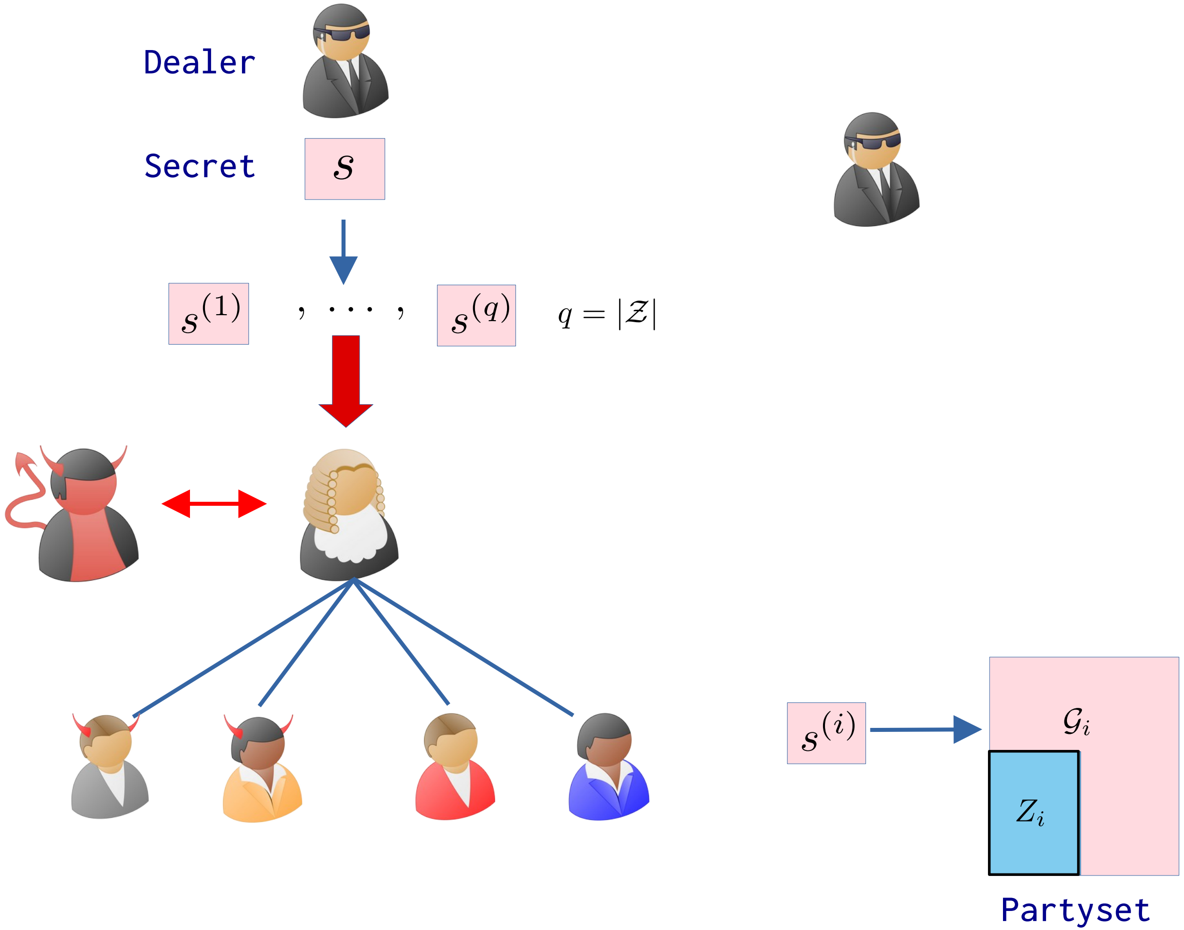
Verifiable Secret-Sharing



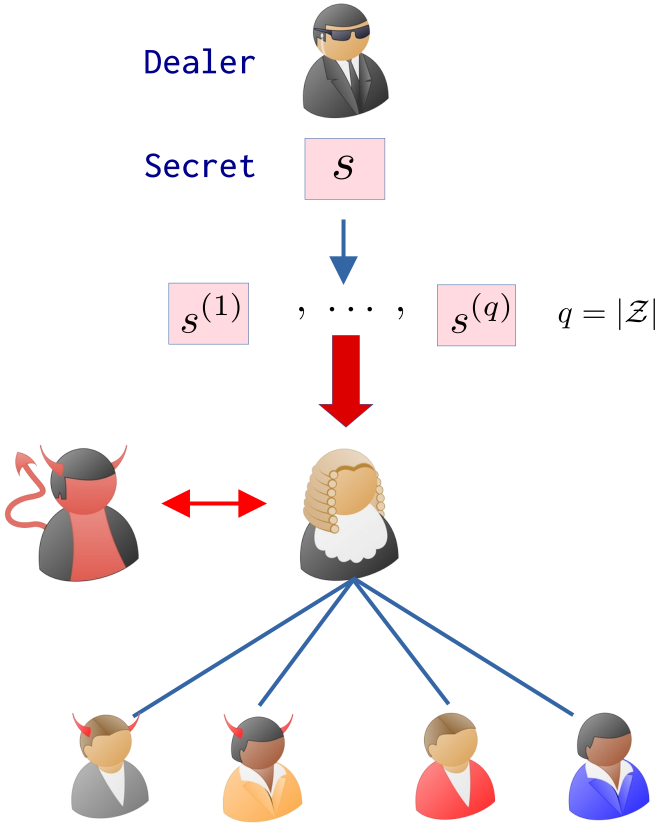
Verifiable Secret-Sharing

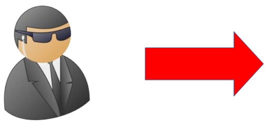


Verifiable Secret-Sharing

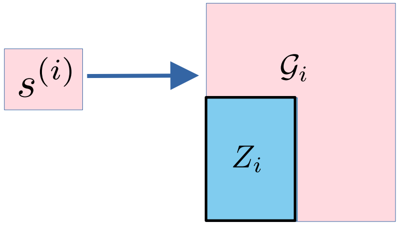


Verifiable Secret-Sharing

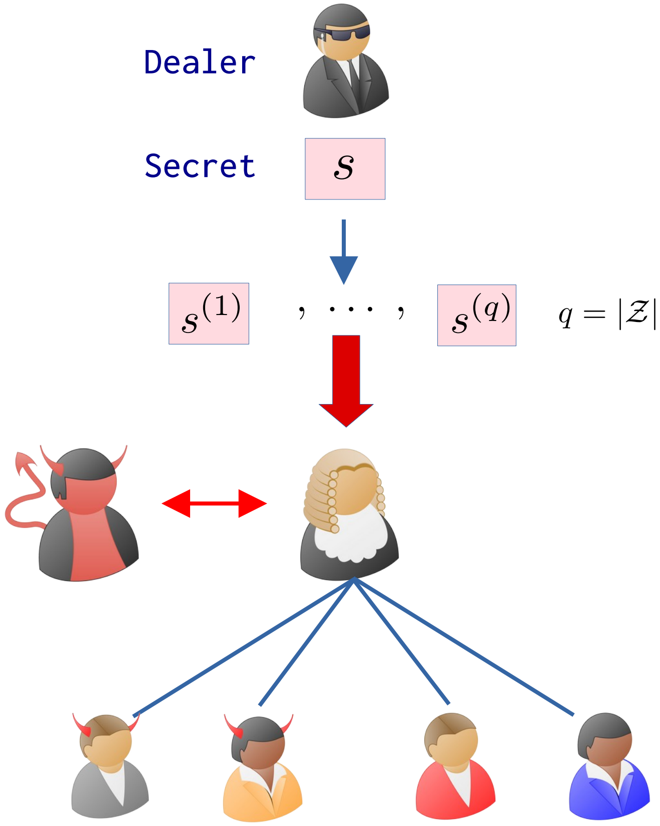


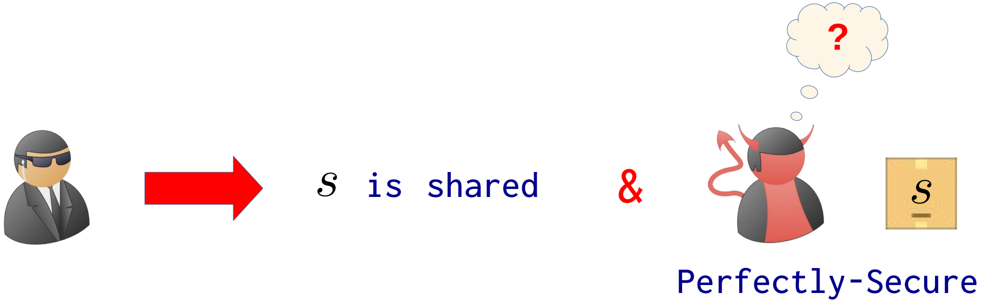


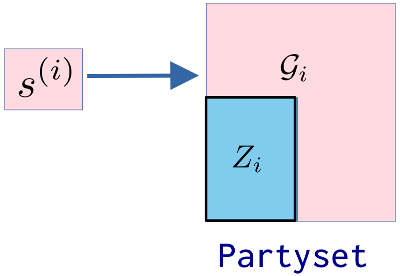
s is shared



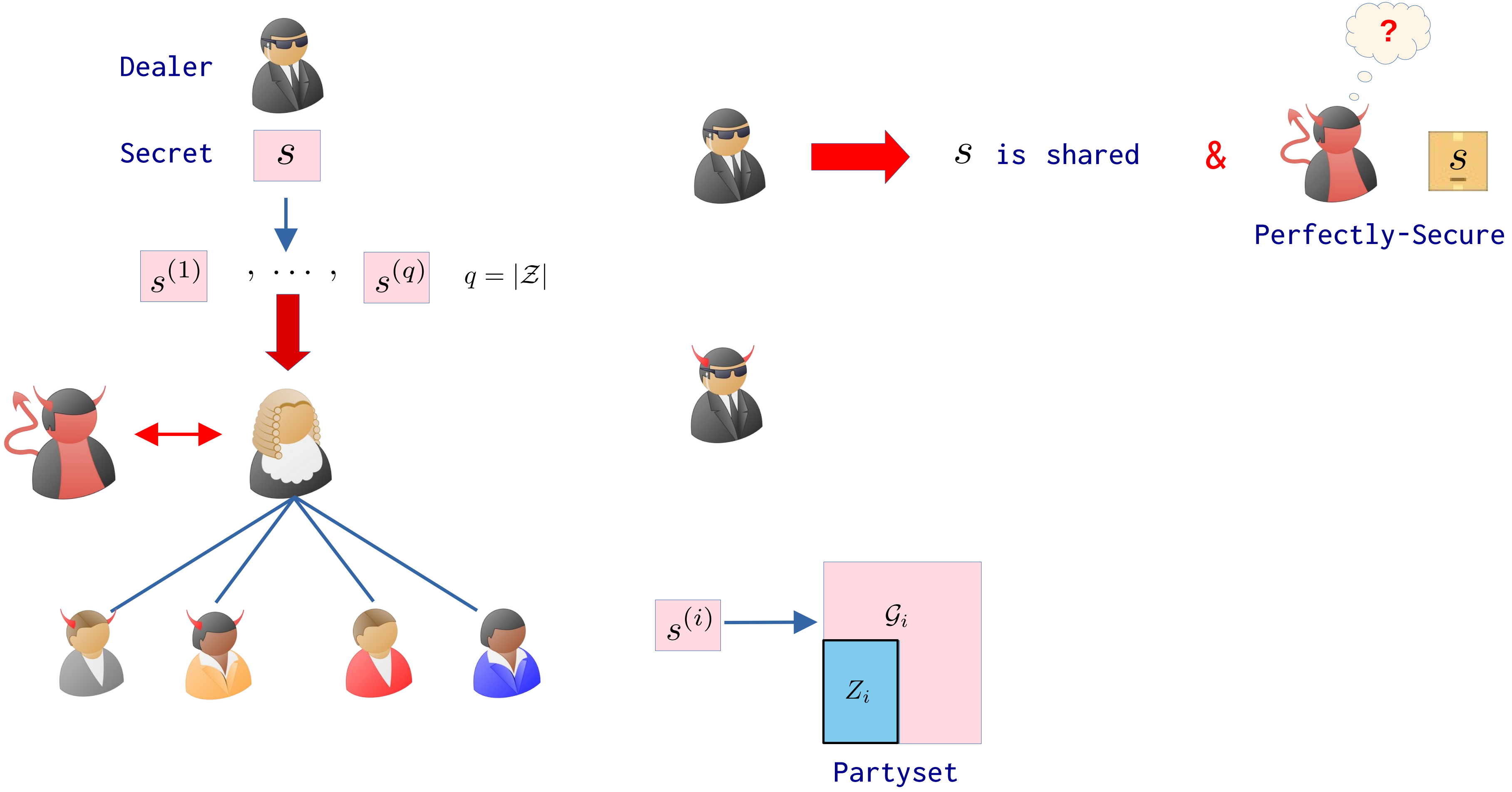
Verifiable Secret-Sharing



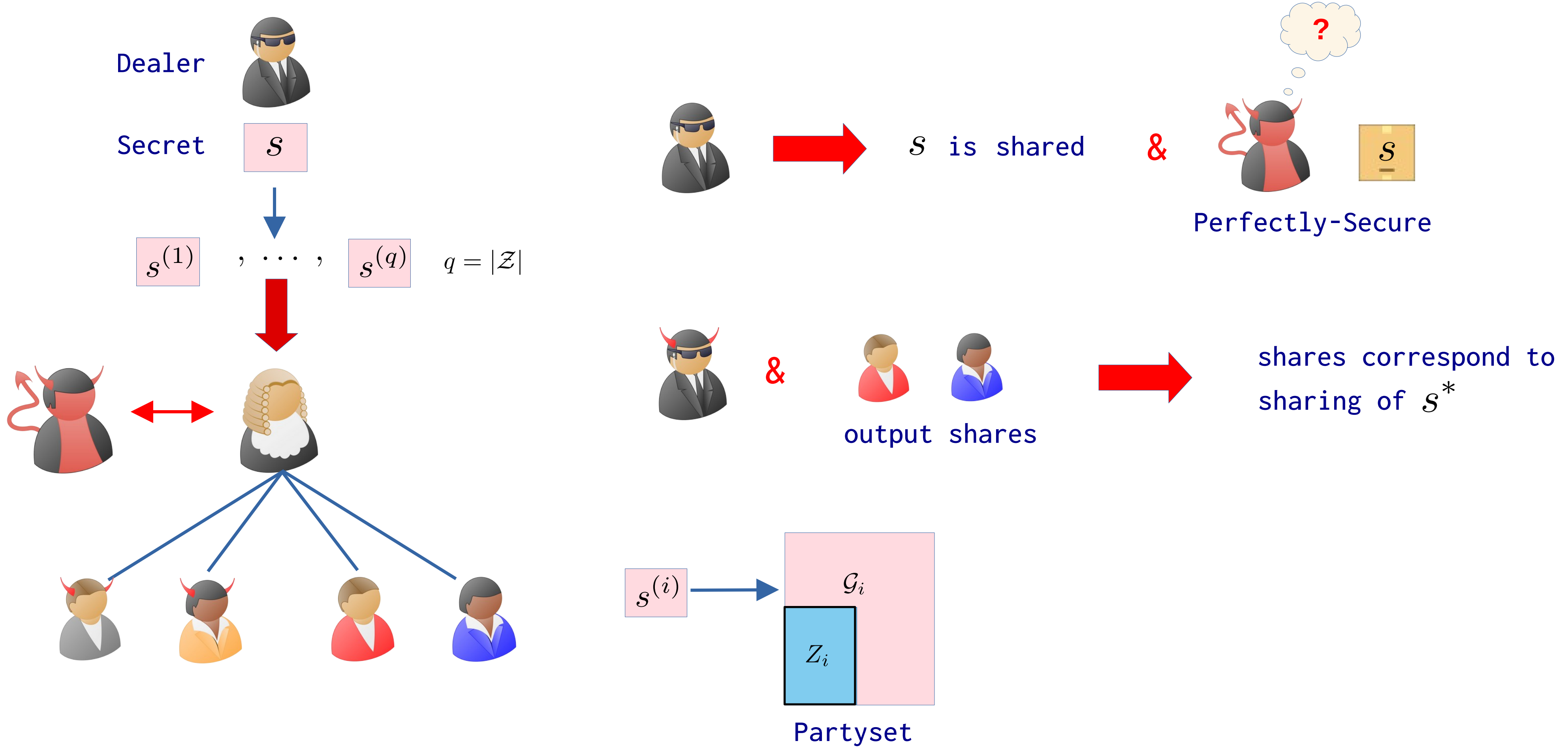




Verifiable Secret-Sharing



Verifiable Secret-Sharing



Verifiable Secret-Sharing

Verifiable Secret-Sharing

Verifiable Secret-Sharing

$$\mathcal{Z} = \{\boxed{\{P_1, P_2\}}, \boxed{\{P_1, P_3\}}, \boxed{\{P_1, P_4\}}, \boxed{\{P_1, P_5, P_6\}}, \boxed{\{P_7\}}\}$$

