Trident: Efficient 4PC Framework for Privacy Preserving Machine Learning

Harsh Chaudhari*, Rahul Rachuri^ and **Ajith Suresh***

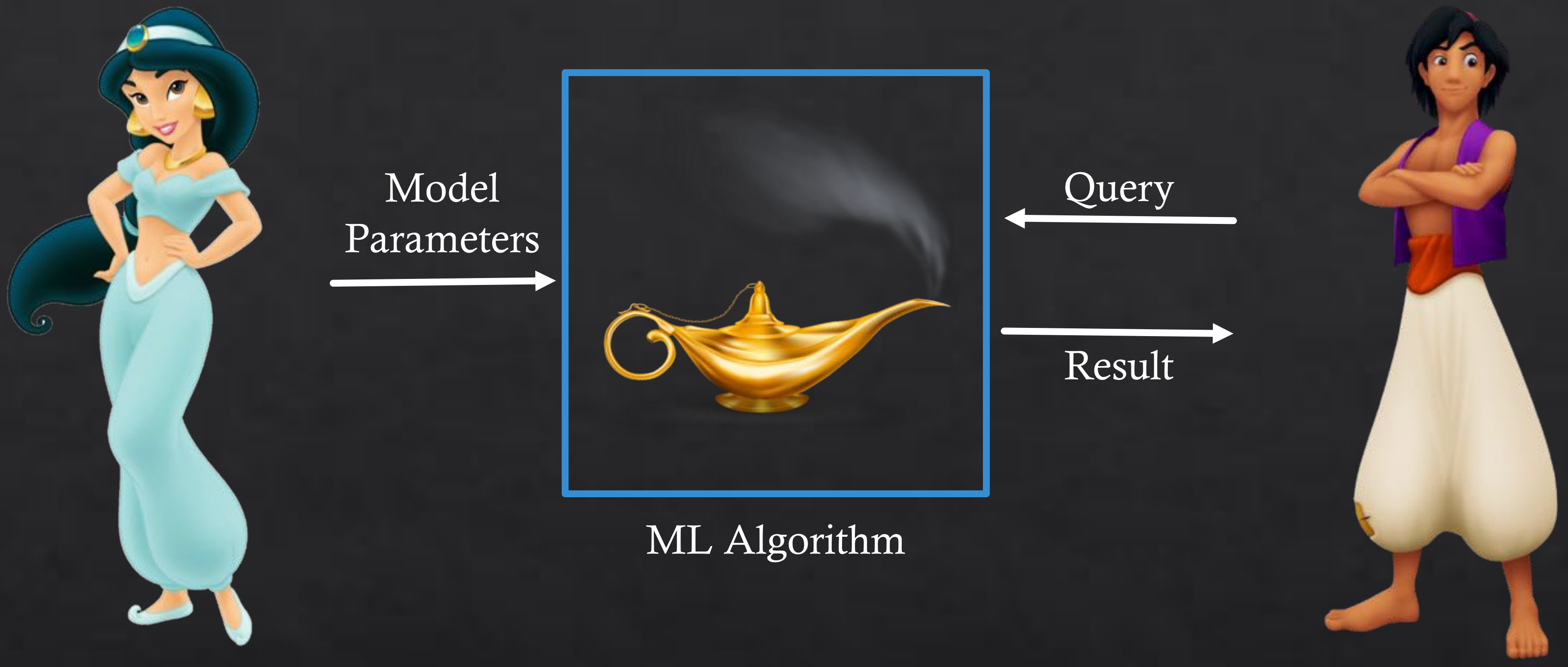
* Indian Institute of Science (IISc), Bangalore
^ Aarhus University, Denmark

Ajith Suresh
CrIS Lab, IISc
https://www.csa.iisc.ac.in/~cris

Outline

- ❑ Privacy Preserving Machine Learning (PPML)
- ❑ Secure Multi-party Computation (MPC)
- ❑ Overview of Trident Protocol
- ❑ Benchmarking Results

Machine Learning (ML) Prediction – An Abstraction



Model Parameters

Query

Result

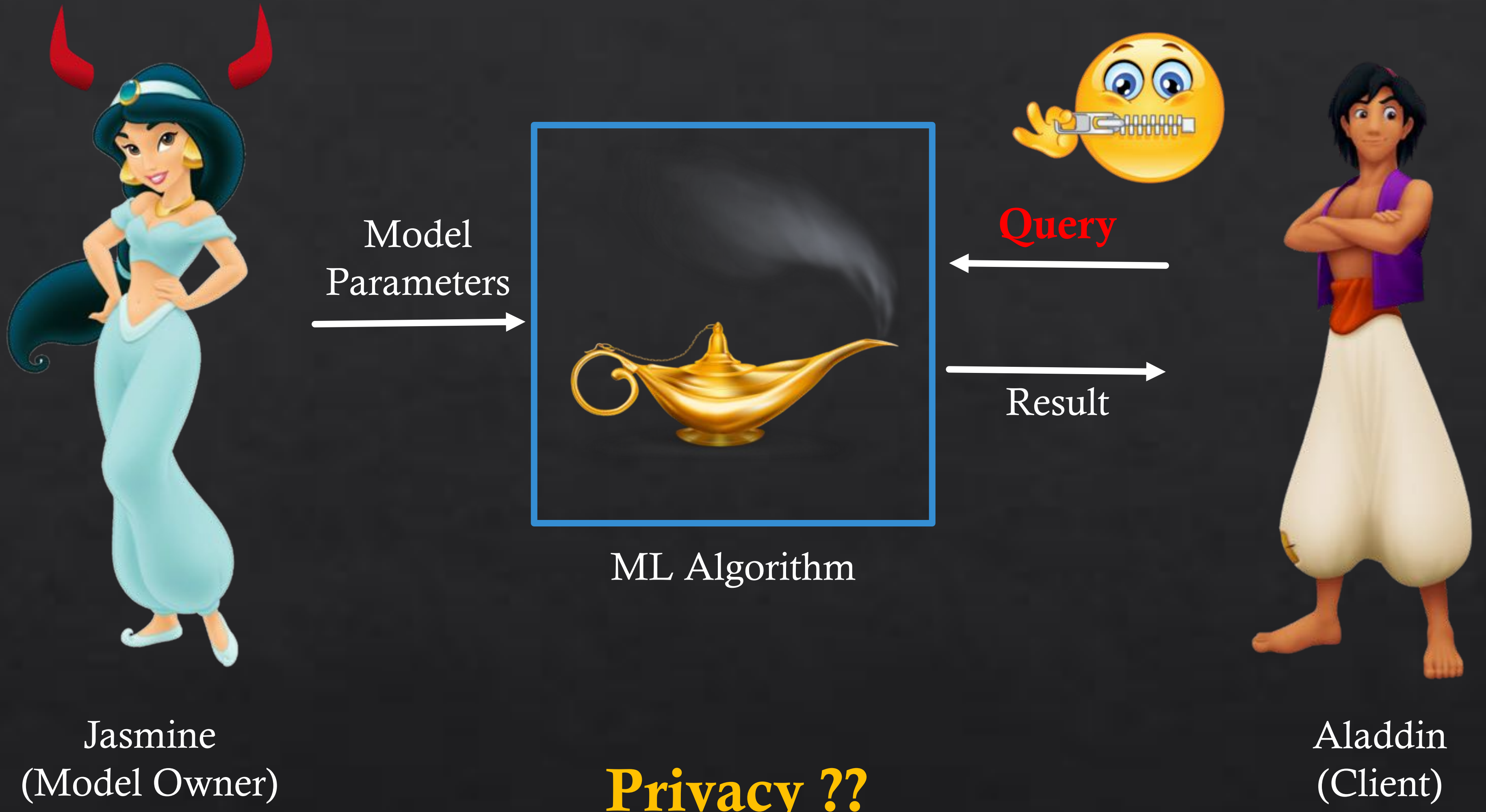
ML Algorithm

Jasmine
(Model Owner)

Aladdin
(Client)

Privacy ??

