MPC in the Preprocessing Model

Shuang Sun - 04/22/2024

s.sun@liacs.leidenuniv.nl

Shuang Sun

PhD candidate

MPC, Secure **M**ulti**p**arty **C**omputation

PPML, **P**rivacy-**P**reserving **M**achine **L**earning

Currently, I’m still learning, reading, exploring

Welcome to communication, collaboration, casual conversation

Questions?

1 MPC

1.1 What is MPC

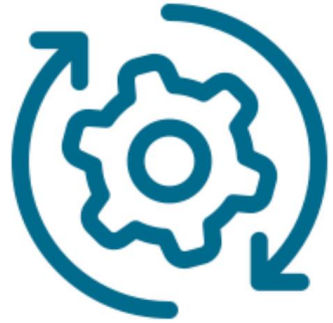
The Three States of Data

Data in Transit

Data at Rest

Traditional Cryptography

Data in Use

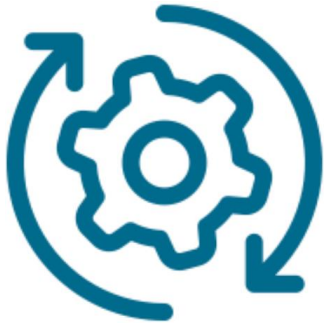


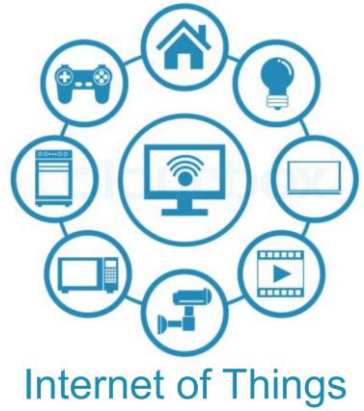
Secure Computation Technologies

1 MPC

1.1 What is MPC

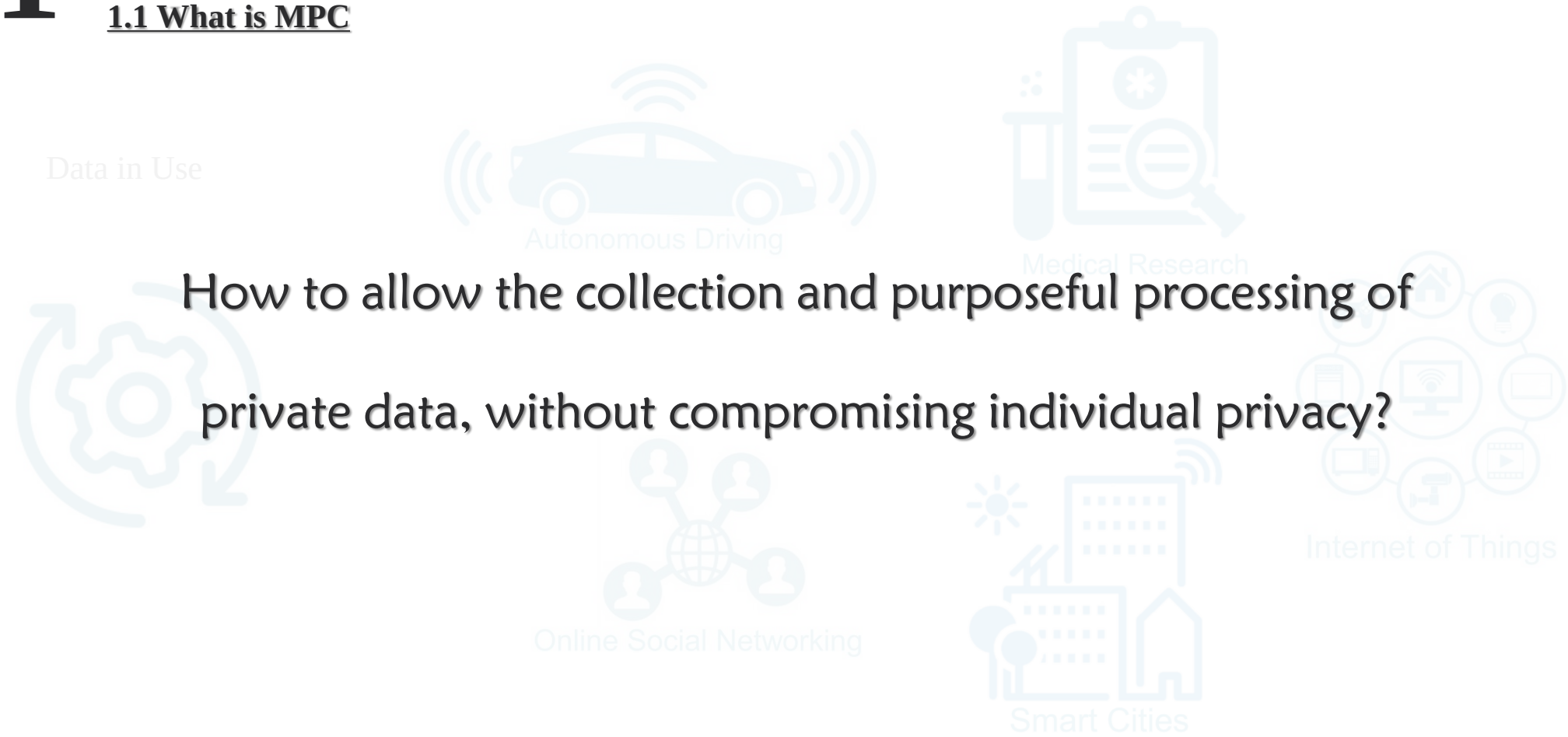
Data in Use





1 MPC

1.1 What is MPC

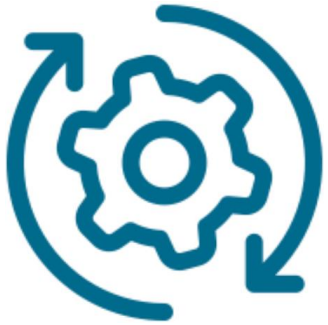


How to allow the collection and purposeful processing of private data, without compromising individual privacy?

1 MPC

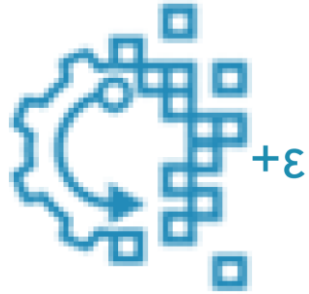
1.1 What is MPC

Data in Use



Privacy-Enhancing Technologies

Data Anonymization



Differential Privacy

Cryptographic Techniques
for Secure Computation

1 MPC

1.1 What is MPC

Yao’s millionaires’ problem

Two millionaires wish to know who is richer. However, they do not want to find out inadvertently any additional information about each other’s wealth. How can they carry out such a conversation?