Verifiable Secret-Sharing

$\mathcal{Z} = \{\boxed{\{P_1, P_2\}}, \boxed{\{P_1, P_3\}}, \boxed{\{P_1, P_4\}}, \boxed{\{P_1, P_5, P_6\}}, \boxed{\{P_7\}}\}$

Dealer

Verifiable Secret-Sharing

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

Secret

s

Dealer

Verifiable Secret-Sharing

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

Secret

s

Dealer

$$s^{(1)} + s^{(2)} + s^{(3)} + \cdots + s^{(q)}$$

$q = |\mathcal{Z}|$

Verifiable Secret-Sharing

$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

Dealer

Secret

$$\boxed{s} = \boxed{s^{(1)}} + \boxed{s^{(2)}} + \boxed{s^{(3)}} + \cdots + \boxed{s^{(q)}}$$

$$q = |\mathcal{Z}|$$

Verifiable Secret-Sharing

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

Dealer

Secret

$$\boxed{s} = \boxed{s^{(1)}} + \boxed{s^{(2)}} + \boxed{s^{(3)}} + \cdots + \boxed{s^{(q)}}$$

$q = |\mathcal{Z}|$

Verifiable Secret-Sharing

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

Dealer

Secret

$$s = s^{(1)} + s^{(2)} + s^{(3)} + \cdots + s^{(q)}$$

$q = |\mathcal{Z}|$

P_2, P_3
P_5, P_6, P_7

$\{P_1, P_4\}$

Verifiable Secret-Sharing

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

$s^{(1)}$

$+$

$s^{(2)}$

[Mau02]

Secret

$+$

s $=$ $s^{(3)}$ $\Rightarrow$ P_2, P_3
P_5, P_6, P_7

$+$

$\{P_1, P_4\}$

$\vdots$

$+$

$s^{(q)}$

Dealer

$q = |\mathcal{Z}|$

Verifiable Secret-Sharing

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

Dealer

Secret

$$s = s^{(1)} + s^{(2)} + s^{(3)} + \cdots + s^{(q)}$$

$q = |\mathcal{Z}|$

[Mau02]

P_2, P_3
P_5, P_6, P_7

$\{P_1, P_4\}$

$s^{(3)} \rightarrow$ one-time pad

Verifiable Secret-Sharing

$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

Dealer

Secret

$$s = s^{(1)} + s^{(2)} + s^{(3)} + \cdots + s^{(q)}$$

$q = |\mathcal{Z}|$

[Mau02]

P_2, P_3
P_5, P_6, P_7

$\{P_1, P_4\}$

$s^{(3)} \rightarrow$ one-time pad

Non-adversary sets

$\downarrow$

$s^{(1)}, \ldots, s^{(q)}$

Verifiable Secret-Sharing

$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

Dealer

Secret

$$s = s^{(1)} + s^{(2)} + s^{(3)} + \cdots + s^{(q)}$$

$q = |\mathcal{Z}|$

[Mau02]

P_2, P_3
P_5, P_6, P_7

$\{P_1, P_4\}$

$s^{(3)} \rightarrow$ one-time pad

Non-adversary sets

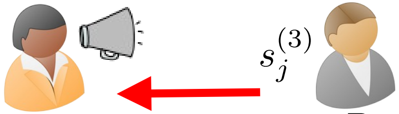
$\downarrow$

$s^{(1)}, \ldots, s^{(q)}$

?

Verifiable Secret-Sharing

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$



$s_i^{(3)}$ P_i $\longleftarrow$ $s_j^{(3)}$ P_j

Dealer

Secret

$$s = s^{(1)} + s^{(2)} + s^{(3)} + \cdots + s^{(q)}$$

$q = |\mathcal{Z}|$

[Mau02]

P_2, P_3
P_5, P_6, P_7

$\{P_1, P_4\}$

?

$s^{(3)} \rightarrow$ one-time pad

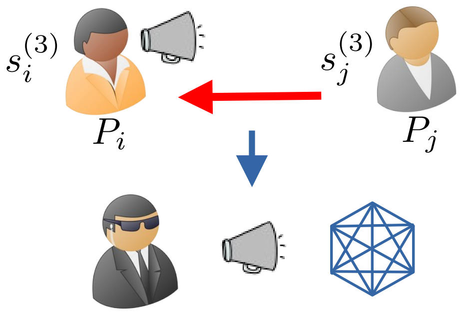
Non-adversary sets

$\downarrow$

$s^{(1)}, \ldots, s^{(q)}$

Verifiable Secret-Sharing

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$



Dealer

Secret

$s = s^{(1)} + s^{(2)} + s^{(3)} + \cdots + s^{(q)}$

$q = |\mathcal{Z}|$

[Mau02]

P_2, P_3
P_5, P_6, P_7

$\{P_1, P_4\}$

?

$s^{(3)} \rightarrow$ one-time pad

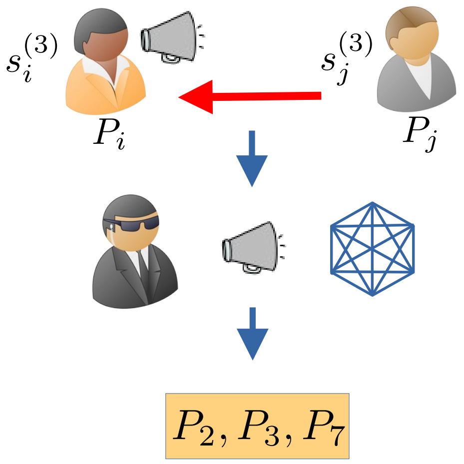
Non-adversary sets

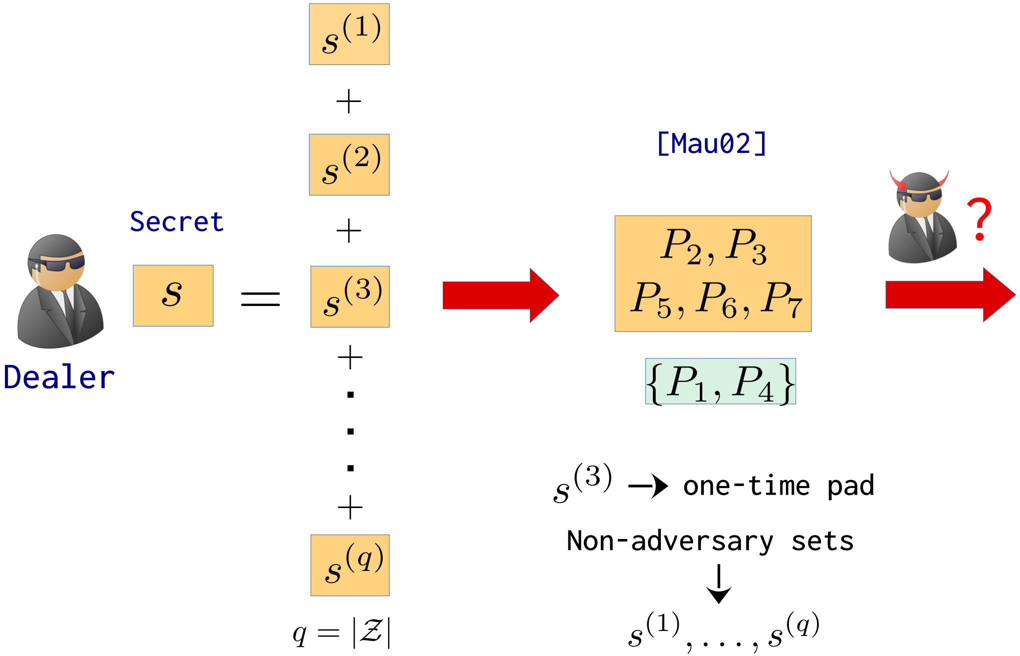
$\downarrow$

$s^{(1)}, \ldots, s^{(q)}$

Verifiable Secret-Sharing

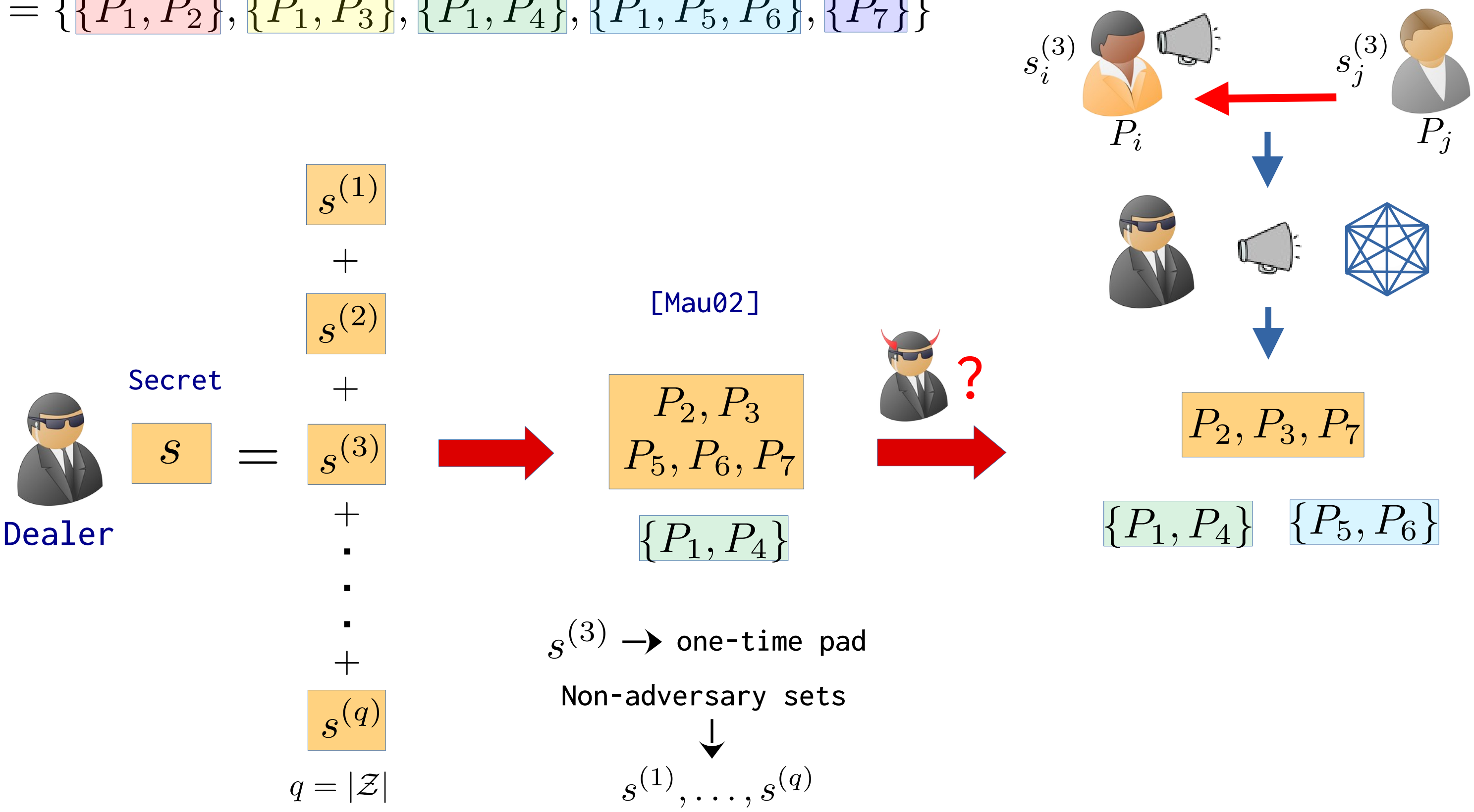
$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$