Machine Learning (ML) Prediction – An Abstraction



Model Parameters

ML Algorithm

Query

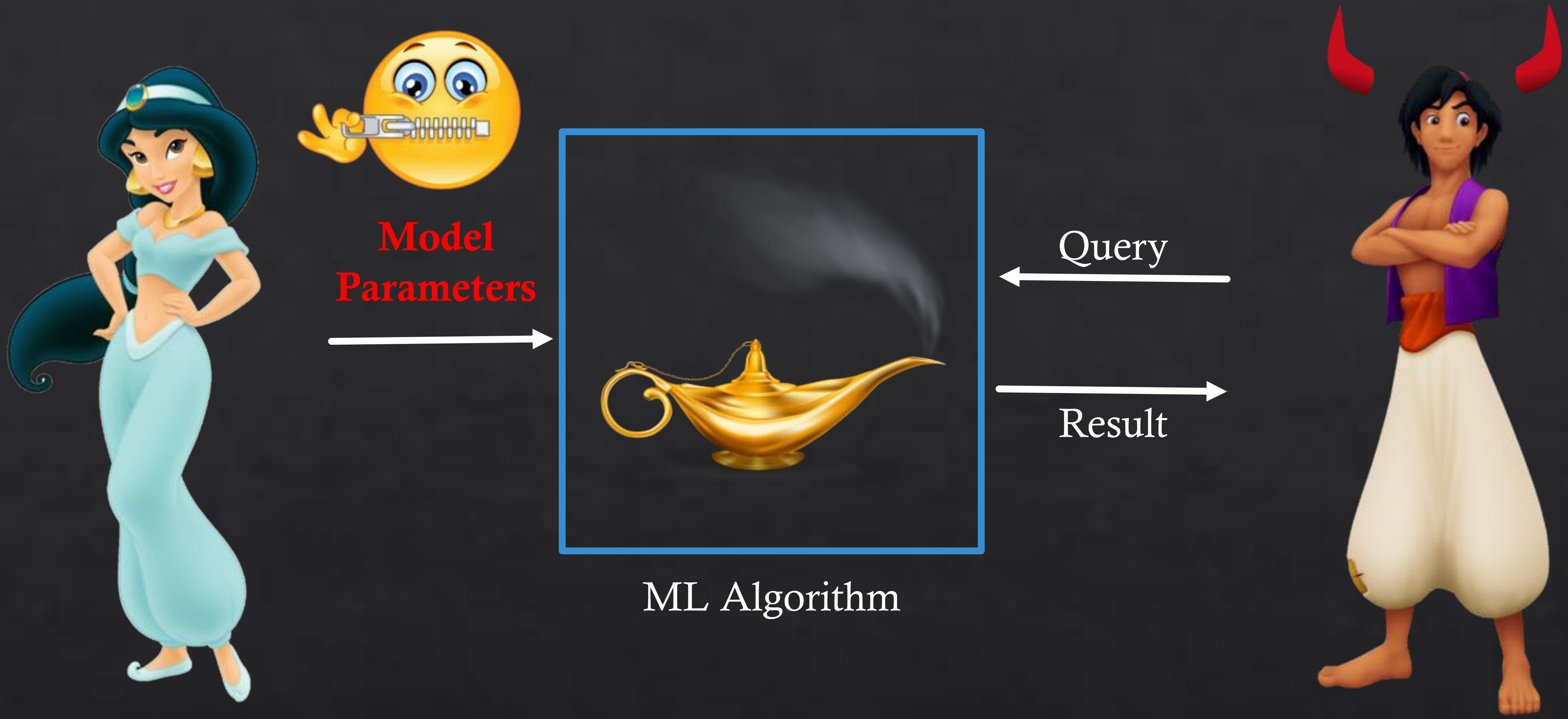
Result

Jasmine
(Model Owner)

Aladdin
(Client)

Privacy ??

Machine Learning (ML) Prediction – An Abstraction



Model Parameters

Query

Result

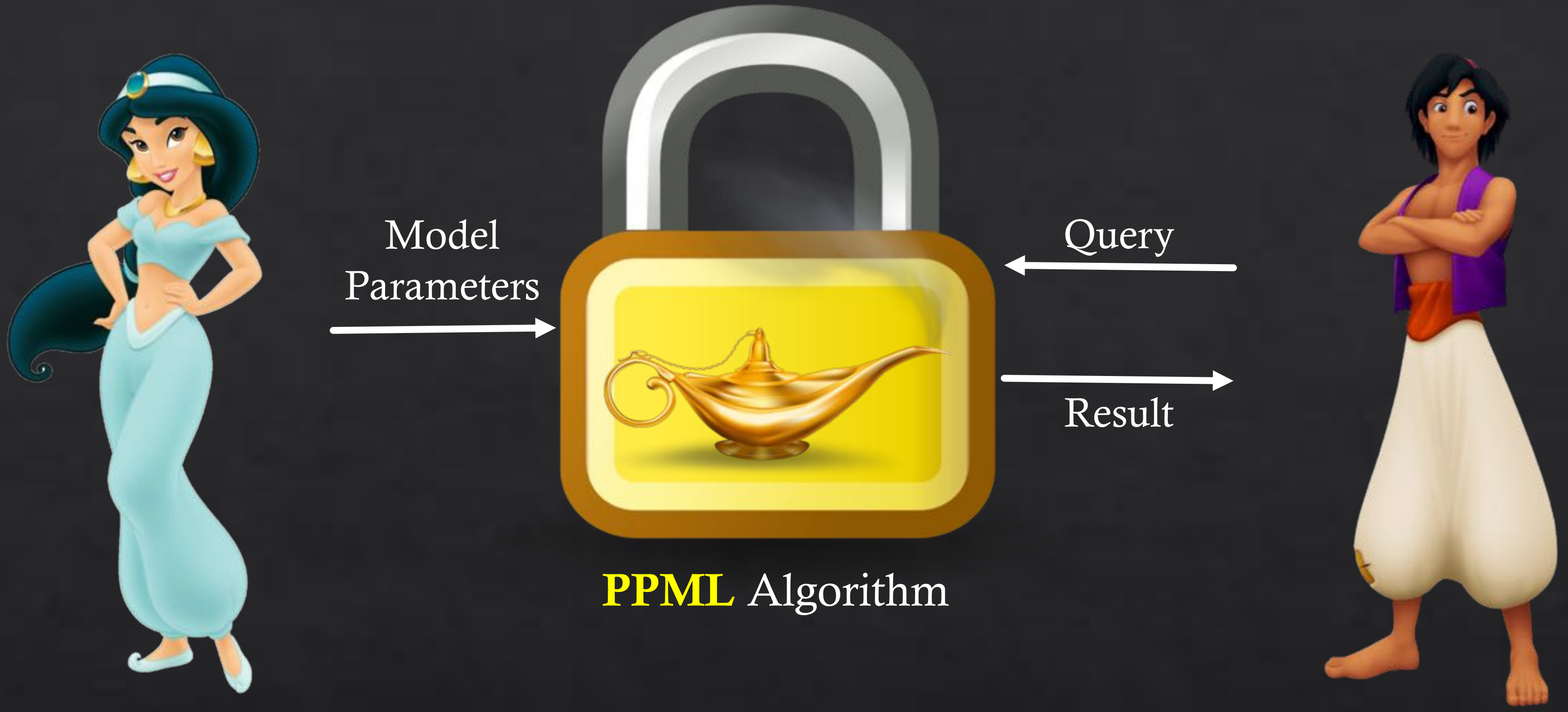
ML Algorithm

Jasmine
(Model Owner)

Aladdin
(Client)

Privacy ??

Privacy Preserving Machine Learning (PPML)



Model Parameters

Query

Result

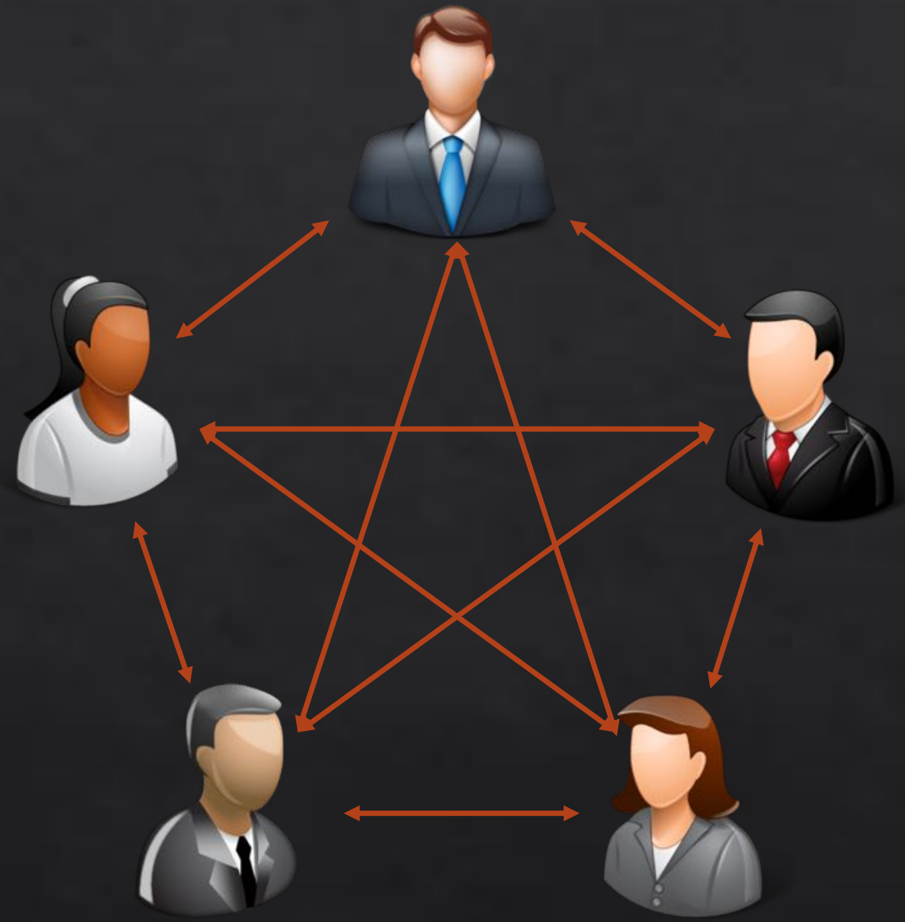
PPML Algorithm

Jasmine
(Model Owner)