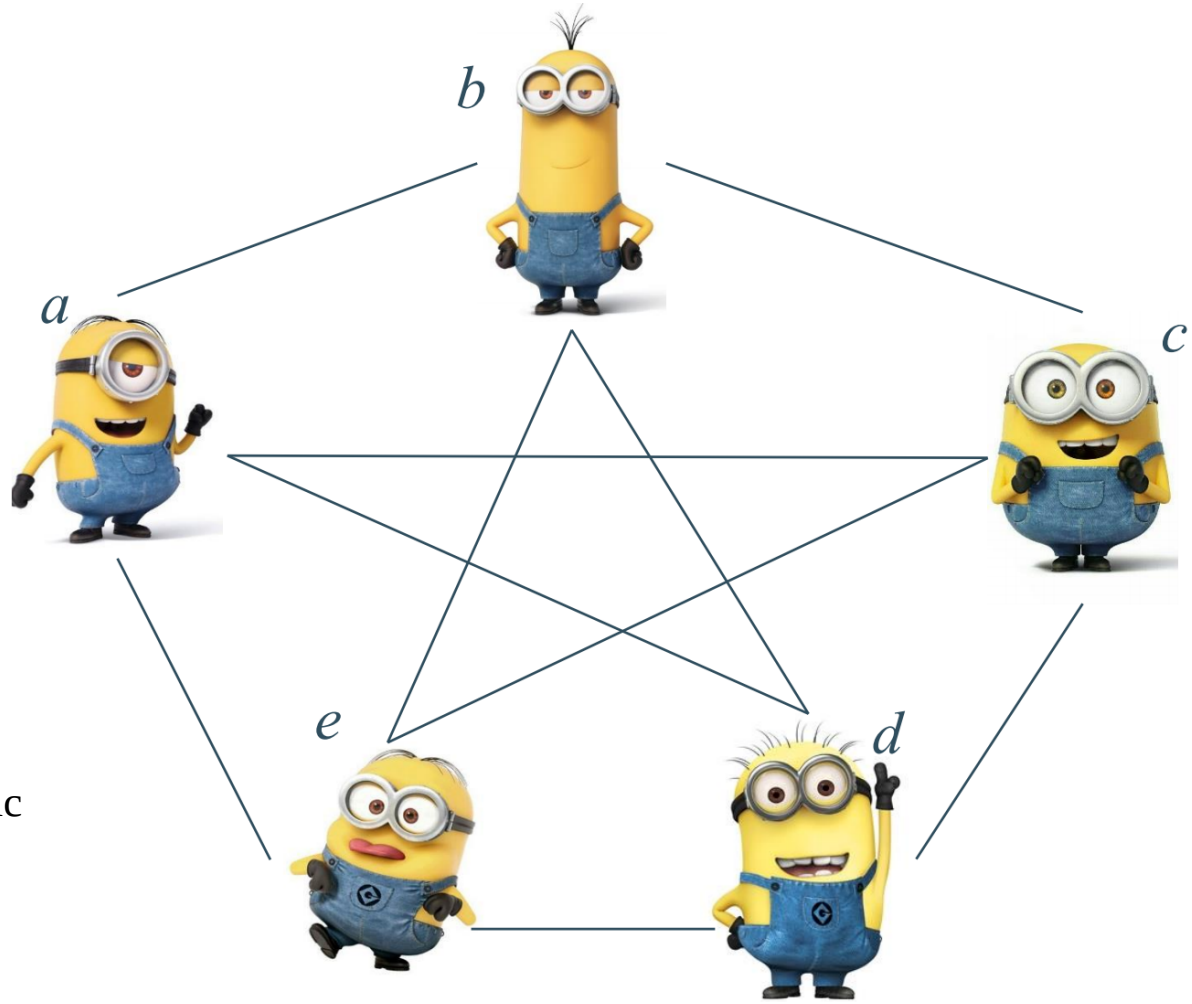
-- *1982*

1 MPC

1.1 What is MPC

Protocols for MPC enable a set of parties to interact and calculate a joint function of their private inputs while revealing nothing but the output

MPC protocols combine multiple cryptographic techniques to achieve varied functionalities.