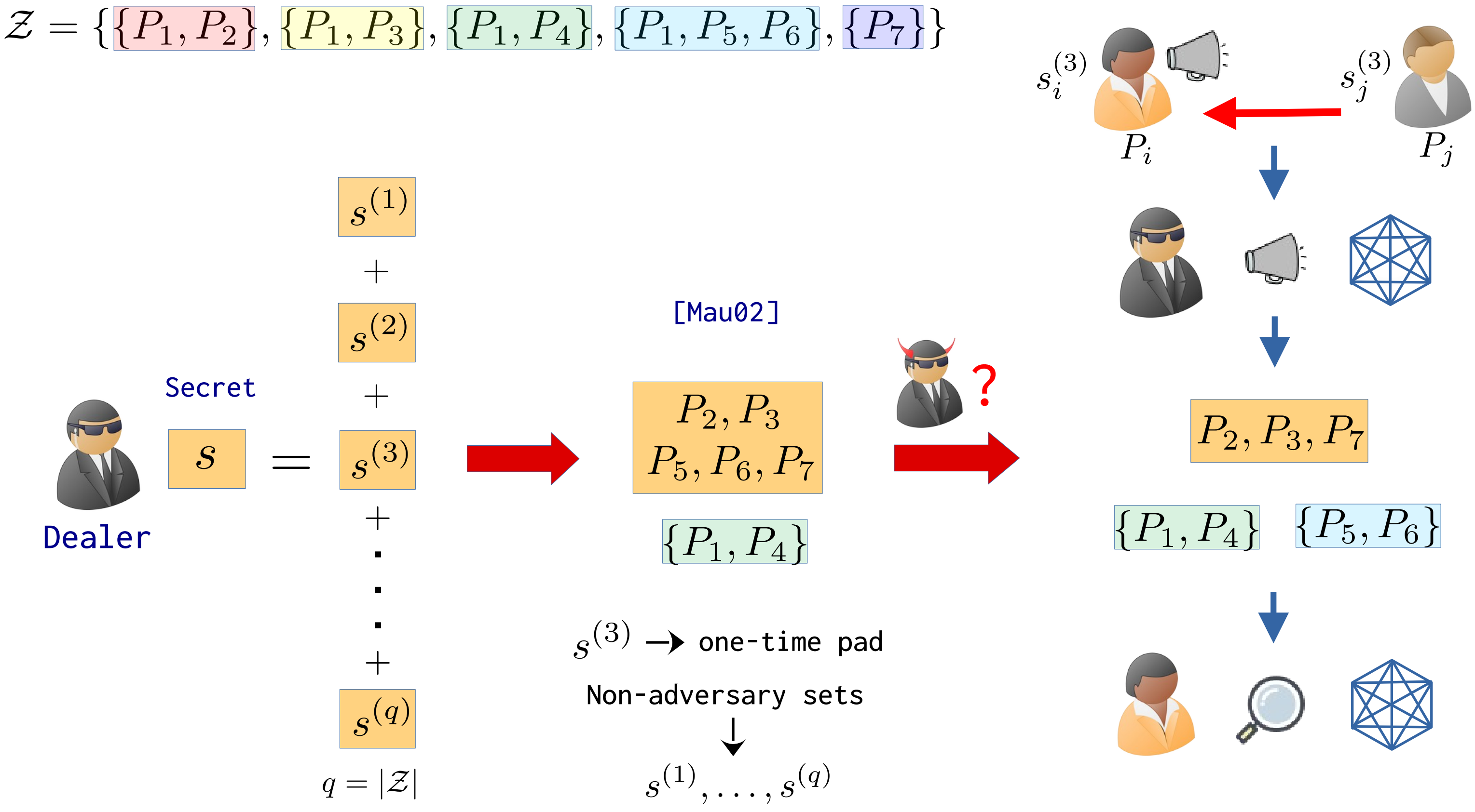


Verifiable Secret-Sharing

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

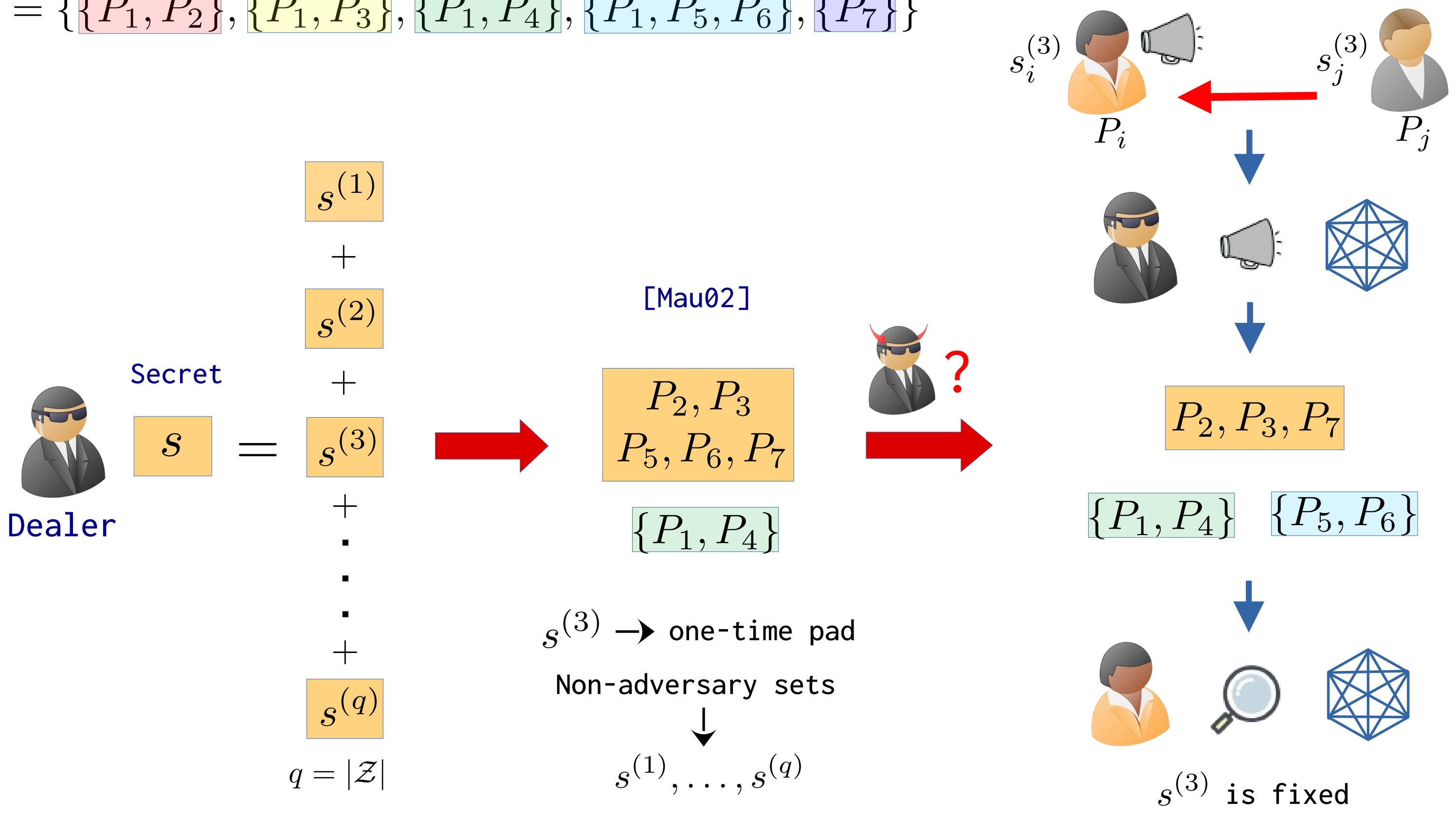


Verifiable Secret-Sharing



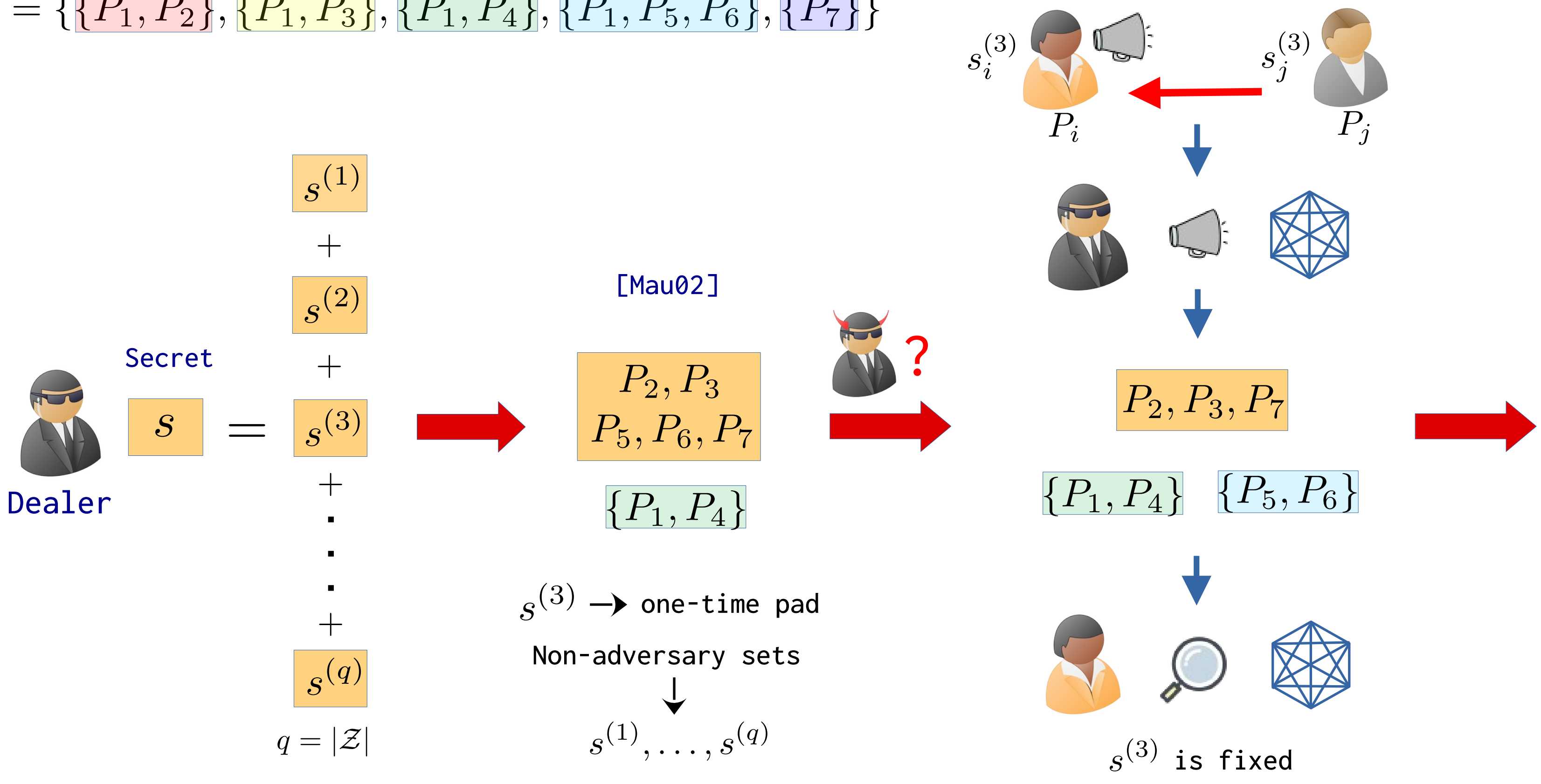
Verifiable Secret-Sharing

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$



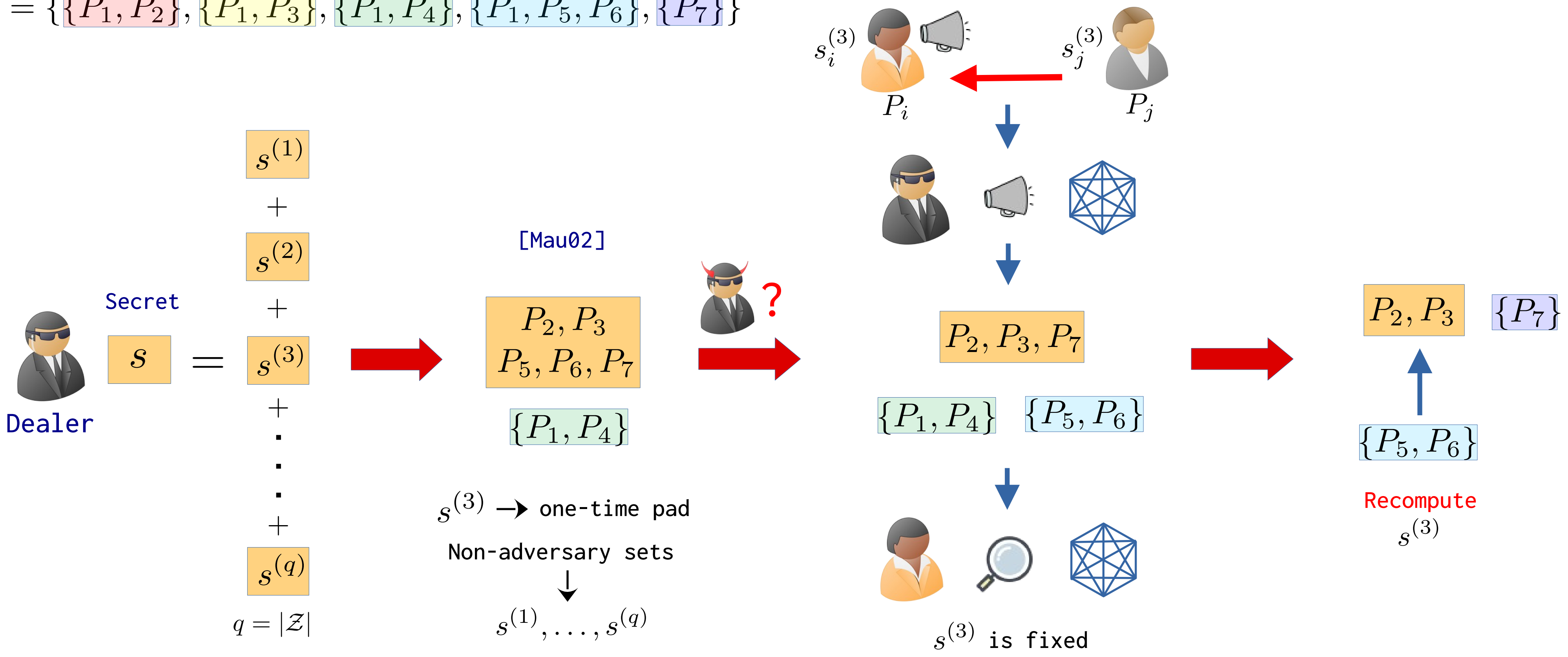
Verifiable Secret-Sharing

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$



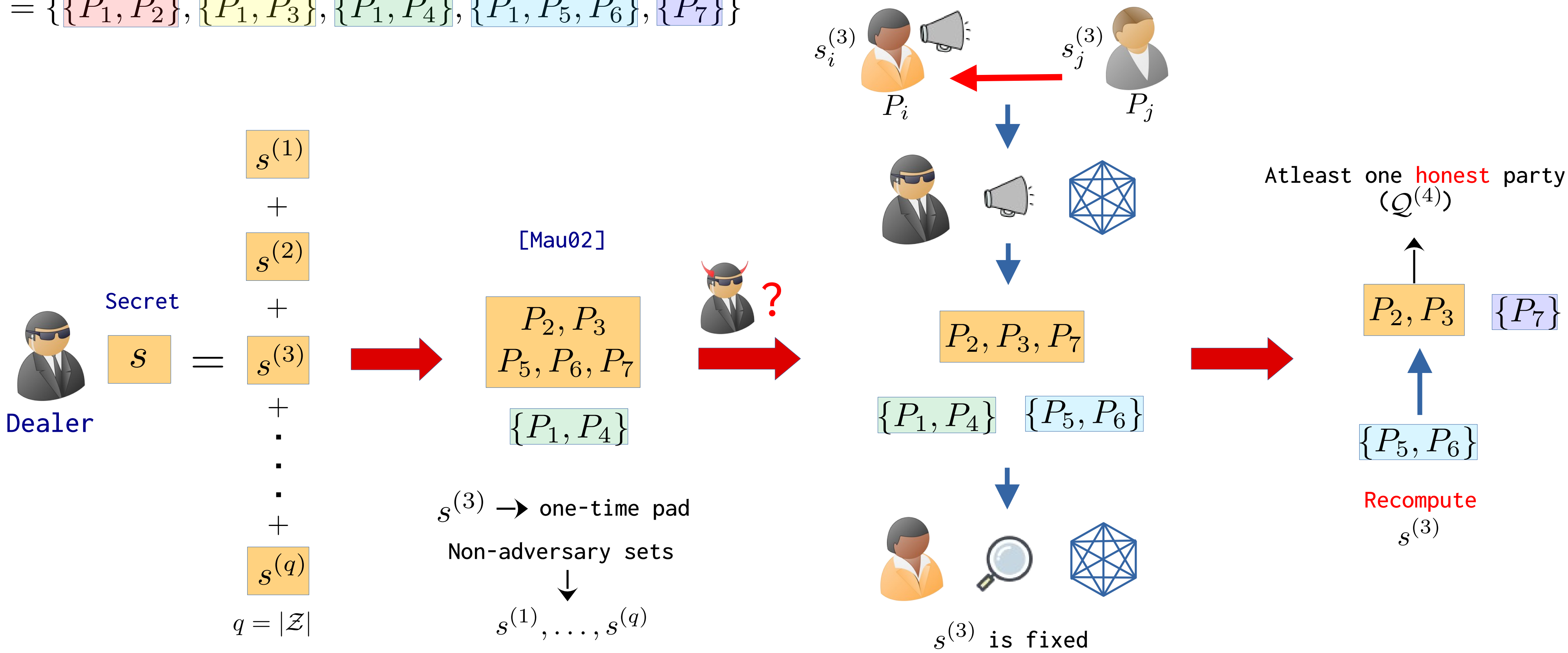
Verifiable Secret-Sharing

$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$



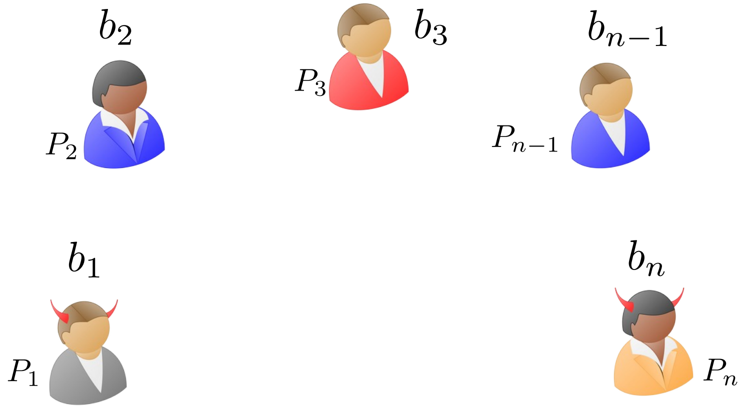
Verifiable Secret-Sharing

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$



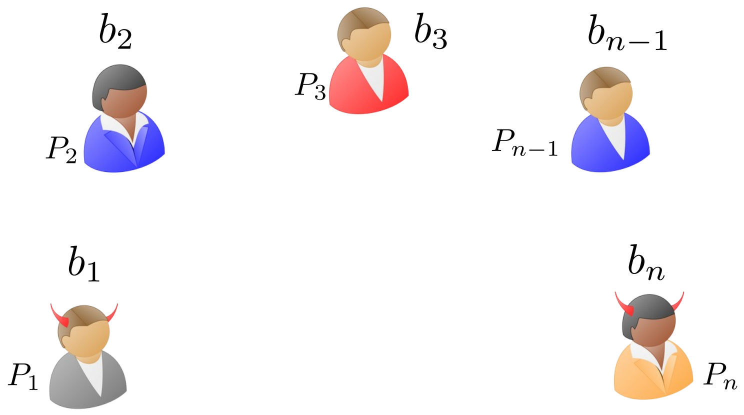
Asynchronous Byzantine Agreement (ABA)