Aladdin
(Client)

MPC meets ML

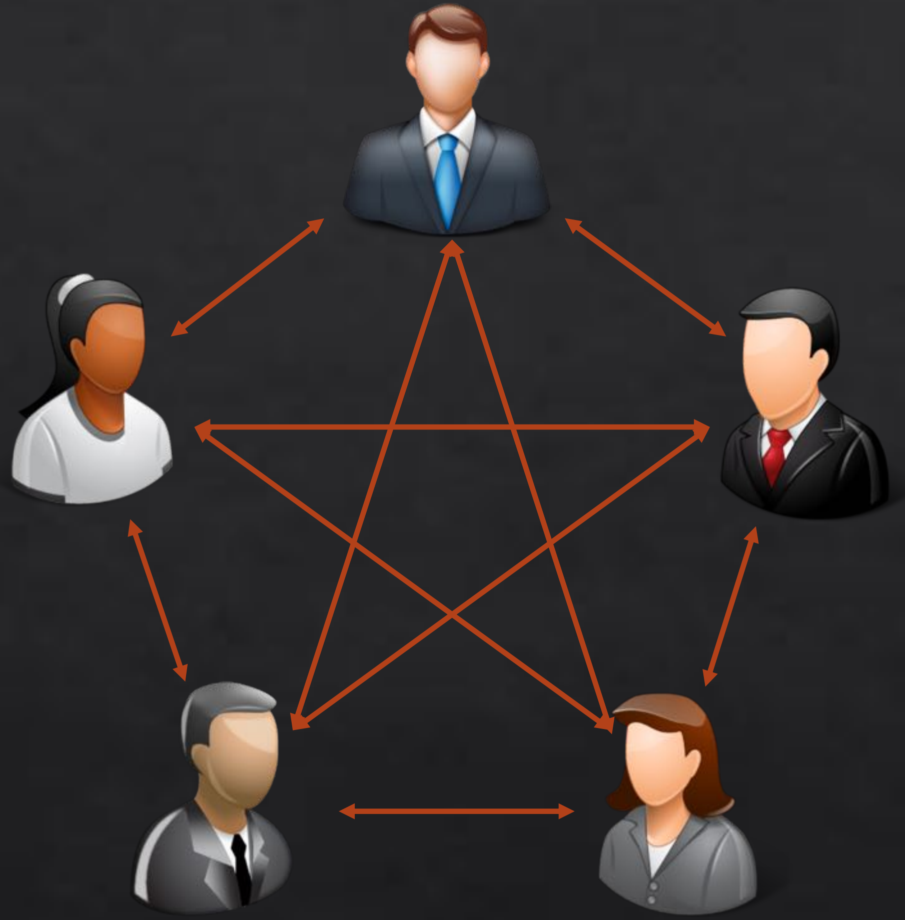
Secure Multi-party Computation (MPC) [Yao’82]



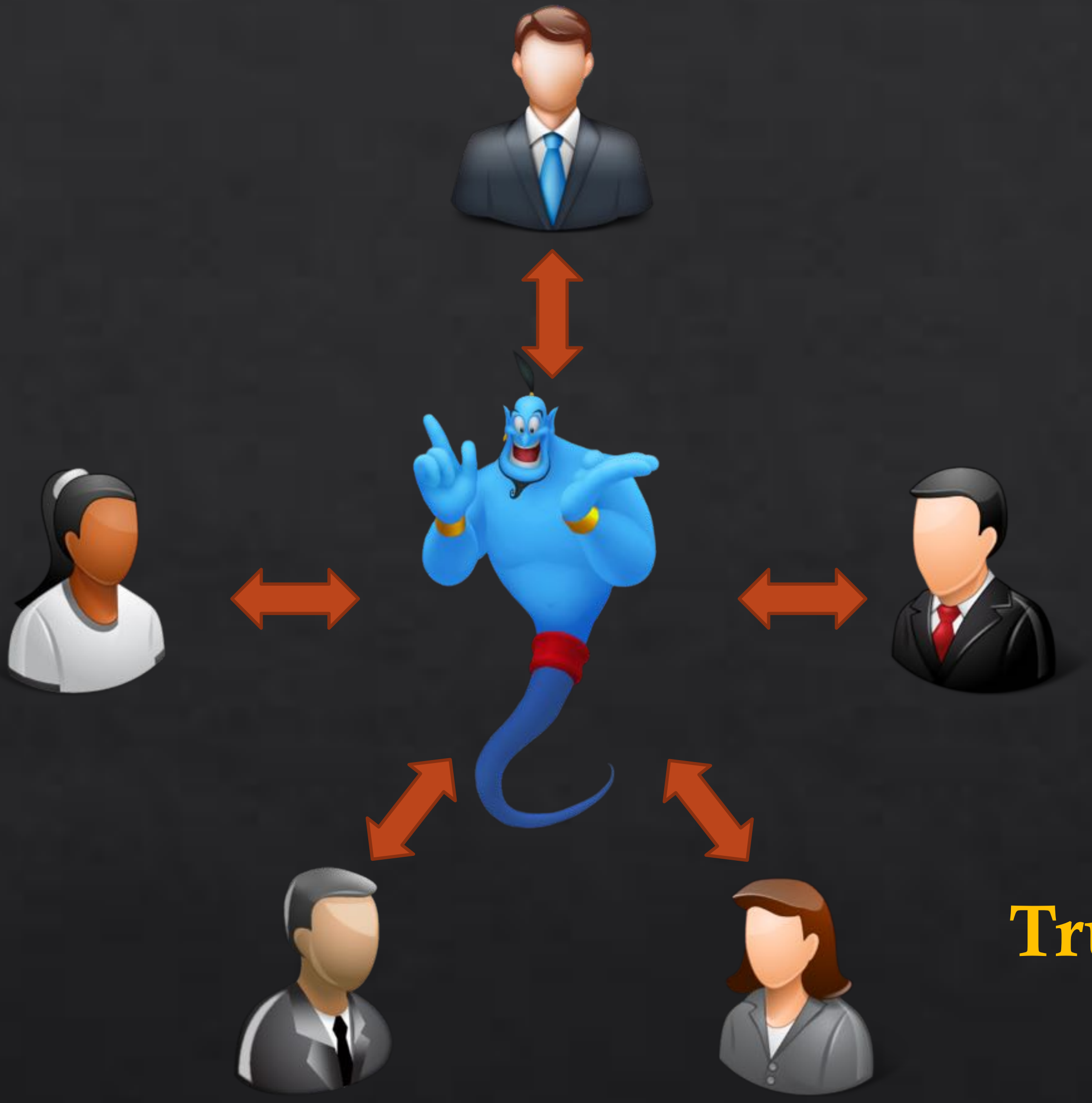
- ✓ A set of parties with private inputs wish to compute some joint function of their inputs.

- ✓ Goals of MPC:
  - **Correctness** – Parties should correctly evaluate the function output.
  - **Privacy** – Nothing more than the function output should be revealed

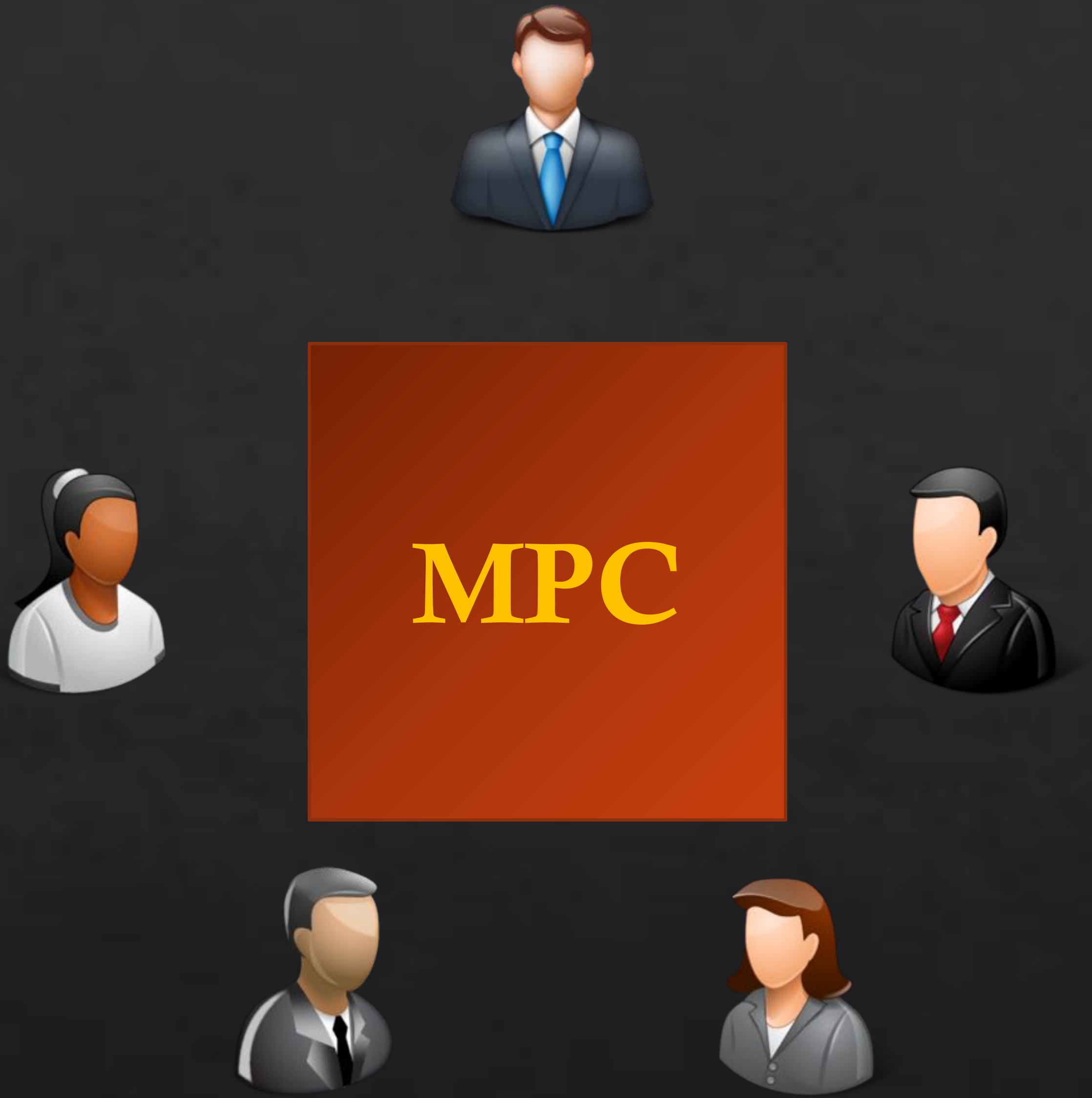
Secure Multi-party Computation (MPC) [Yao'82]



Trusted Third Party (TTP)



Trusted Third Party (TTP)



MPC emulates TTP

TRIDENT PROTOCOL

Trident protocol

- A new 4PC protocol over ring in the pre-processing model

Trident protocol

- A new **4PC protocol** over ring in the pre-processing model

  - 4 parties
  - Honest majority
  - At most 1 corruption

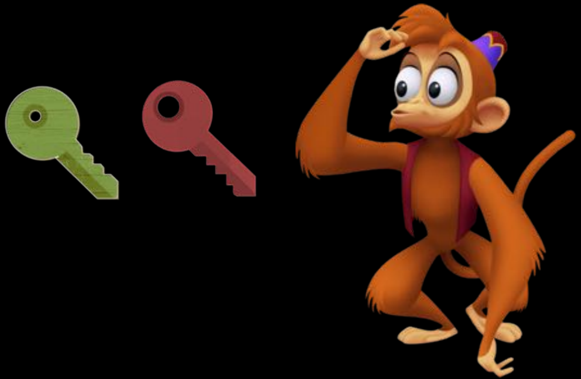
Trident protocol

- A new 4PC protocol over ring in the **pre-processing** model

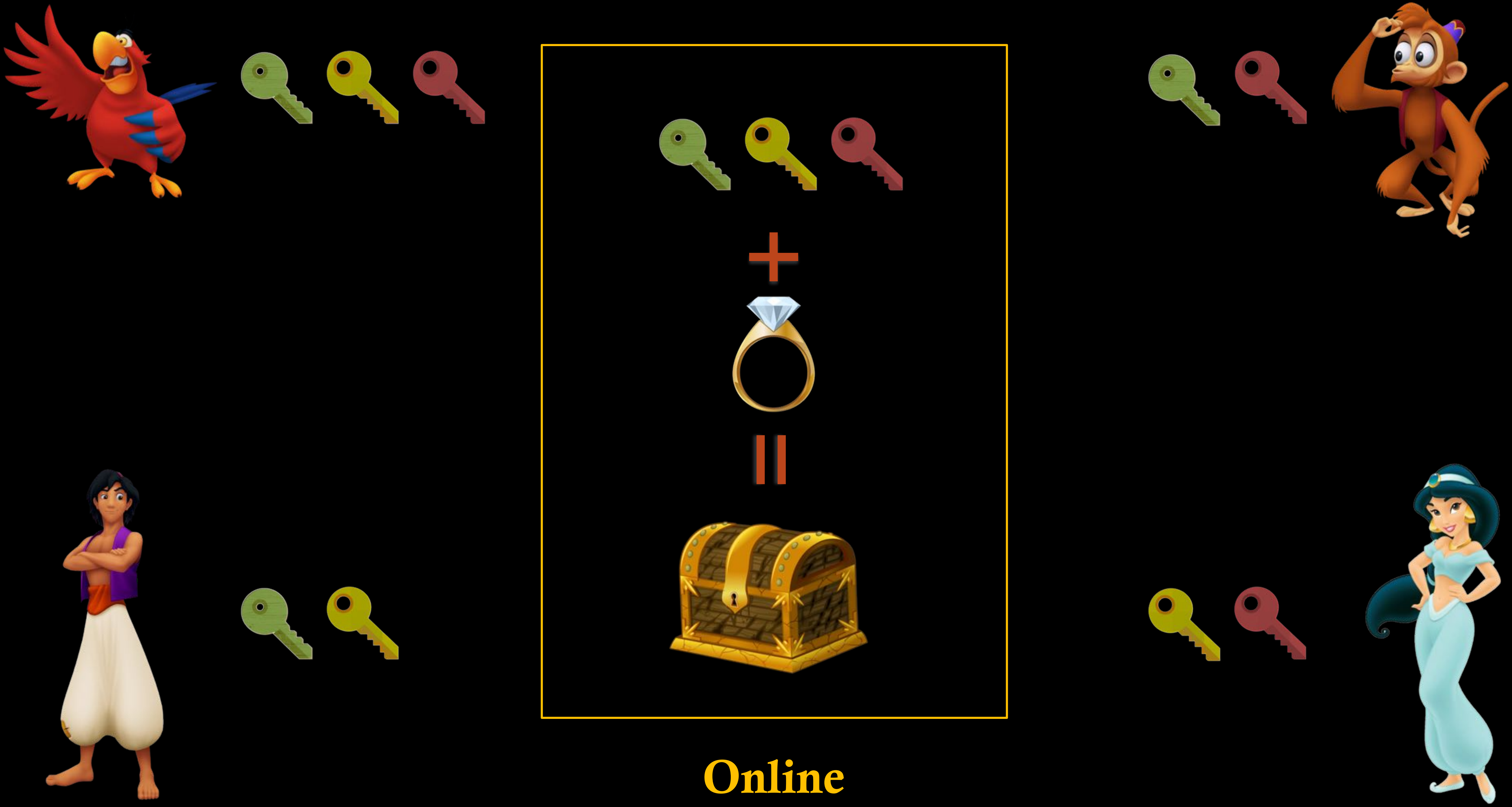
  - Data independent pre-processing
  - Fast online phase