Asynchronous Byzantine Agreement (ABA)



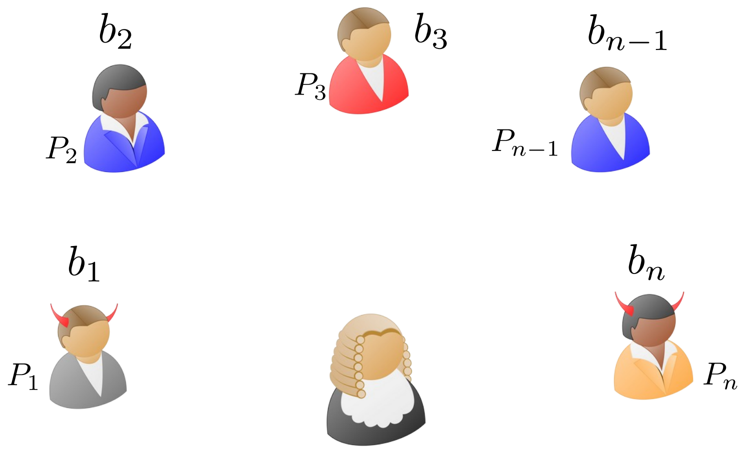
Asynchronous Byzantine Agreement (ABA)

Agree on a common bit



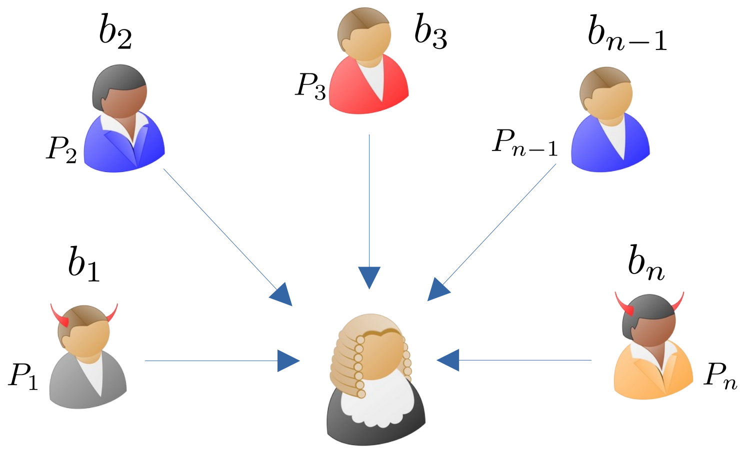
Asynchronous Byzantine Agreement (ABA)

Agree on a common bit



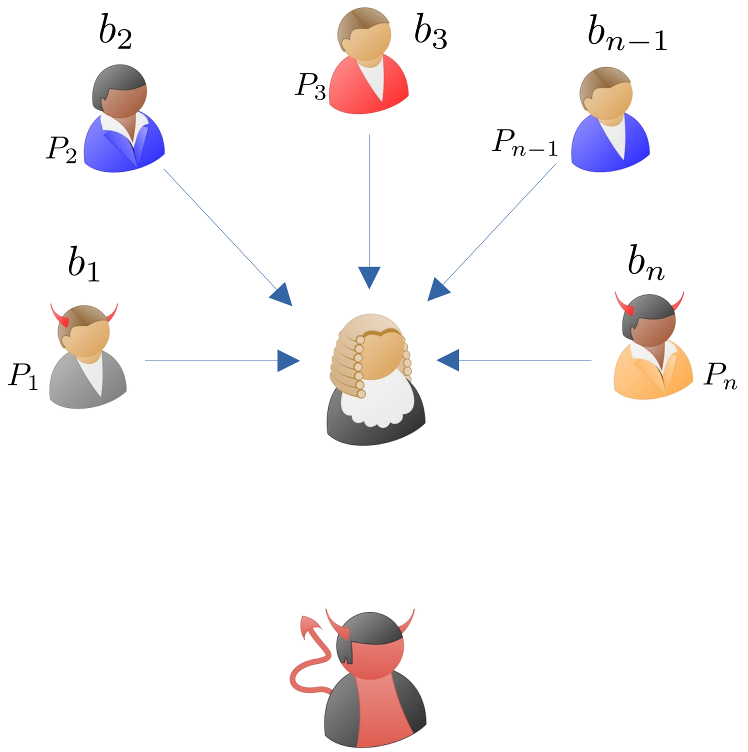
Asynchronous Byzantine Agreement (ABA)

Agree on a common bit



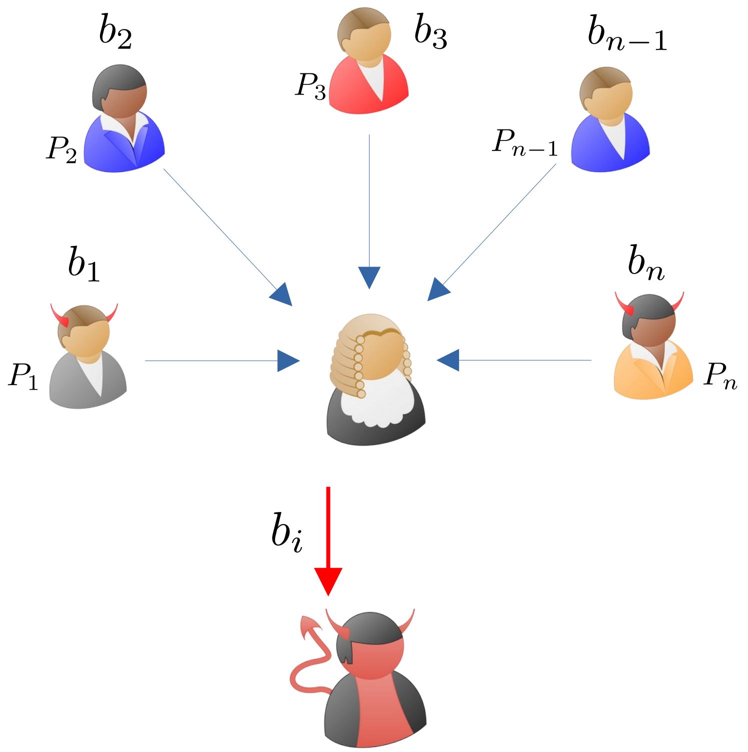
Asynchronous Byzantine Agreement (ABA)

Agree on a common bit



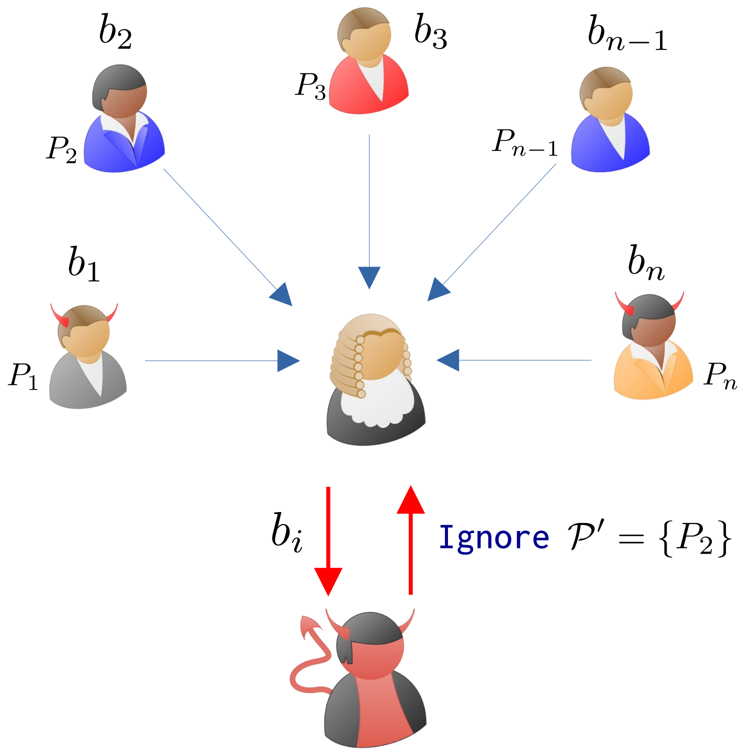
Asynchronous Byzantine Agreement (ABA)

Agree on a common bit



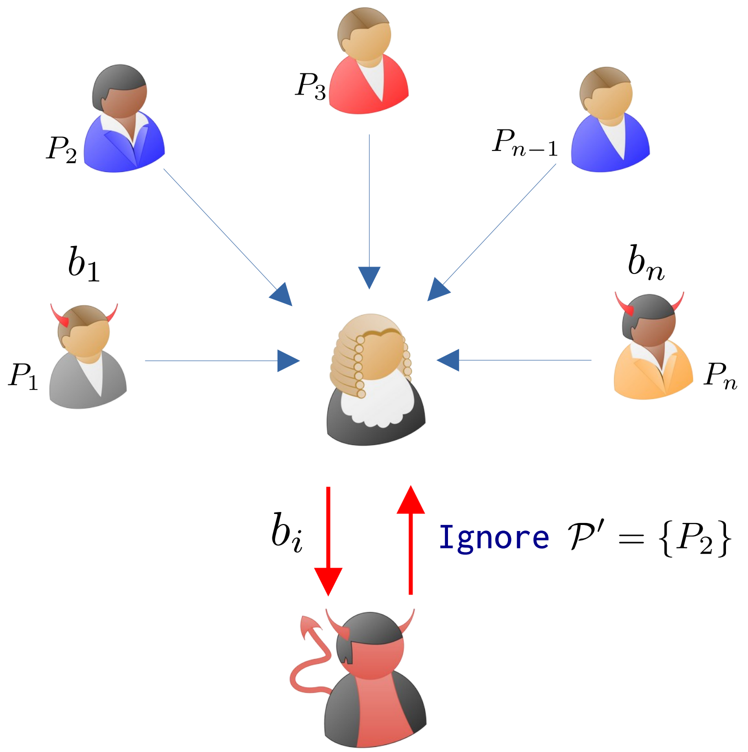
Asynchronous Byzantine Agreement (ABA)

Agree on a common bit



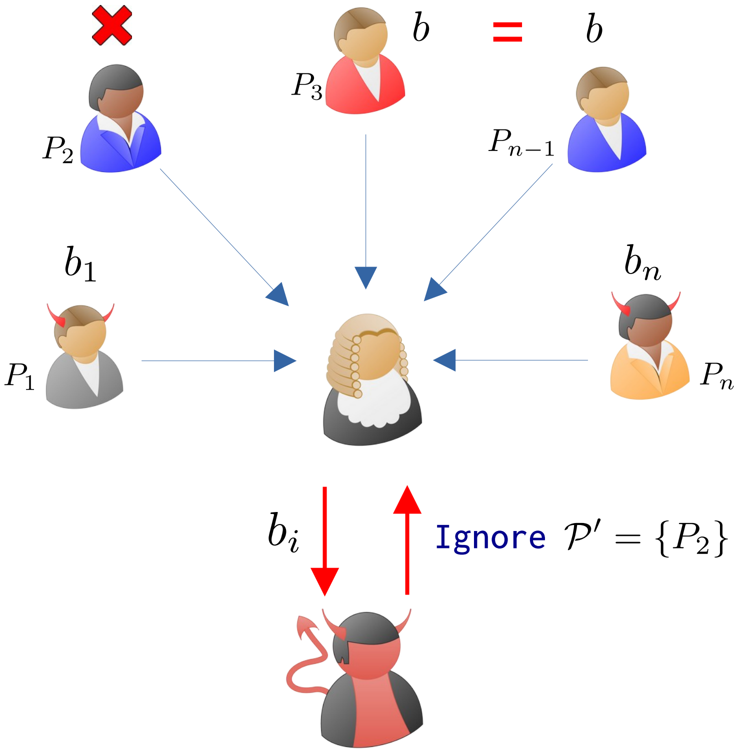
Asynchronous Byzantine Agreement (ABA)

Agree on a common bit



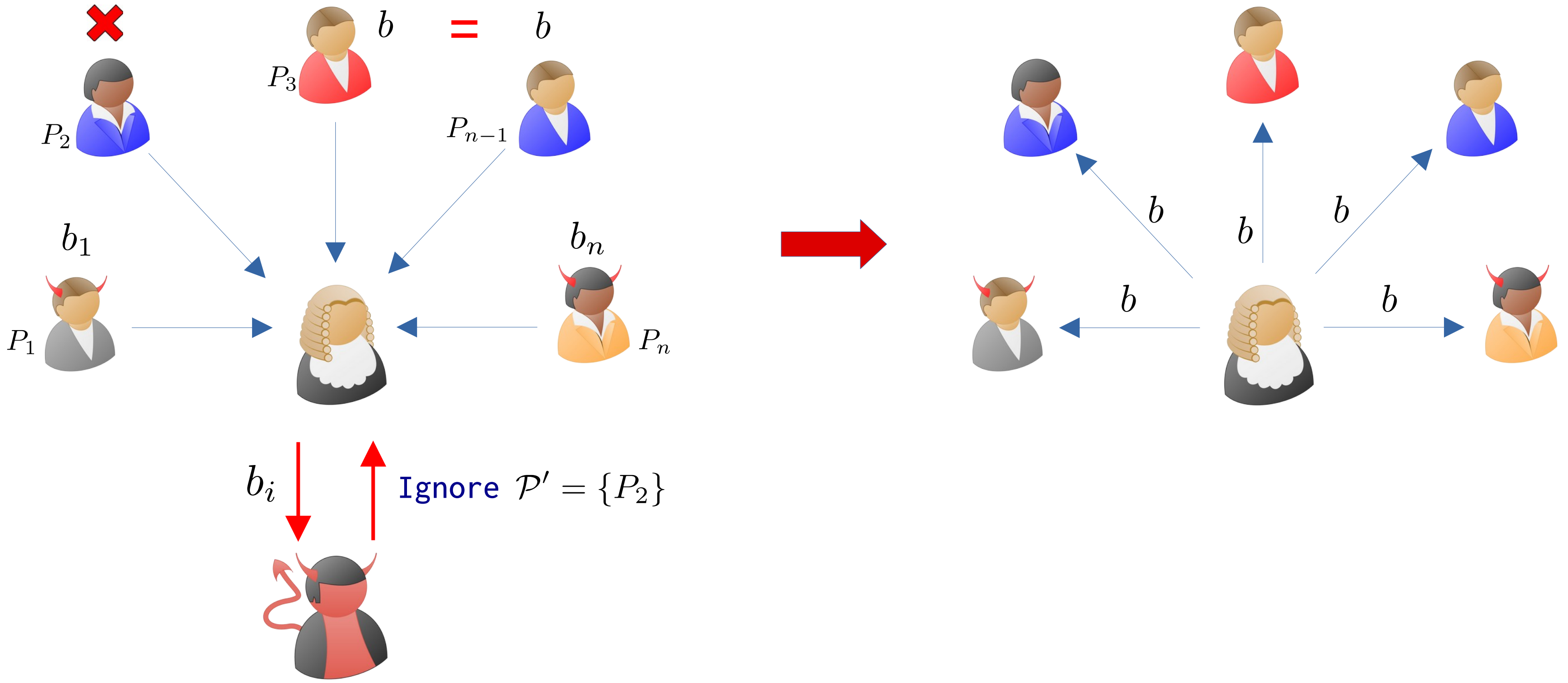
Asynchronous Byzantine Agreement (ABA)

Agree on a common bit



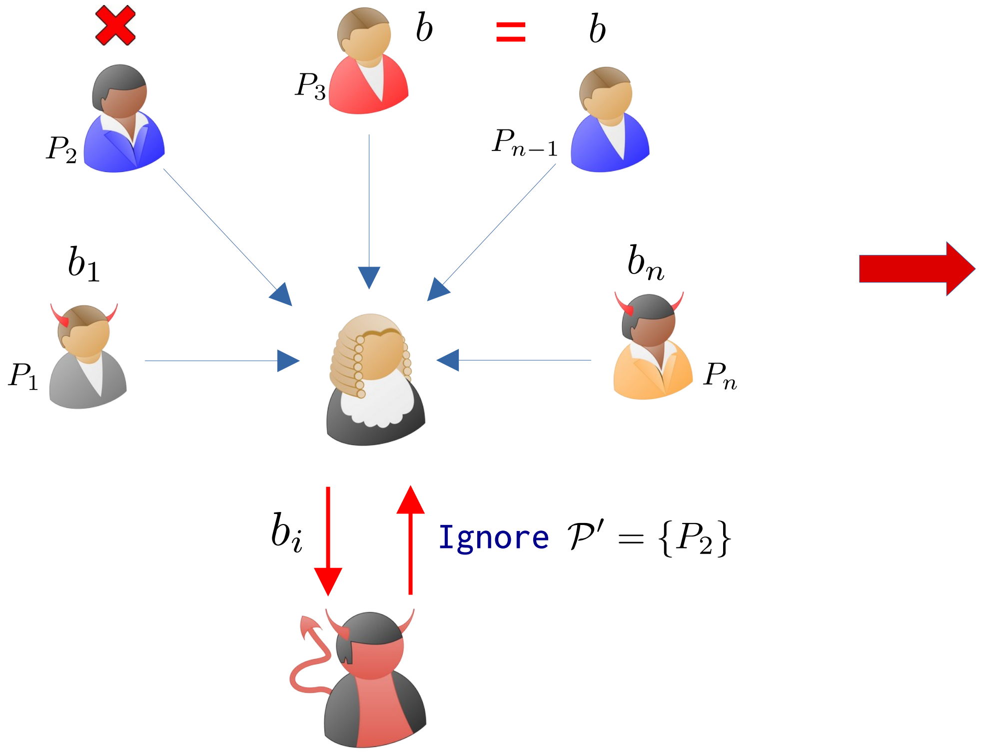
Asynchronous Byzantine Agreement (ABA)

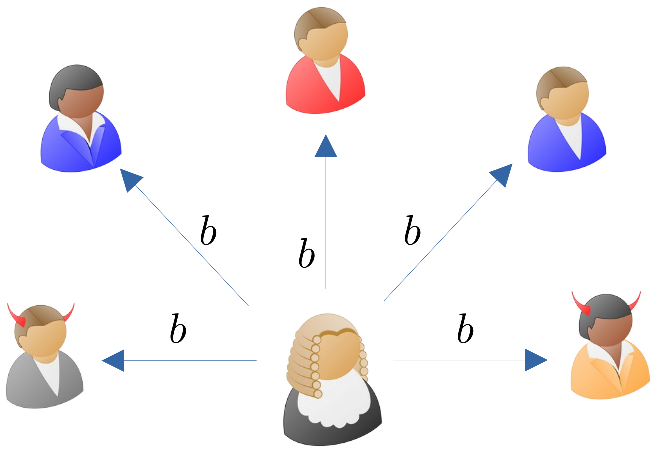
Agree on a common bit



Asynchronous Byzantine Agreement (ABA)

Agree on a common bit

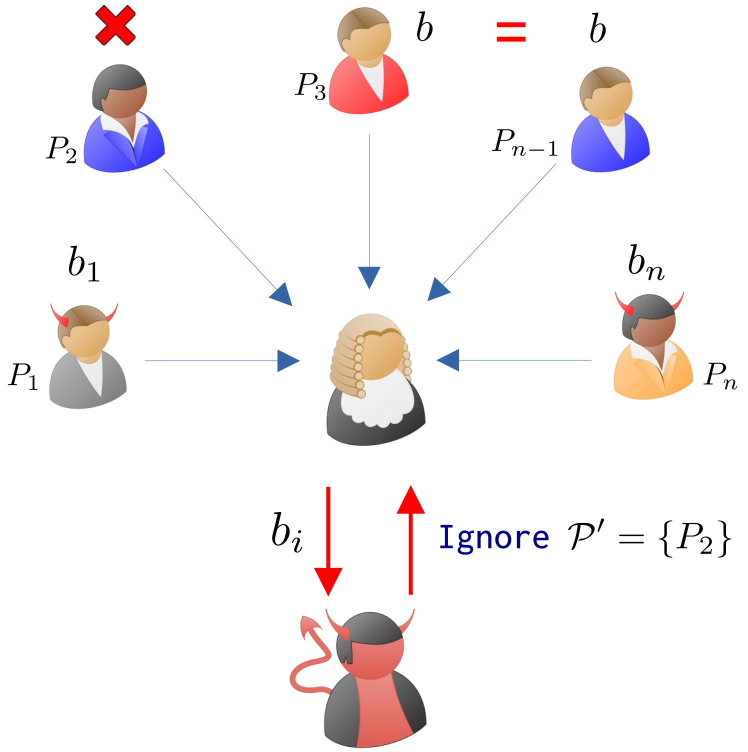




Validity

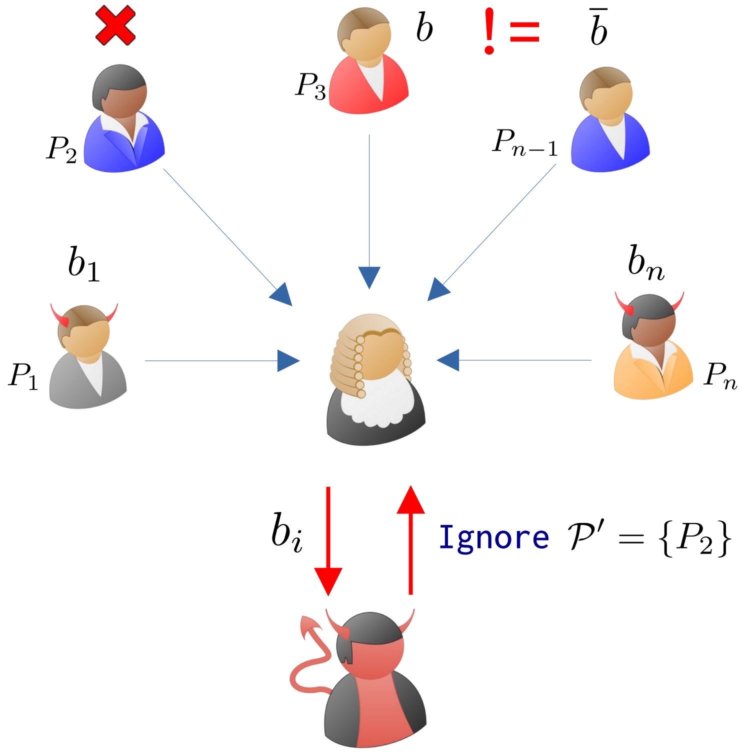
Asynchronous Byzantine Agreement (ABA)

Agree on a common bit



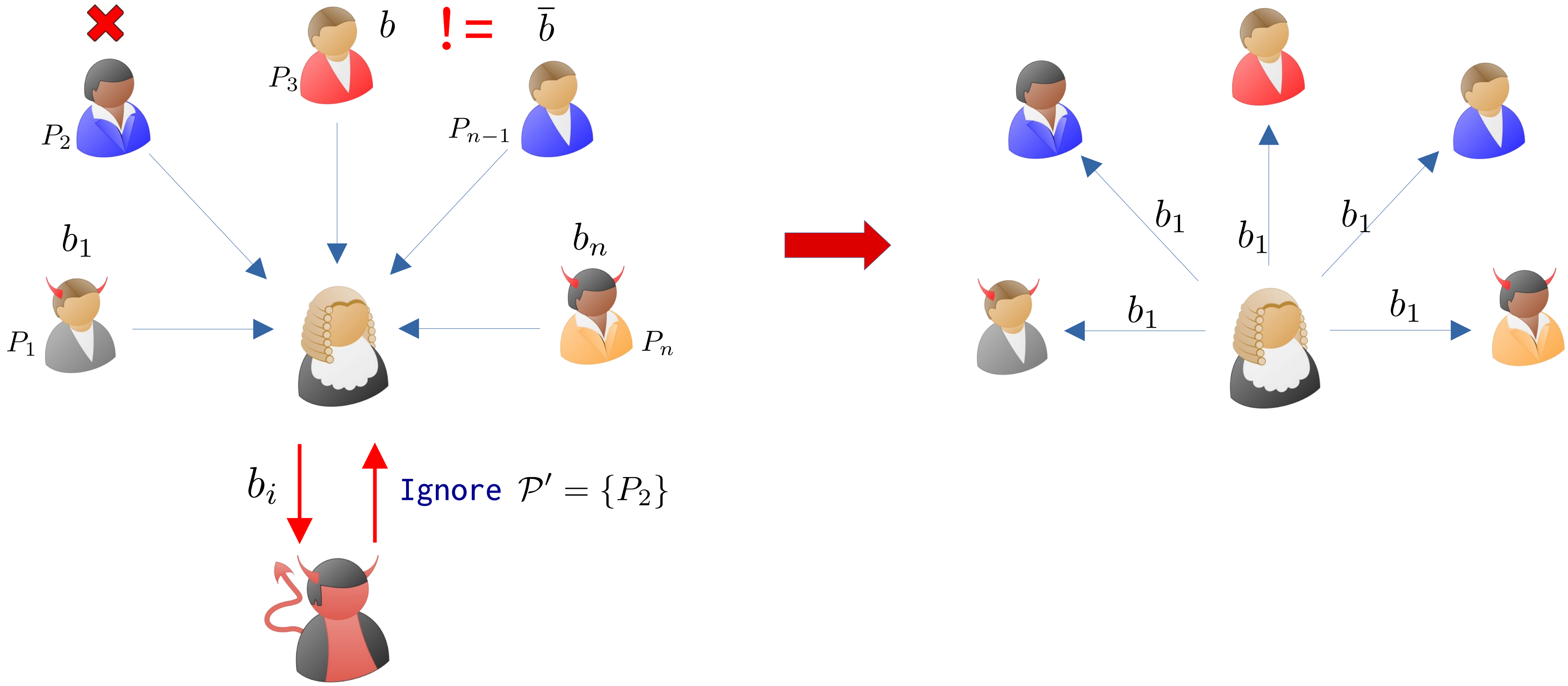
Asynchronous Byzantine Agreement (ABA)

Agree on a common bit



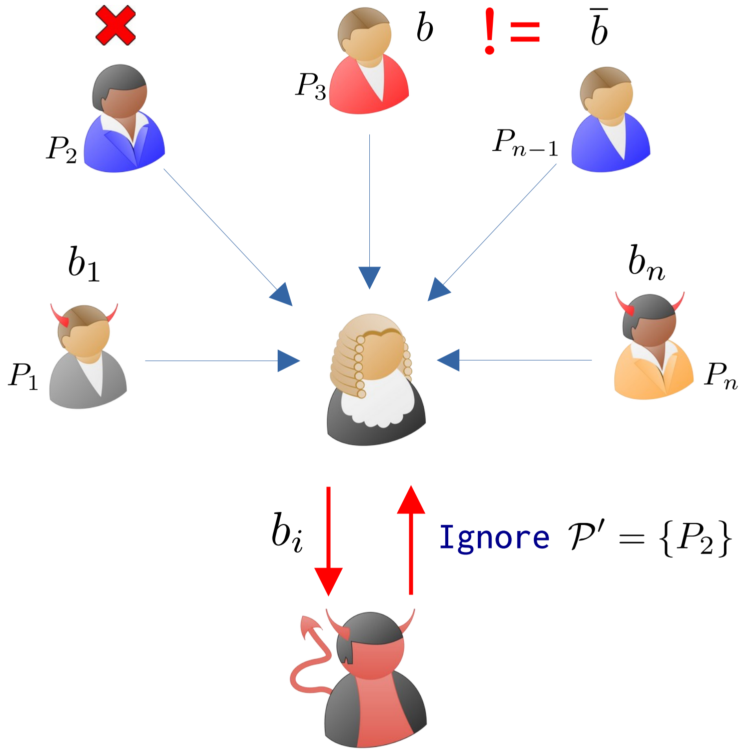
Asynchronous Byzantine Agreement (ABA)

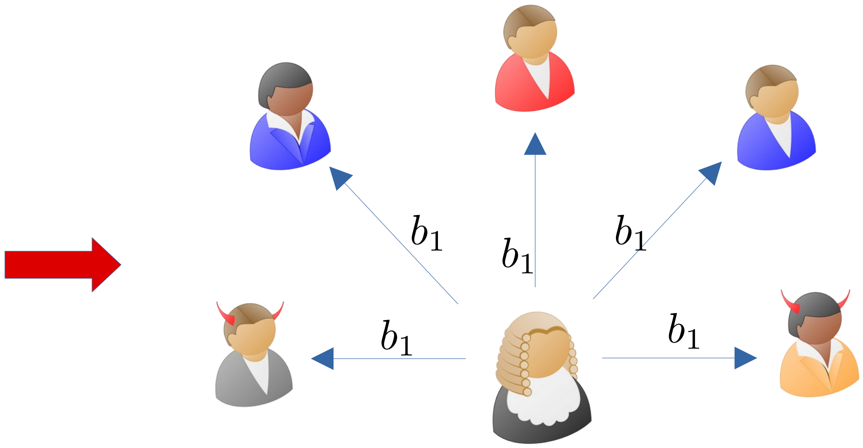
Agree on a common bit



Asynchronous Byzantine Agreement (ABA)

Agree on a common bit





Agreement

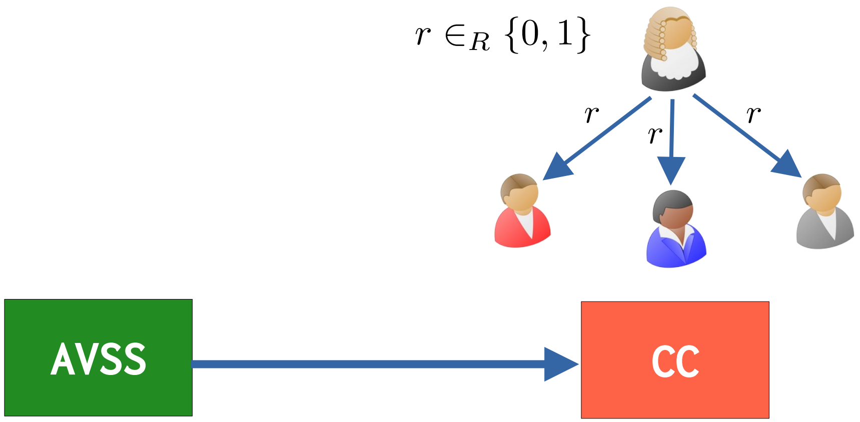
Asynchronous Byzantine Agreement (ABA)

Asynchronous Byzantine Agreement (ABA)