Sharing Semantics

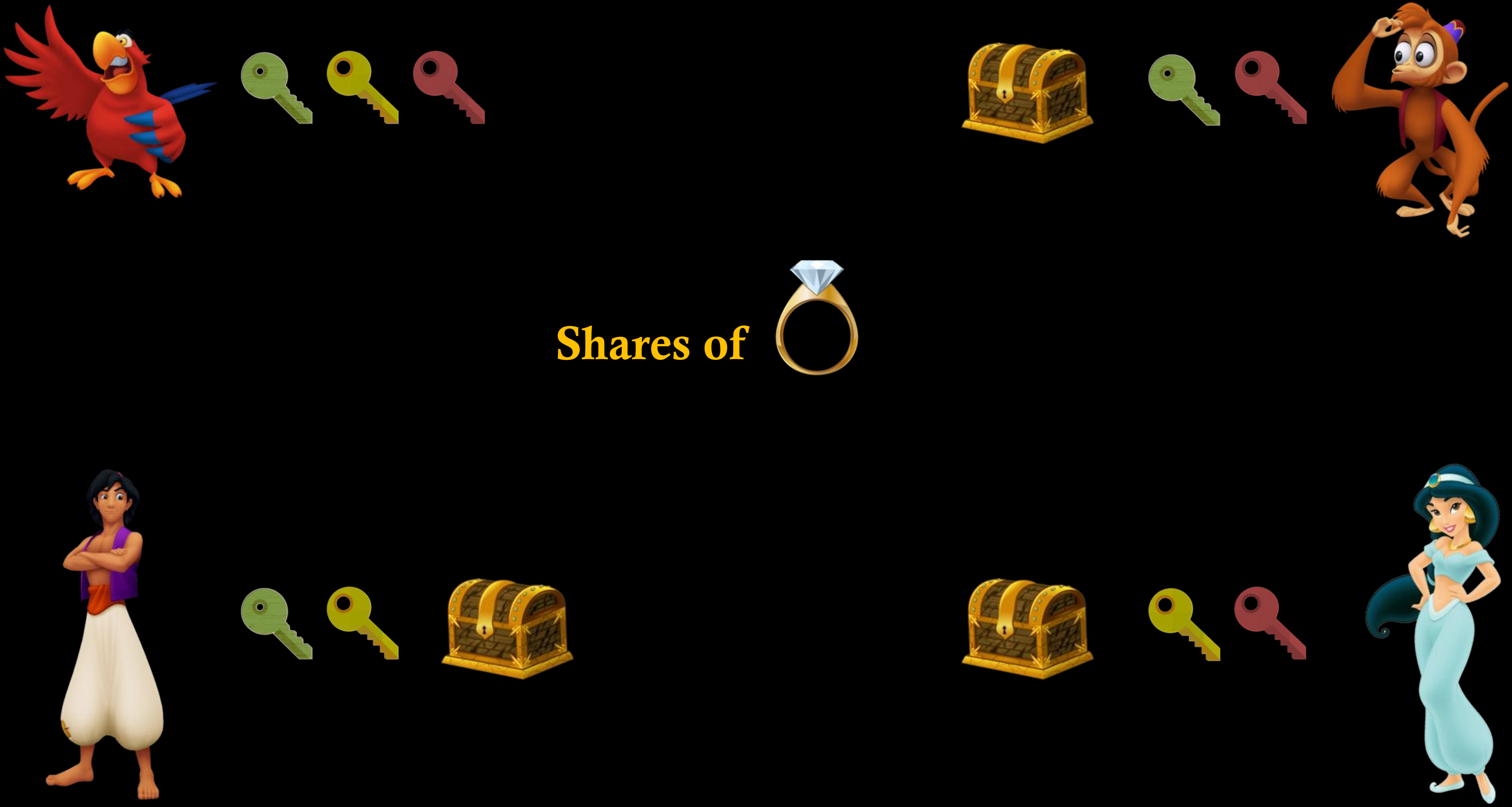
Pre-processing



Pre-processing



Online



Shares of 💍

Trident protocol

- A new 4PC protocol over ring in the pre-processing model
- Malicious security with guarantee of fairness

Trident protocol

- A new 4PC protocol over ring in the pre-processing model
- **Malicious** security with guarantee of fairness

Corrupt parties arbitrarily deviate

Trident protocol

- A new 4PC protocol over ring in the pre-processing model
- Malicious security with guarantee of **fairness**

Honest parties get output whenever corrupt parties get output

Multiplication $(x.y)$

Ref	Pre-processing (#elements)	Online (#elements)	Security
Araki et al'17 (3PC)	12	9	Abort

Multiplication $(x.y)$

Ref	Pre-processing (#elements)	Online (#elements)	Security
Araki et al’17 (3PC)	12	9	Abort
ASTRA (3PC)	21	4	Fair

Multiplication $(x.y)$

Ref	Pre-processing (#elements)	Online (#elements)	Security
Araki et al’17 (3PC)	12	9	Abort
ASTRA (3PC)	21	4	Fair
Gordon et al.’18 (4PC)	2	4	Abort

Multiplication $(x.y)$

Ref	Pre-processing (#elements)	Online (#elements)	Security
Araki et al’17 (3PC)	12	9	Abort
ASTRA (3PC)	21	4	Fair
Gordon et al.’18 (4PC)	2	4	Abort
Trident	**3**	**3**	**Fair**

Trident protocol

- A new 4PC protocol over ring in the pre-processing model
- Malicious security with guarantee of fairness
- Efficient Mixed World Conversions

Mixed World Conversions

Boolean

Boolean World

- Comparison, Bit Extraction …

Mixed World Conversions

Boolean

Arithmetic

Boolean World

- Comparison, Bit Extraction …

Arithmetic World

- Addition, Multiplication …

Mixed World Conversions

Boolean

Arithmetic

Garbled

Boolean World

- Comparison, Bit Extraction …

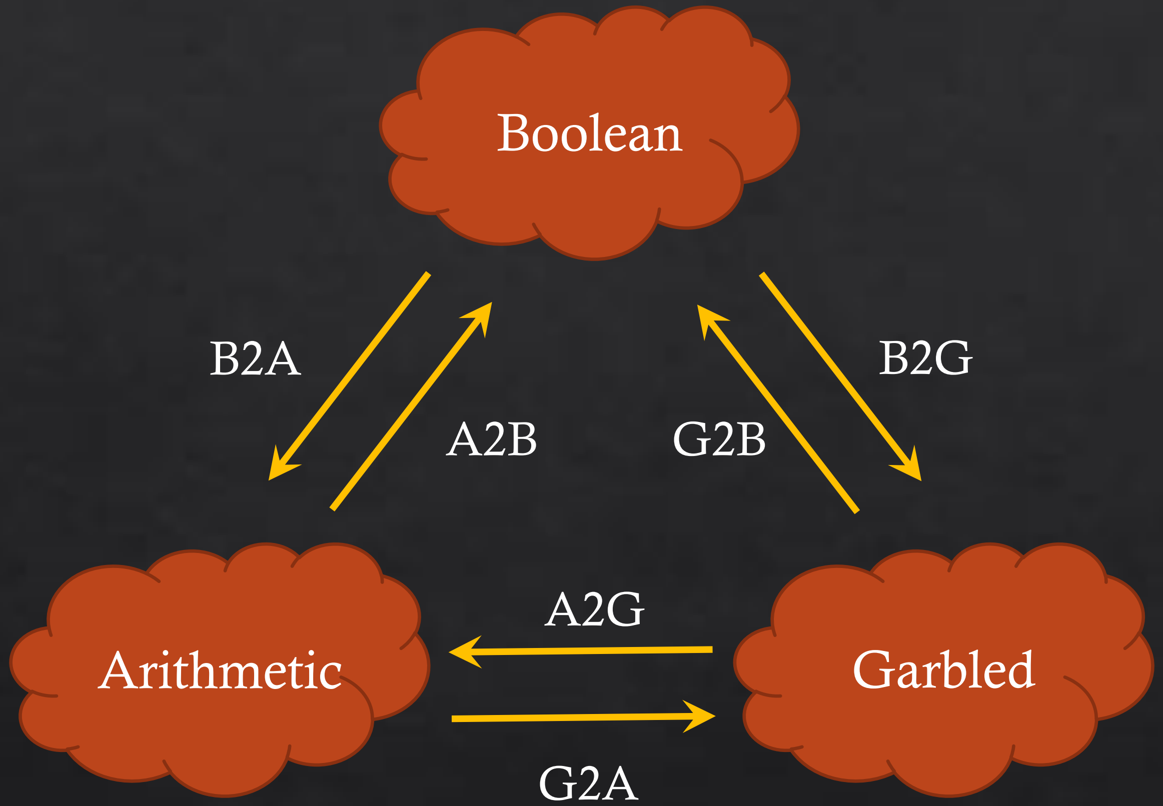
Arithmetic World

- Addition, Multiplication …

Garbled World

- Division over rings …

Mixed World Conversions



Online Rounds	Online Communication
Up to 7x	2x - 67x

Range of improvement over ABY3

Mixed World Conversions – An Example

$$\frac{\min(x_1 + x_2, x_3)}{x_4}$$

Mixed World Conversions – An Example

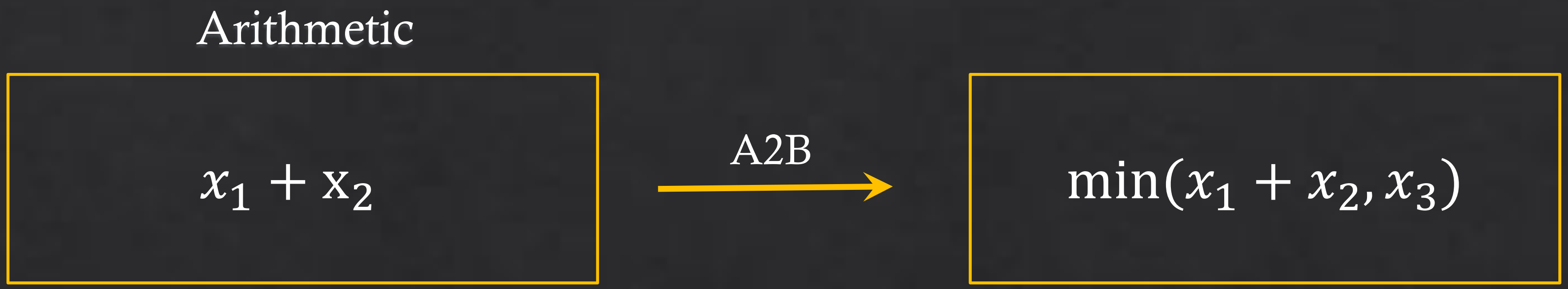
$$x_1 + \mathrm{x}_2$$

Mixed World Conversions – An Example

Arithmetic

$$x_1 + \mathrm{x}_2$$

Mixed World Conversions – An Example



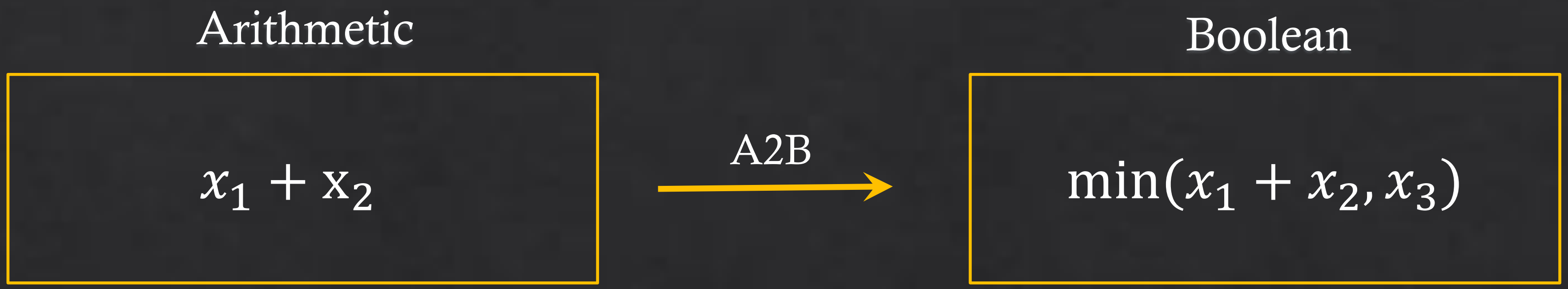
Arithmetic

$x_1 + \mathrm{x}_2$

A2B

$\min(x_1 + x_2, x_3)$

Mixed World Conversions – An Example



Arithmetic

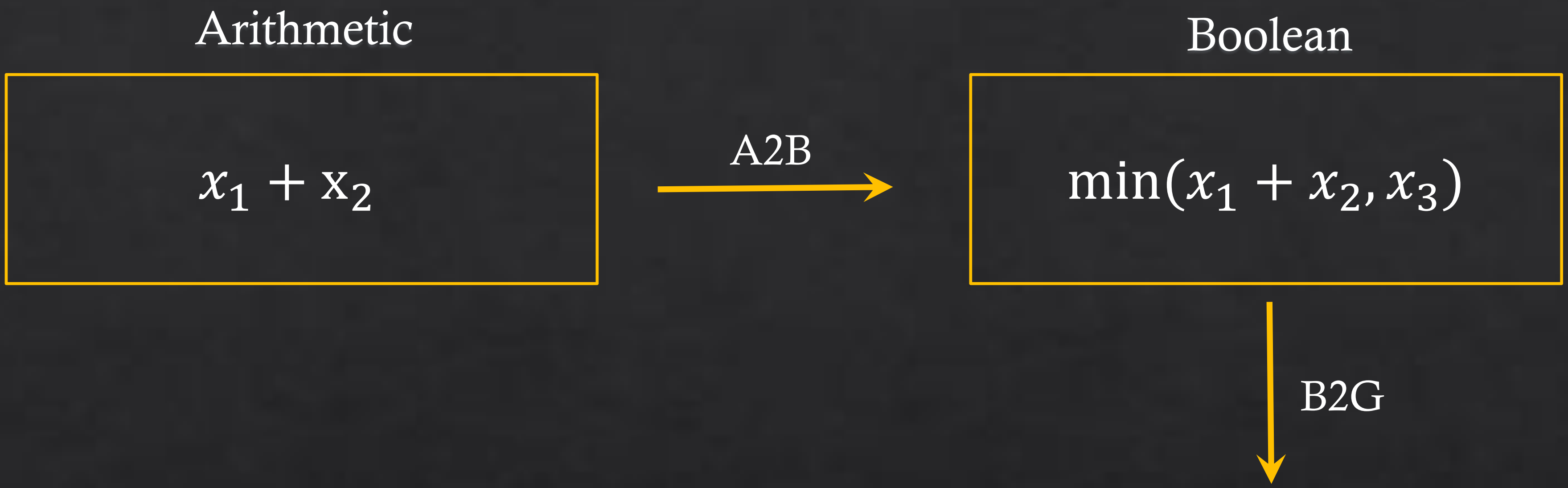
$x_1 + \mathrm{x}_2$

A2B

Boolean

$\min(x_1 + x_2, x_3)$