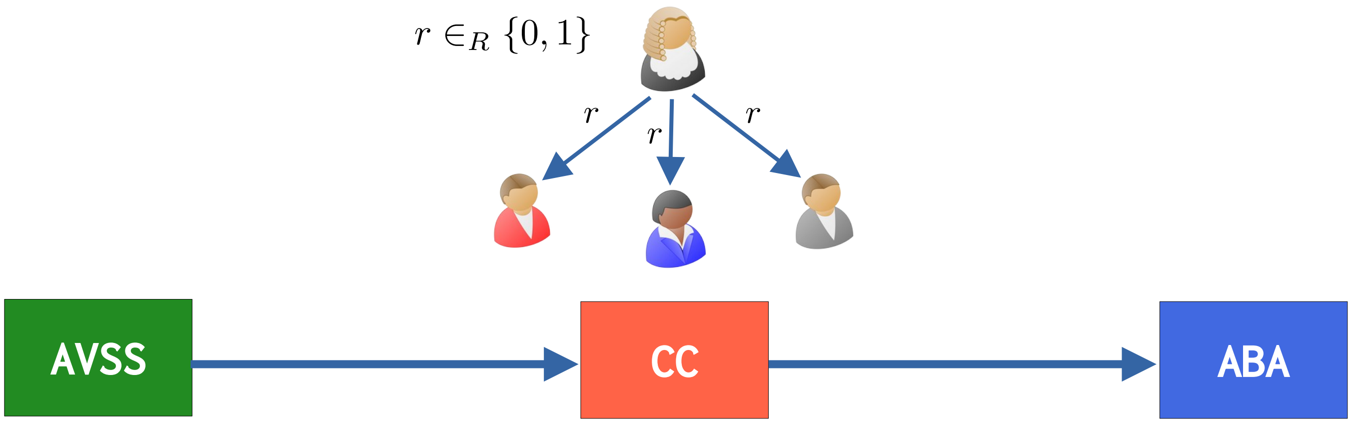
AVSS

Asynchronous Byzantine Agreement (ABA)

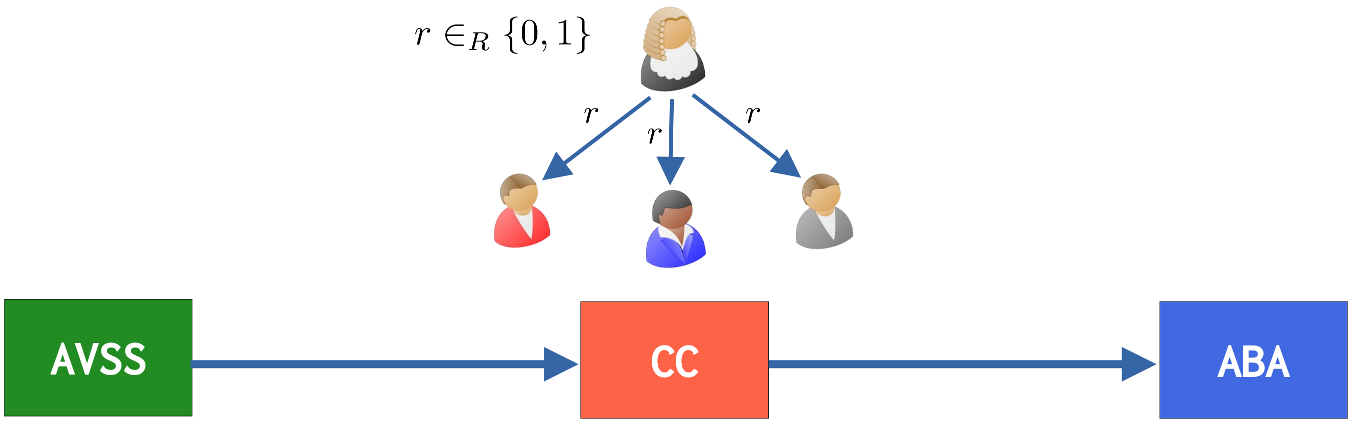
Asynchronous Byzantine Agreement (ABA)



Asynchronous Byzantine Agreement (ABA)

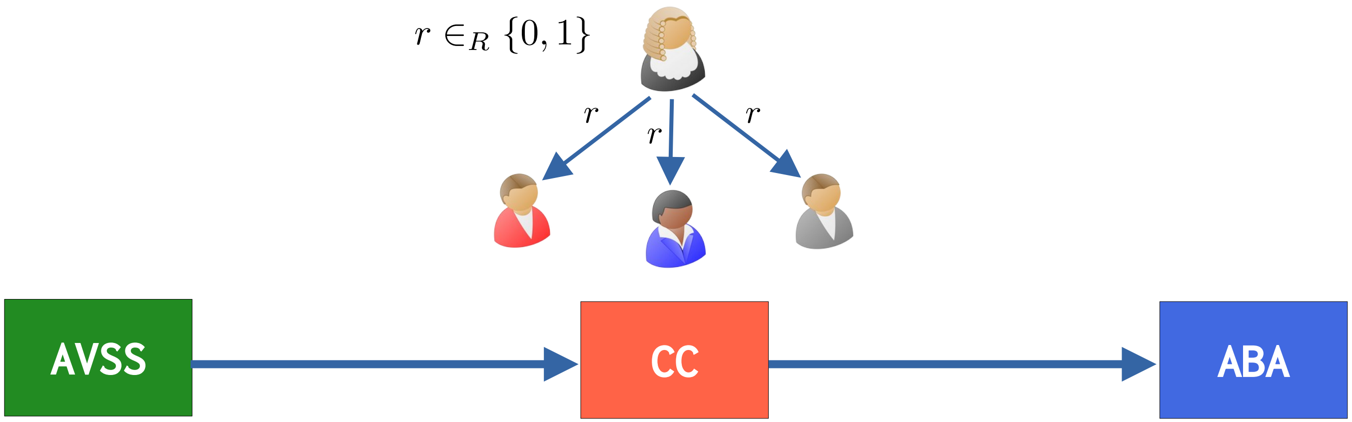


Asynchronous Byzantine Agreement (ABA)



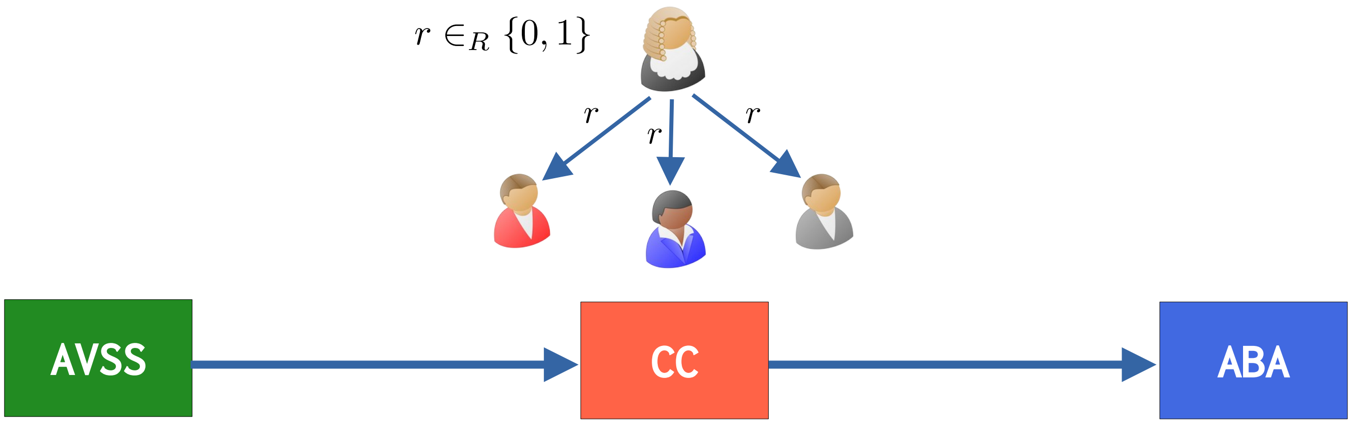
- Perfectly-Secure

Asynchronous Byzantine Agreement (ABA)



- Perfectly-Secure
- Generalization of [CR93]

Asynchronous Byzantine Agreement (ABA)

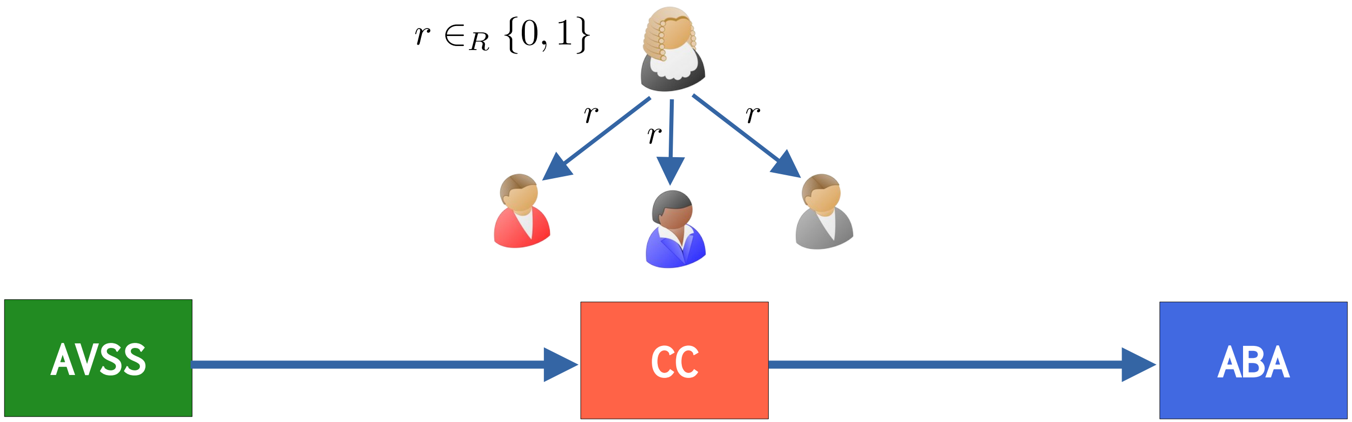


- Perfectly-Secure

- Generalization of [CR93]

- Success Probability $> 1/n$

Asynchronous Byzantine Agreement (ABA)



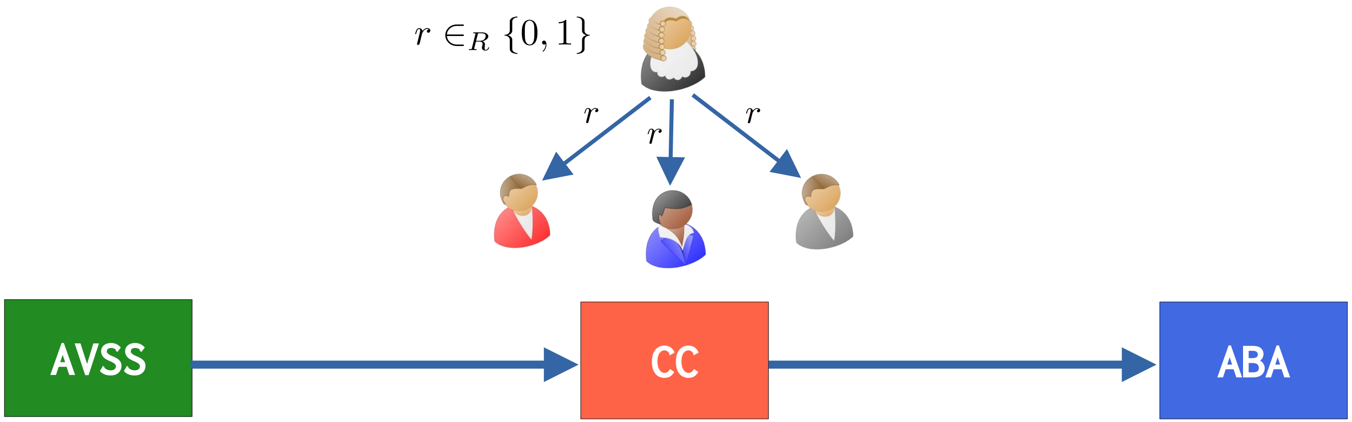
- Perfectly-Secure

- Generalization of [CR93]

- Success Probability $> 1/n$

  Depends on largest set in $\mathcal{Z}$

Asynchronous Byzantine Agreement (ABA)



- Perfectly-Secure

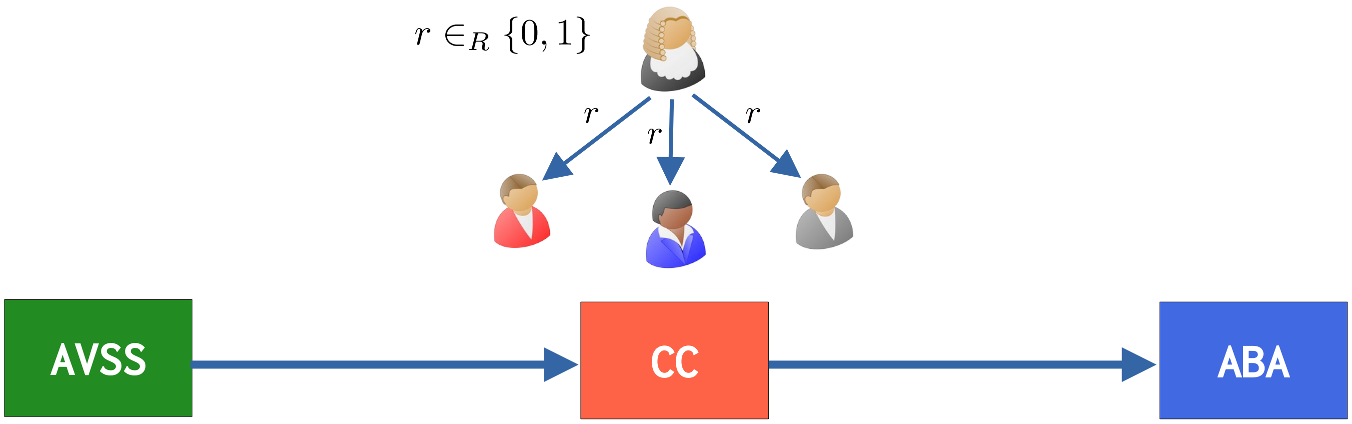
- Generalization of [CR93]

- Success Probability $> 1/n$

  Depends on largest set in $\mathcal{Z}$

- Terminates with probability 1

Asynchronous Byzantine Agreement (ABA)

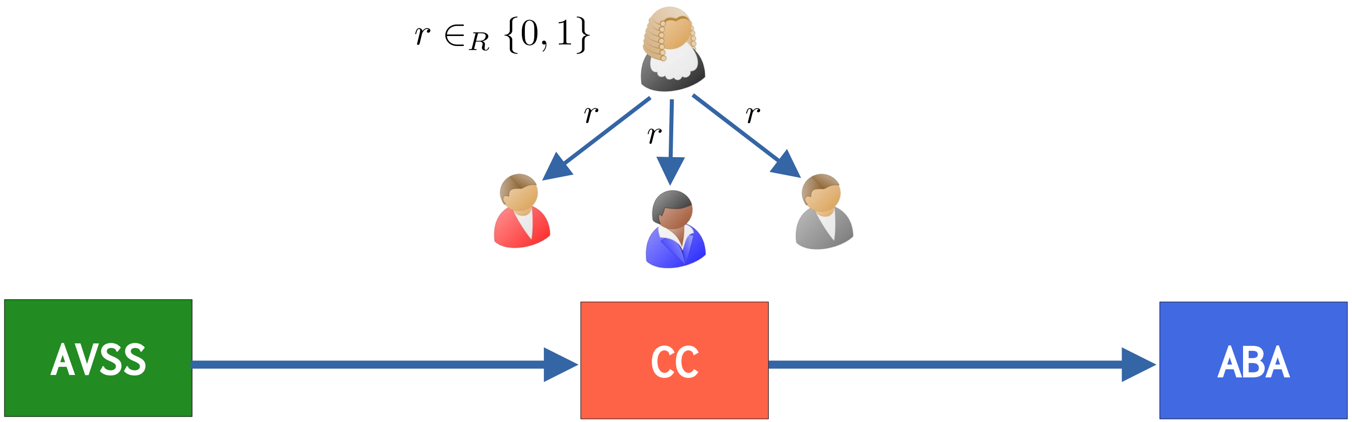


- Perfectly-Secure

- Generalization of [CR93]
- Success Probability $> 1/n$
  Depends on largest set in $\mathcal{Z}$