Mixed World Conversions – An Example



Arithmetic

$x_1 + \mathrm{x}_2$

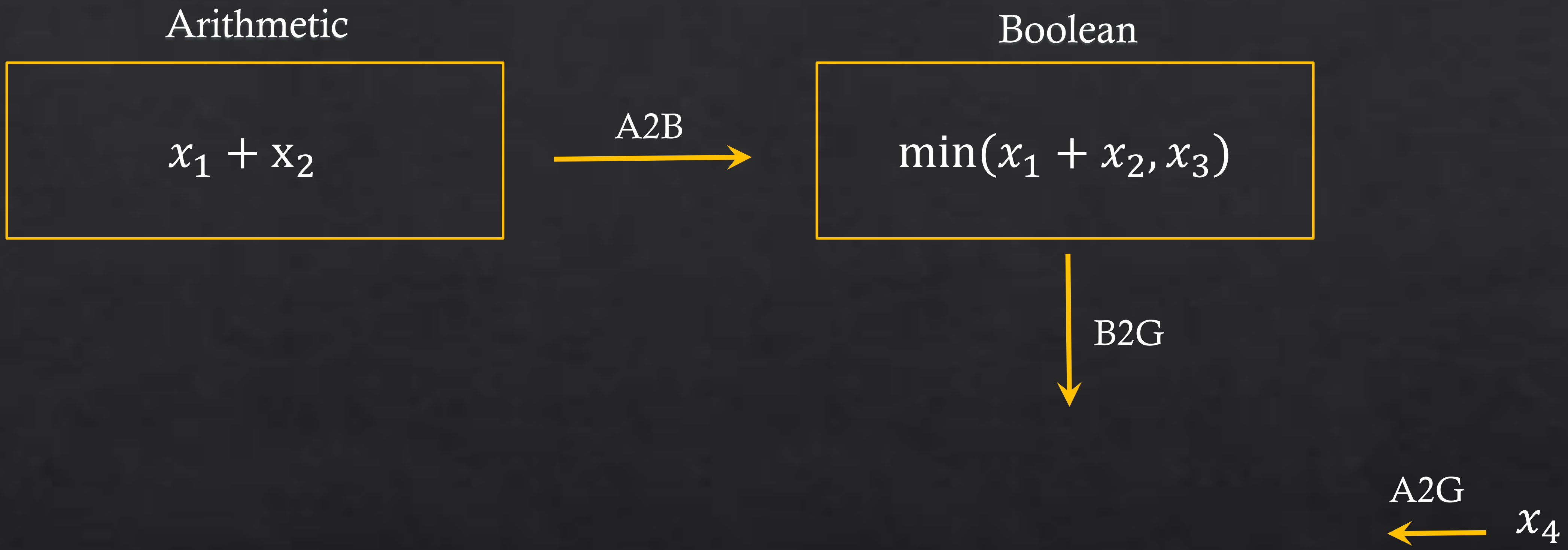
A2B

Boolean

$\min(x_1 + x_2, x_3)$

B2G

Mixed World Conversions – An Example



Arithmetic

$x_1 + x_2$

A2B

Boolean

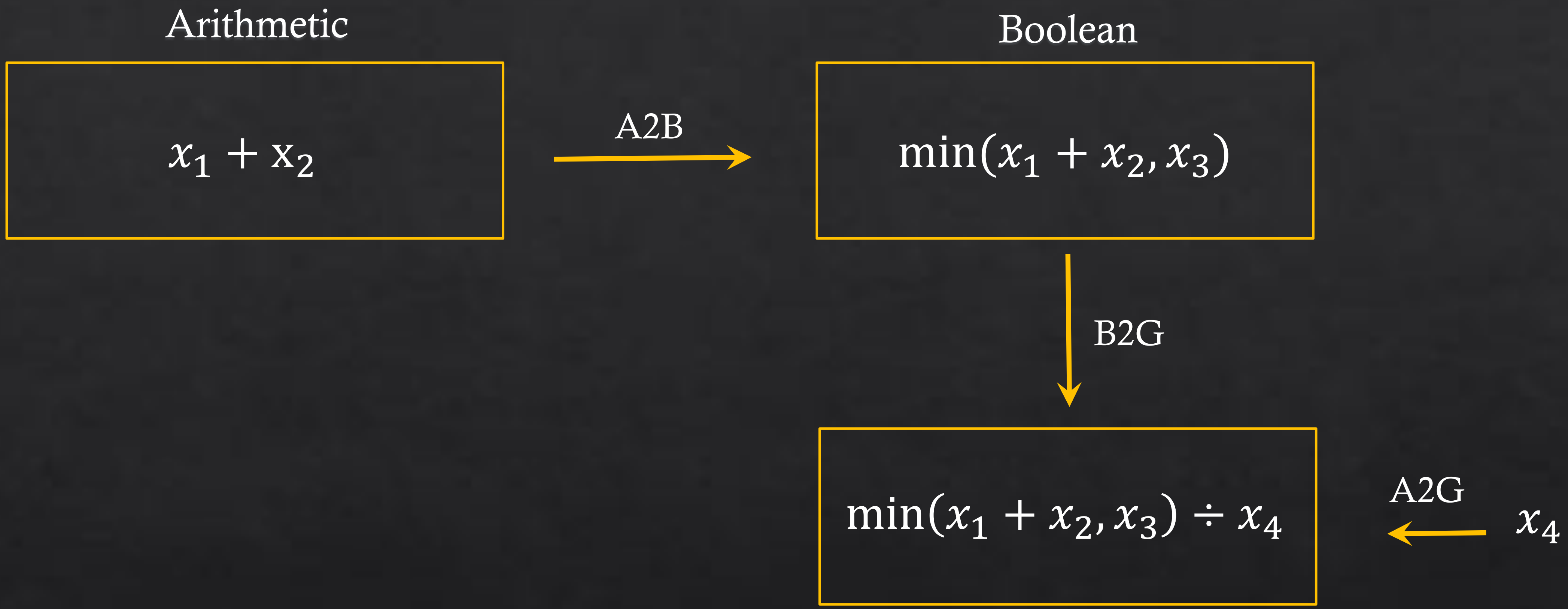
$\min(x_1 + x_2, x_3)$

B2G

A2G

x_4

Mixed World Conversions – An Example



Arithmetic

$x_1 + x_2$

A2B

Boolean

$\min(x_1 + x_2, x_3)$

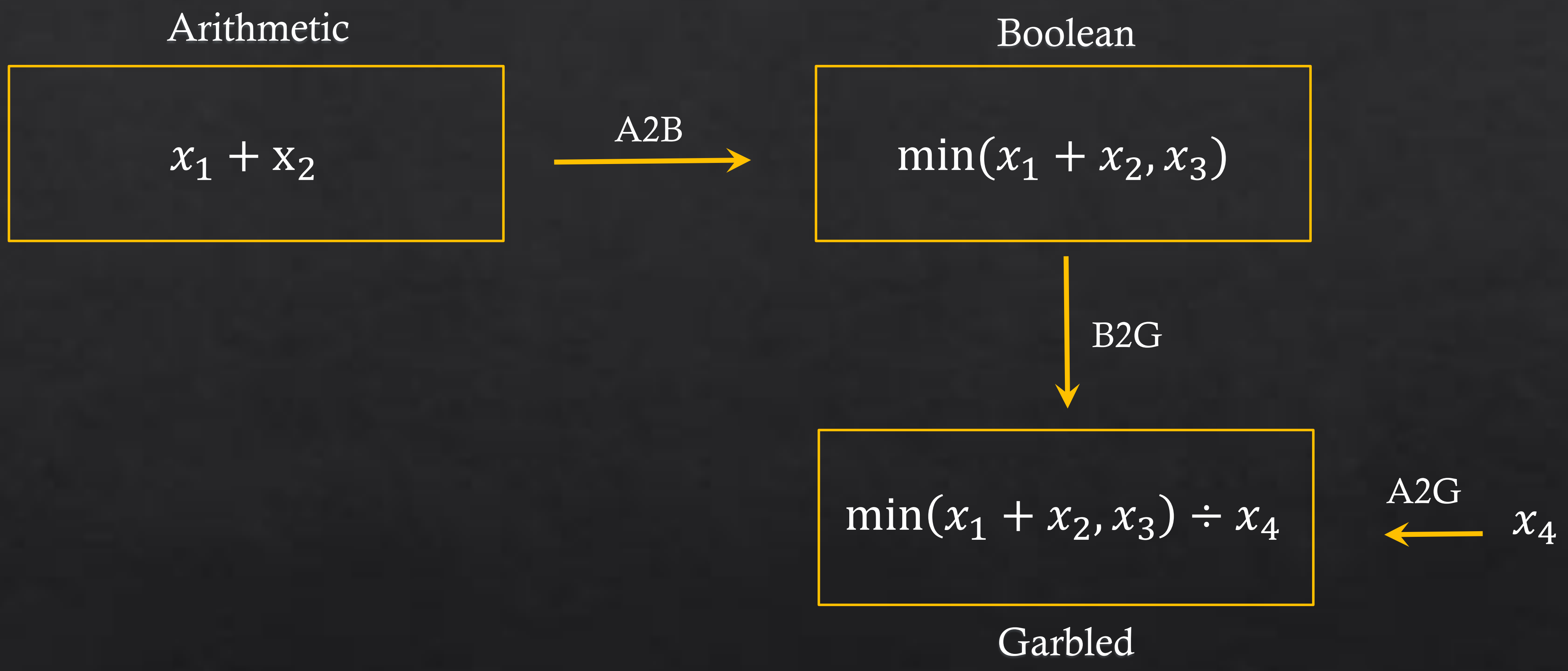
B2G

$\min(x_1 + x_2, x_3) \div x_4$

A2G

x_4

Mixed World Conversions – An Example



Arithmetic

$x_1 + \mathrm{x}_2$

A2B

Boolean

$\min(x_1 + x_2, x_3)$

B2G

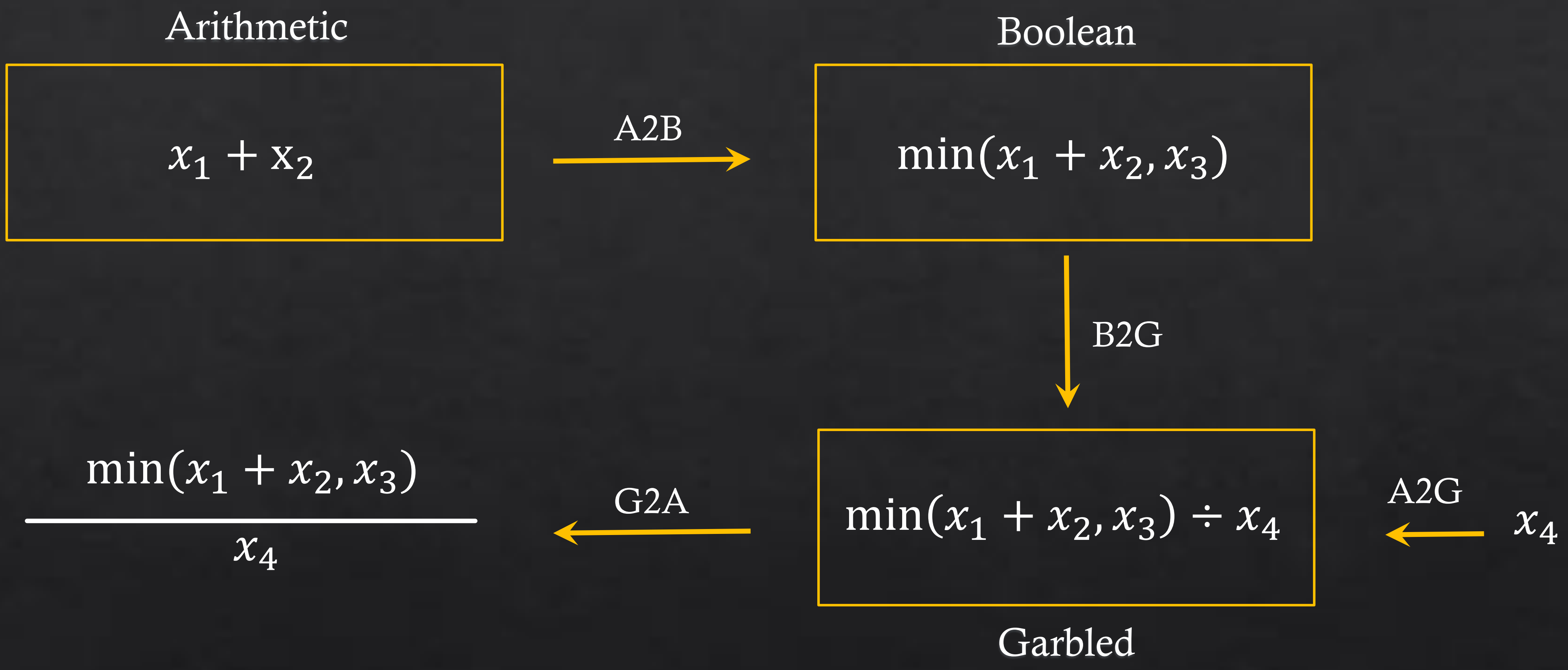
$\min(x_1 + x_2, x_3) \div x_4$

Garbled

A2G

x_4

Mixed World Conversions – An Example



Arithmetic

$x_1 + \mathrm{x}_2$

A2B

Boolean

$\min(x_1 + x_2, x_3)$

B2G

$\min(x_1 + x_2, x_3) \div x_4$

Garbled

A2G

x_4

G2A

$$\frac{\min(x_1 + x_2, x_3)}{x_4}$$

Trident protocol

- A new 4PC protocol over ring in the pre-processing model
- Malicious security with guarantee of fairness
- Efficient Mixed World Conversions
- Special tools for PPML