- Terminates with probability 1
- Expected Running Time
  $R = \mathcal{O}(n^2)$

Asynchronous Byzantine Agreement (ABA)



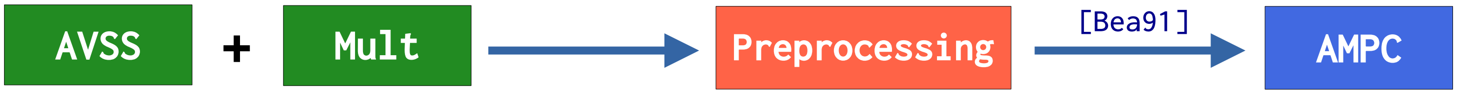
- Perfectly-Secure

- Generalization of [CR93]
- Success Probability $> 1/n$
  Depends on largest set in $\mathcal{Z}$

- Terminates with probability 1
- Expected Running Time
  $R = \mathcal{O}(n^2)$

The MPC Protocol

The MPC Protocol



The MPC Protocol

Mult

The MPC Protocol

$[a]$ $[b]$ Mult

The MPC Protocol

$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$

The MPC Protocol

$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

The MPC Protocol

$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$

$a^{(1)}$

$b^{(3)}$

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

The MPC Protocol

$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$

$\{P_1, P_2\}$

P_3, P_4
P_5, P_6, P_7

$a^{(1)}$

$b^{(3)}$

P_2, P_3
P_5, P_6, P_7

$\{P_1, P_4\}$

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

The MPC Protocol

$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$

$\{P_1, P_2\}$

$\mathcal{Q}^{(3)}$ P_3, P_4
P_5, P_6, P_7

$a^{(1)}$

$b^{(3)}$

P_2, P_3
$\mathcal{Q}^{(3)}$ P_5, P_6, P_7

$\{P_1, P_4\}$

$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

The MPC Protocol

$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m) \in \{1 \ldots q\} \times \{1 \ldots q\}} [a^{(l)} \cdot b^{(m)}]$

$\{P_1, P_2\}$

$\mathcal{Q}^{(3)}$ P_3, P_4
P_5, P_6, P_7

$a^{(1)}$

P_3, P_5
P_6, P_7

$b^{(3)}$

P_2, P_3
P_5, P_6, P_7 $\mathcal{Q}^{(3)}$

$\{P_1, P_4\}$

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

The MPC Protocol

$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m) \in \{1 \ldots q\} \times \{1 \ldots q\}} [a^{(l)} \cdot b^{(m)}]$

$\{P_1, P_2\}$

$\mathcal{Q}^{(3)}$ P_3, P_4 P_5, P_6, P_7

$\mathcal{Q}^{(2)}$

$a^{(1)}$

P_3, P_5 P_6, P_7

$b^{(3)}$

P_2, P_3 P_5, P_6, P_7 $\mathcal{Q}^{(3)}$

$\{P_1, P_4\}$

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

The MPC Protocol

$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$

$\{P_1, P_2\}$

$\mathcal{Q}^{(3)}$ P_3, P_4 P_5, P_6, P_7

$\mathcal{Q}^{(2)}$

$a^{(1)}$

P_3, P_5 P_6, P_7

$b^{(3)}$

P_2, P_3 P_5, P_6, P_7 $\mathcal{Q}^{(3)}$

$\{P_1, P_4\}$

P_i

$[\, a^{(1)} \cdot b^{(3)} \,]$

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

The MPC Protocol

$[a]$ $[b]$ **Mult** $$[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$$

$\{P_1, P_2\}$

$\mathcal{Q}^{(3)}$ P_3, P_4 P_5, P_6, P_7

$\mathcal{Q}^{(2)}$

$a^{(1)}$

$b^{(3)}$

P_3, P_5 P_6, P_7 $\rightarrow$ P_3, P_5 P_6

$\{P_7\}$

P_2, P_3 P_5, P_6, P_7 $\mathcal{Q}^{(3)}$

P_i

$\{P_1, P_4\}$

$[a^{(1)} \cdot b^{(3)}]$

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

The MPC Protocol

$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m) \in \{1 \ldots q\} \times \{1 \ldots q\}} [a^{(l)} \cdot b^{(m)}]$

$\{P_1, P_2\}$

$\mathcal{Q}^{(3)}$ P_3, P_4 P_5, P_6, P_7

$a^{(1)}$

$b^{(3)}$

$\mathcal{Q}^{(3)}$ P_2, P_3 P_5, P_6, P_7

$\{P_1, P_4\}$

$\mathcal{Q}^{(2)}$

P_3, P_5 P_6, P_7

P_i

$[\, a^{(1)} \cdot b^{(3)} \,]$

n

ABA . . . ABA

ACS

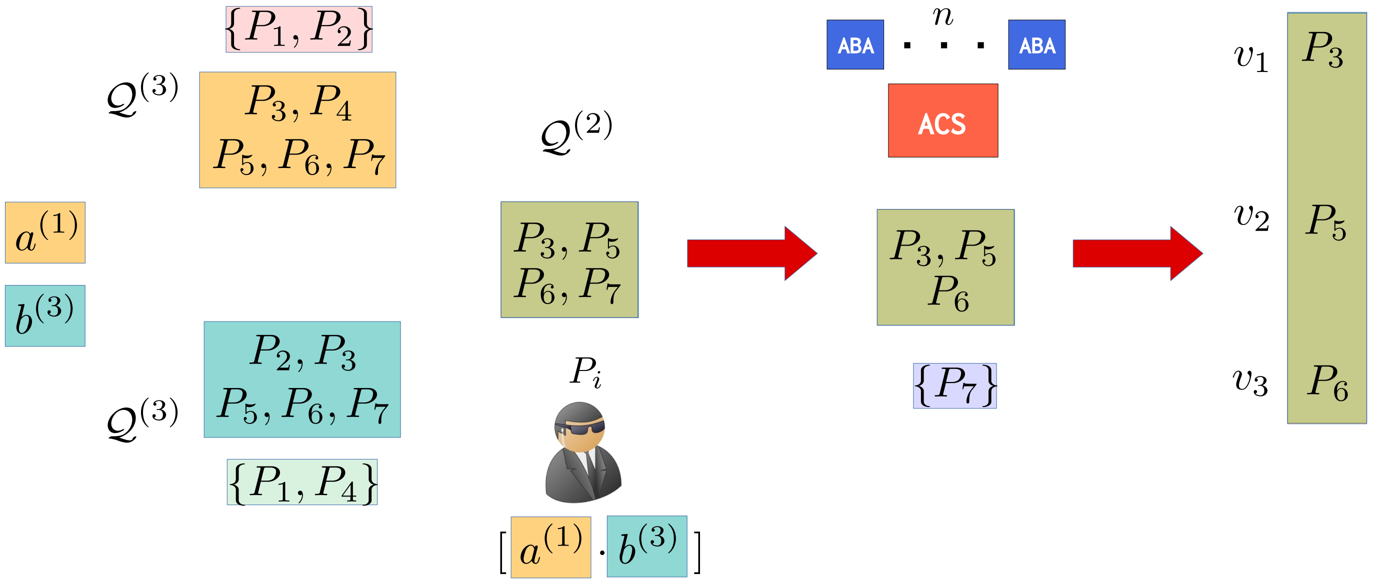
P_3, P_5 P_6

$\{P_7\}$

$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

The MPC Protocol

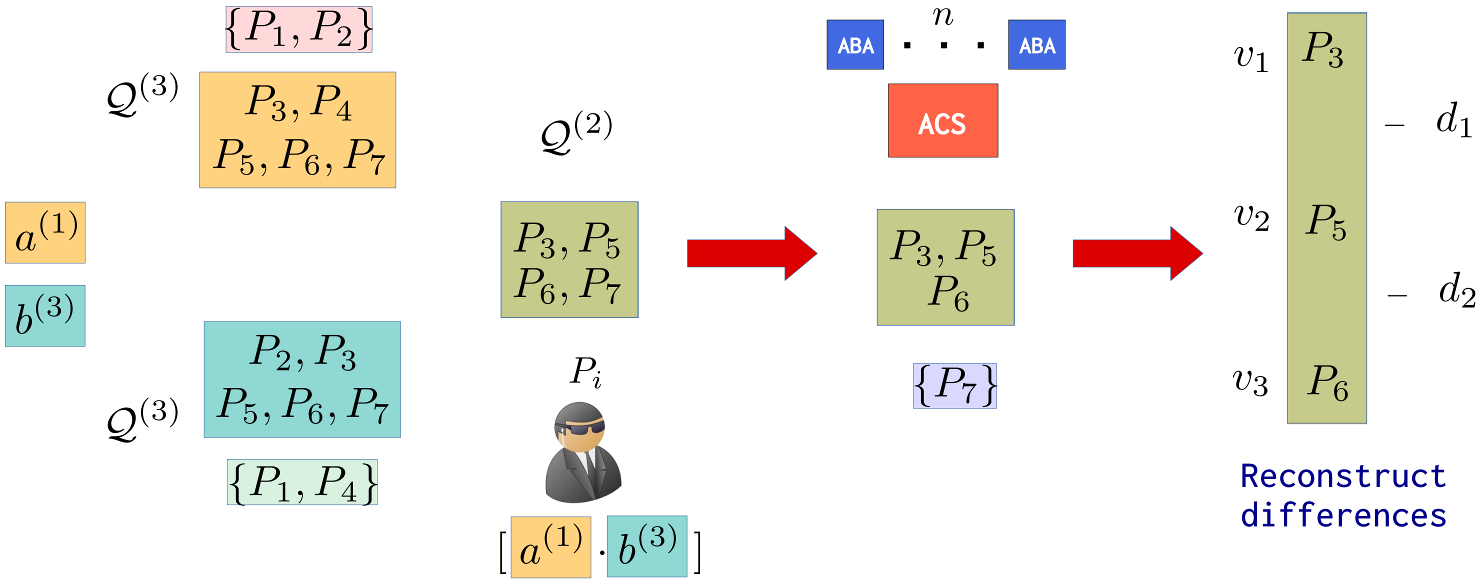
$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$



$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

The MPC Protocol

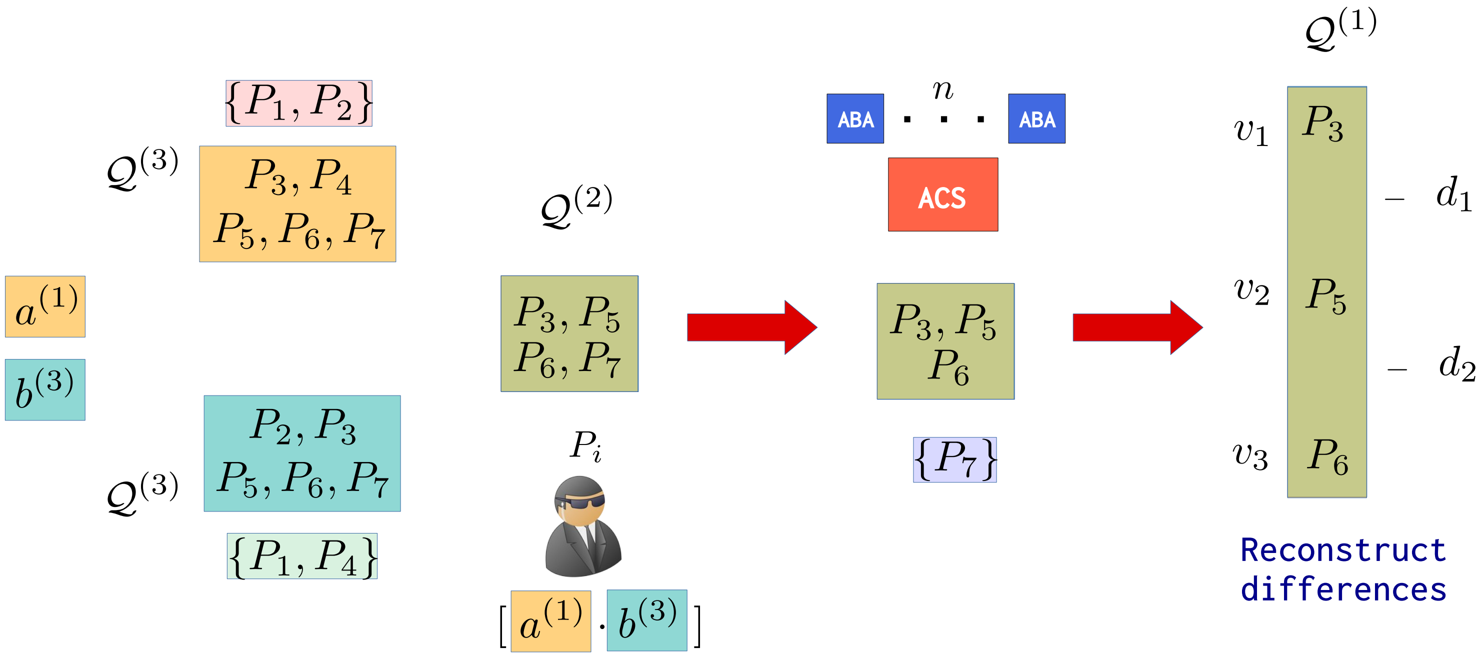
$[a]$ $[b]$ **Mult** $$[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$$



$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

The MPC Protocol

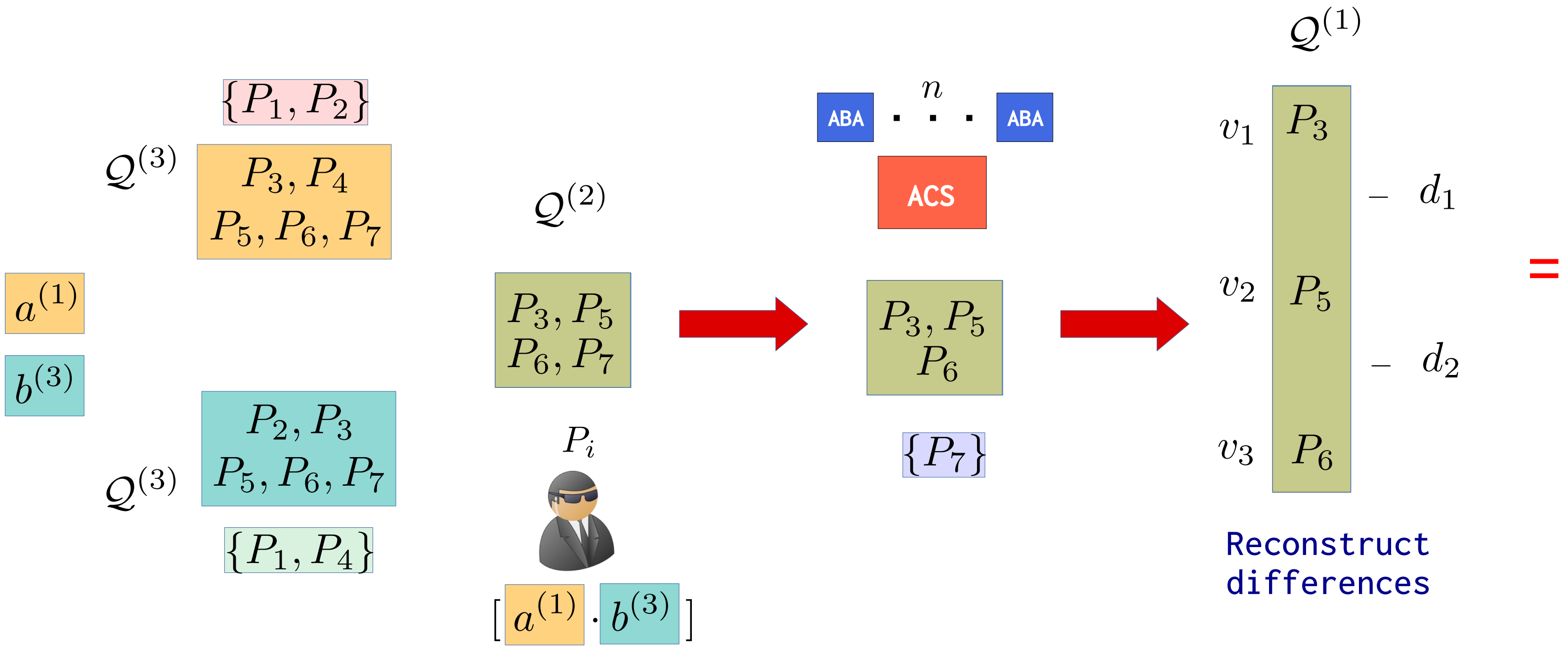
$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$