Dot Product

$$X \blacksquare Y = \sum_{i=1}^{d} x_i \, . \, yi$$

Ref	Pre-processing (#elements)	Online (#elements)	Security
ABY3 (3PC)	12d	9d	Abort

d – #elements in each vector

Dot Product

$$X \blacksquare Y = \sum_{i=1}^{d} x_i \,. yi$$

Ref	Pre-processing (#elements)	Online (#elements)	Security
ABY3 (3PC)	12d	9d	Abort
ASTRA (3PC)	21d	2d+2	Fair

d – #elements in each vector

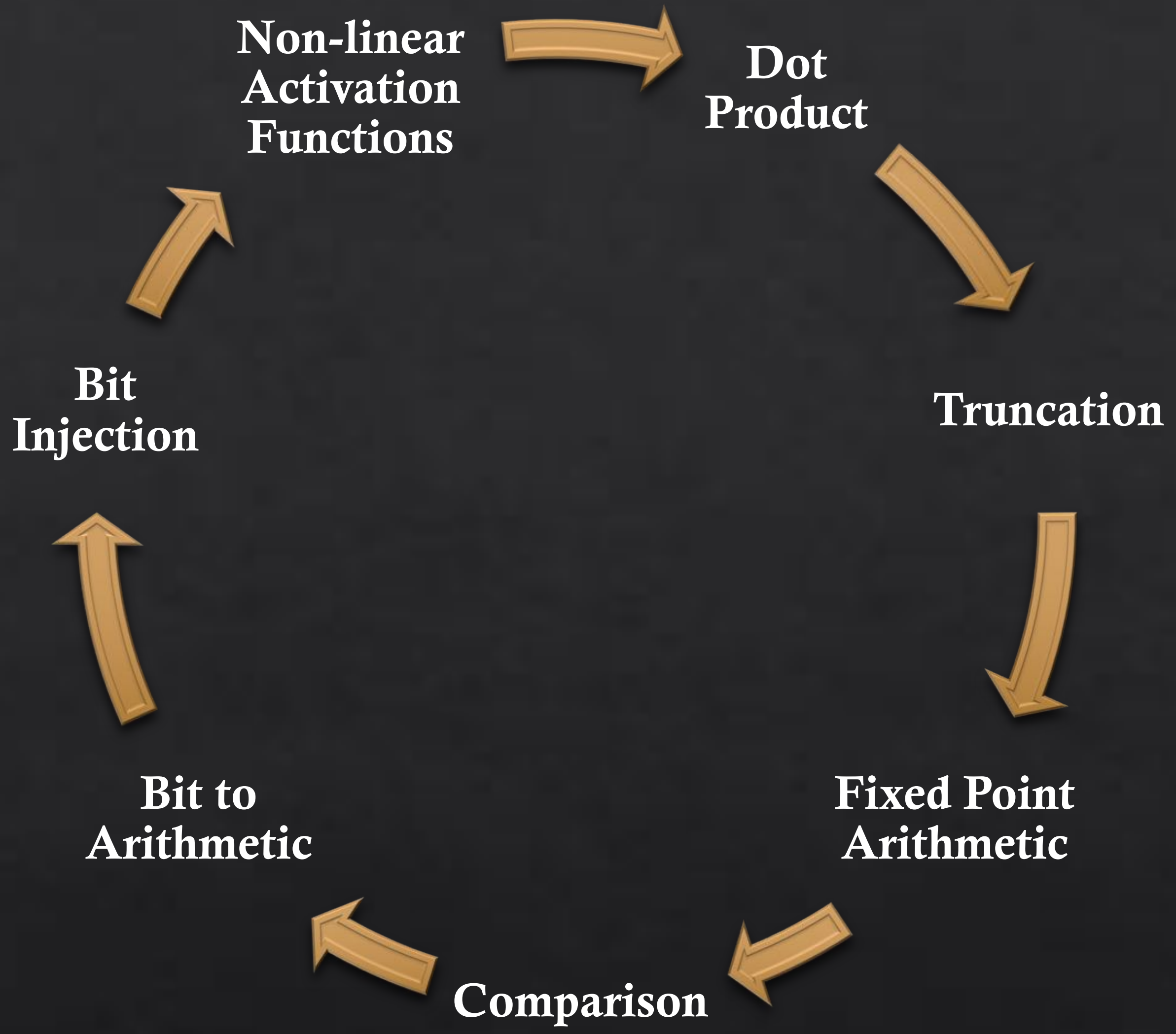
Dot Product

$$X \blacksquare Y = \sum_{i=1}^{d} x_i \,.\, yi$$

Ref	Pre-processing (#elements)	Online (#elements)	Security
ABY3 (3PC)	12d	9d	Abort
ASTRA (3PC)	21d	2d+2	Fair
Trident	**3**	**3**	**Fair**

d – #elements in each vector

Tools for PPML



Trident protocol

- A new 4PC protocol over ring in the pre-processing model
- Malicious security with guarantee of fairness
- Efficient Mixed World Conversions
- Special tools for PPML
- Lower monetary cost in the outsourced setting

Trident protocol

- A new 4PC protocol over ring in the pre-processing model
- Malicious security with guarantee of fairness
- Efficient Mixed World Conversions
- Special tools for PPML
- Lower monetary cost in the **outsourced setting**

Computation is outsourced to a set of hired servers

Benchmarking

- Implemented both Trident and ABY3, using the ENCRYPTO library.
- Benchmarked the protocols over LAN (40 Mbps) and WAN (1 Gbps) with the Google Cloud Platform.
- Servers located in West Europe, East Australia, South Asia, and South East Asia.
- For benchmarking, we used batch sizes up to 512 and feature sizes up to 1000.

Summary of Our Benchmarking Results

ML Algorithm	Improvement in terms of Online Throughput over ABY3	
	Training	Prediction
Linear Regression	251.84x	145.81x
Logistic Regression	34.58x	149.63x
Neural Networks	63.71x	407.12x
Convolutional Neural Networks	42.81x	741.56x

*Throughput for Training - #iterations processed by servers / minute
*Throughput for Prediction - #queries processed by servers / minute

thank you!

References

1. Andrew Chi-Chih Yao. *Protocols for secure computations* (extended abstract). In FOCS, pages 160-164, 1982.
2. P. Mohassel, M. Rosulek, and Y. Zhang. *Fast and Secure Three party Computation: Garbled Circuit Approach*. In CCS, 2015.
3. T. Araki, A. Barak, J. Furukawa, T. Lichter, Y. Lindell, A. Nof, K. Ohara, A. Watzman, and O. Weinstein. *Optimized Honest-Majority MPC for Malicious Adversaries - Breaking the 1 Billion-Gate Per Second Barrier*. In IEEE S&P, 2017.
4. J. Furukawa, Y. Lindell, A. Nof, and O. Weinstein. *High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority*. In EUROCRYPT, 2017.
5. K. Chida, D. Genkin, K. Hamada, D. Ikarashi, R. Kikuchi, Y. Lindell, and A. Nof. *Fast Large-Scale Honest-Majority MPC for Malicious Adversaries*. In CRYPTO, 2018.
6. P. Mohassel and P. Rindal, ABY3: A Mixed Protocol Framework for Machine Learning. In ACM CCS, 2018.
7. H. Chaudhari, A. Choudhury, A. Patra and A. Suresh. ASTRA: High-throughput 3PC over Rings with Application to Secure Prediction, In ACM CCSW, 2019.
8. S. D. Gordon and S. Ranellucci and X. Wang. Secure Computation with Low Communication from Cross-checking. In ASIACRYPT, 2018.