$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

The MPC Protocol

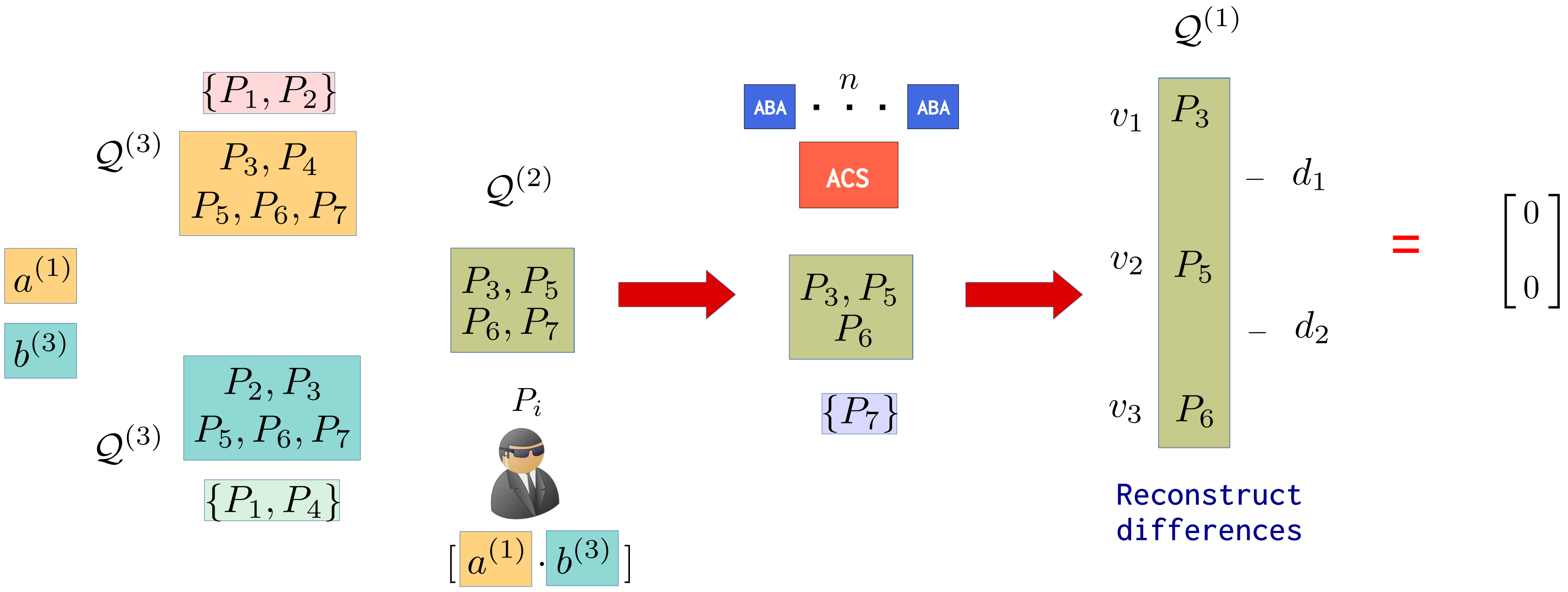
$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$



$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

The MPC Protocol

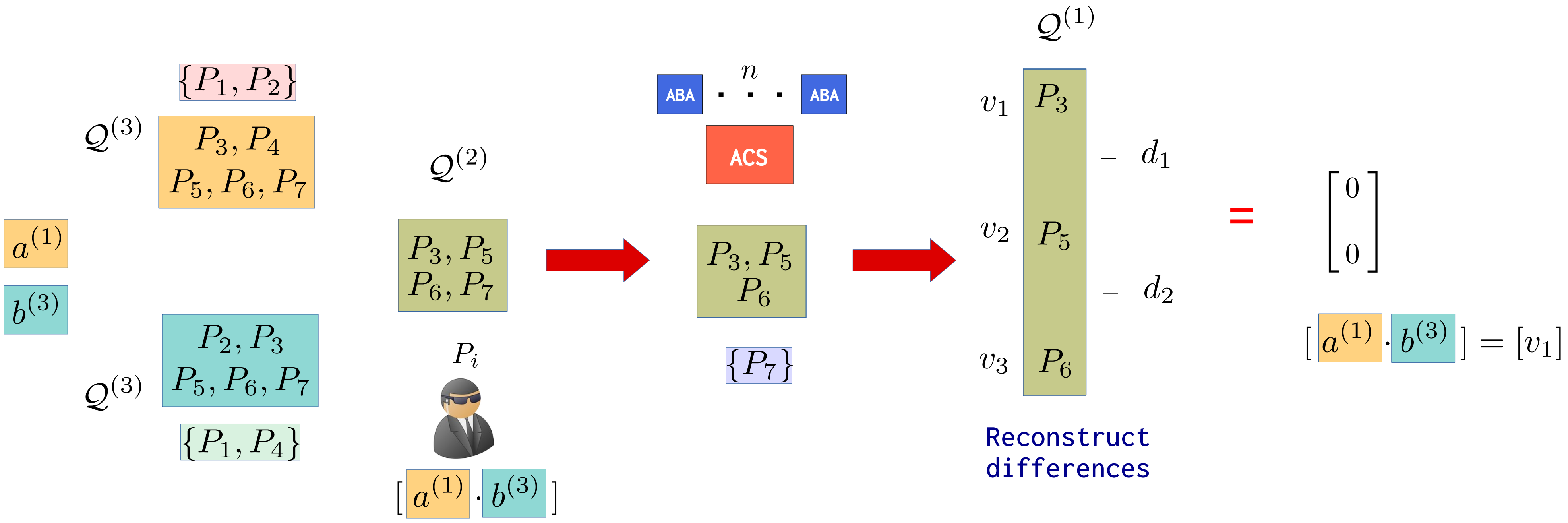
$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$



$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

The MPC Protocol

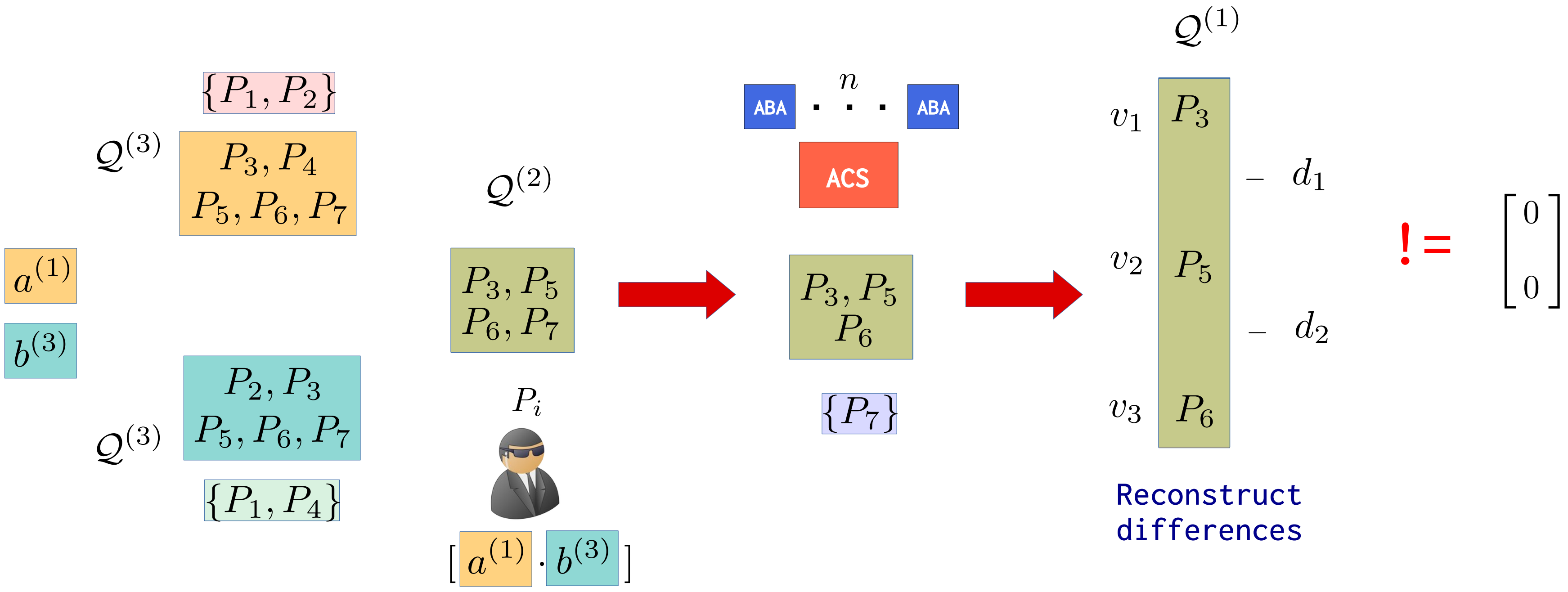
$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$



$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$

The MPC Protocol

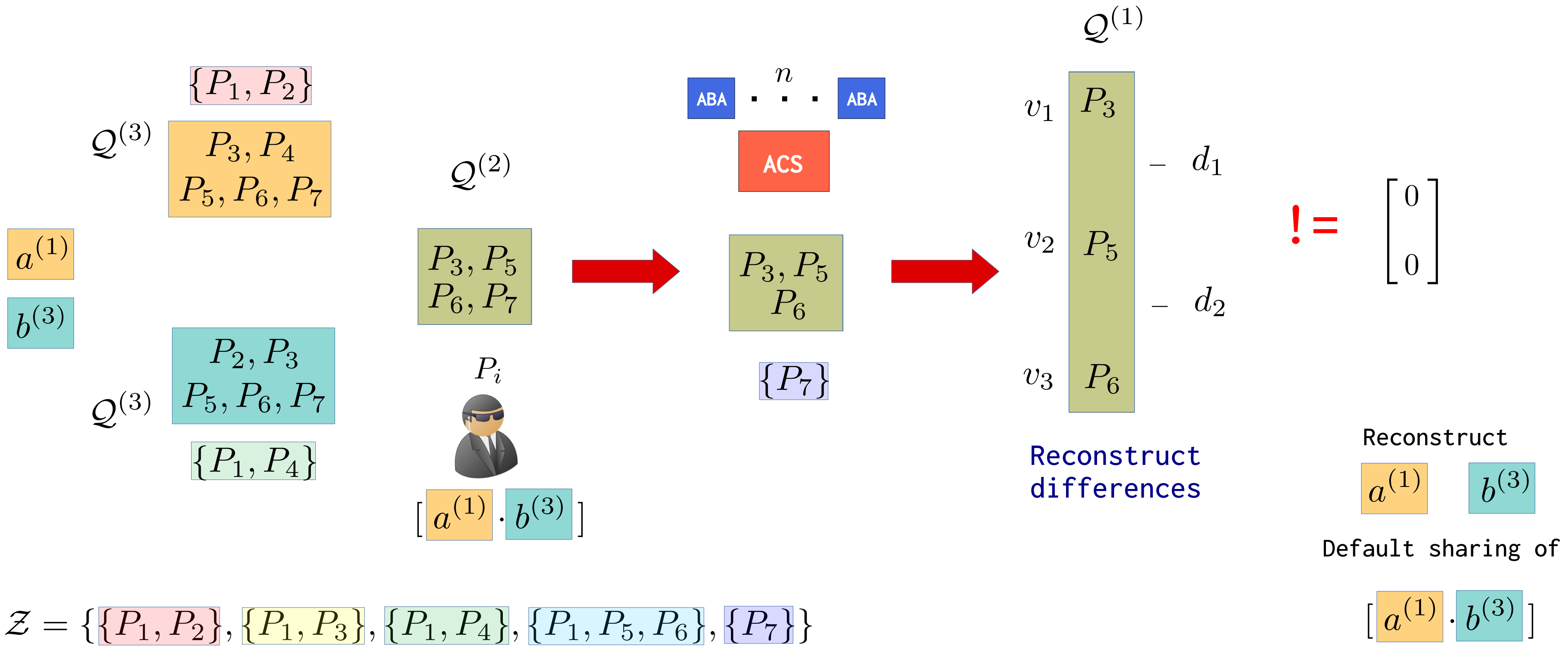
$[a]$ $[b]$ **Mult** $$[a \cdot b] = \sum_{(l,m) \in \{1 \ldots q\} \times \{1 \ldots q\}} [a^{(l)} \cdot b^{(m)}]$$



$$\mathcal{Z} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_1, P_5, P_6\}, \{P_7\}\}$$

The MPC Protocol

$[a]$ $[b]$ **Mult** $[a \cdot b] = \sum_{(l,m)\in\{1\ldots q\}\times\{1\ldots q\}} [a^{(l)} \cdot b^{(m)}]$



Conclusion

Conclusion

Summary:

Conclusion

Summary:

We studied AMPC tolerant to general adversaries.

Conclusion

Summary:

We studied AMPC tolerant to general adversaries.

- Flaw in the MPC protocol of [KSR02]

Conclusion

Summary:

We studied AMPC tolerant to general adversaries.

- Flaw in the MPC protocol of [KSR02]
- Perfectly-Secure AVSS and AMPC protocols

Conclusion

Summary:

We studied AMPC tolerant to general adversaries.

- Flaw in the MPC protocol of [KSR02]
- Perfectly-Secure AVSS and AMPC protocols
- ABA Protocol (Generalization of [CR93])

Conclusion

Summary:

We studied AMPC tolerant to general adversaries.

- Flaw in the MPC protocol of [KSR02]
- Perfectly-Secure AVSS and AMPC protocols
- ABA Protocol (Generalization of [CR93])

Future Directions:

Conclusion

Summary:

We studied AMPC tolerant to general adversaries.

- Flaw in the MPC protocol of [KSR02]
- Perfectly-Secure AVSS and AMPC protocols
- ABA Protocol (Generalization of [CR93])

Future Directions:

- Improving Communication Complexity

Conclusion

Summary:

We studied AMPC tolerant to general adversaries.

- Flaw in the MPC protocol of [KSR02]
- Perfectly-Secure AVSS and AMPC protocols
- ABA Protocol (Generalization of [CR93])

Future Directions:

- Improving Communication Complexity
- Monotone Span Program based Protocols

Conclusion

Summary:

We studied AMPC tolerant to general adversaries.

- Flaw in the MPC protocol of [KSR02]
- Perfectly-Secure AVSS and AMPC protocols
- ABA Protocol (Generalization of [CR93])

Future Directions:

- Improving Communication Complexity
- Monotone Span Program based Protocols
- Efficient Non-Optimally Resilient Protocols

Conclusion

Summary:

We studied AMPC tolerant to general adversaries.

- Flaw in the MPC protocol of [KSR02]
- Perfectly-Secure AVSS and AMPC protocols
- ABA Protocol (Generalization of [CR93])

Future Directions:

- Improving Communication Complexity
- Monotone Span Program based Protocols
- Efficient Non-Optimally Resilient Protocols
- Statistical and Computational Security

Conclusion

Summary:

We studied AMPC tolerant to general adversaries.

- Flaw in the MPC protocol of [KSR02]
- Perfectly-Secure AVSS and AMPC protocols
- ABA Protocol (Generalization of [CR93])

Future Directions:

- Improving Communication Complexity
- Monotone Span Program based Protocols
- Efficient Non-Optimally Resilient Protocols
- Statistical and Computational Security

Thanks!