Securely calculate $f(a, b, c, d, e)$

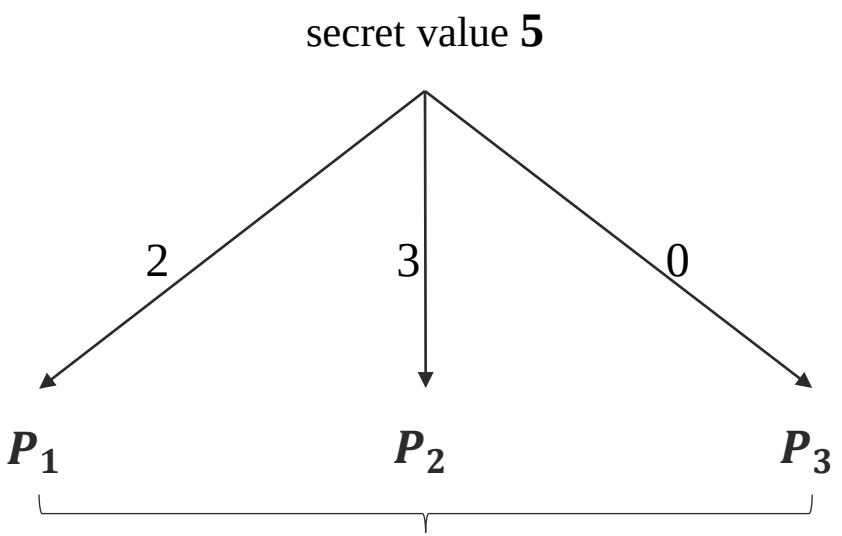
1 MPC

1.2 Research Topics

Preventing a single shareholder

from having any useful knowledge

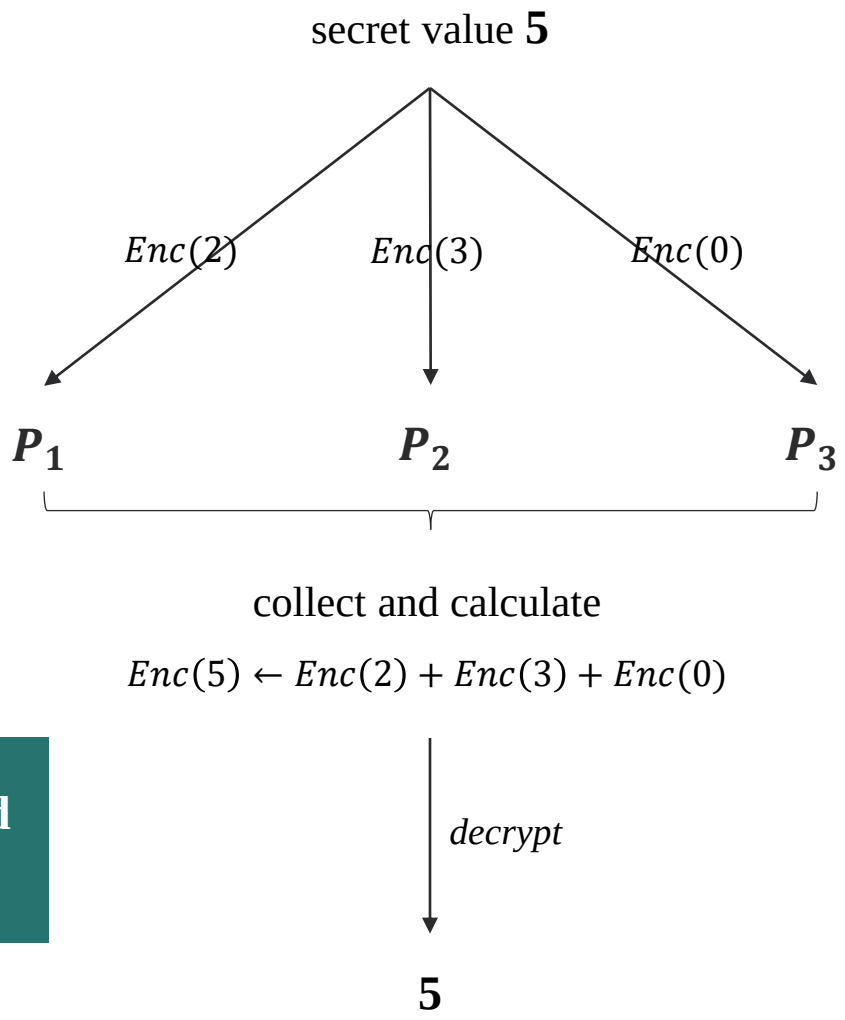
of the original secret value



Secret Sharing-based MPC Protocols

1 MPC

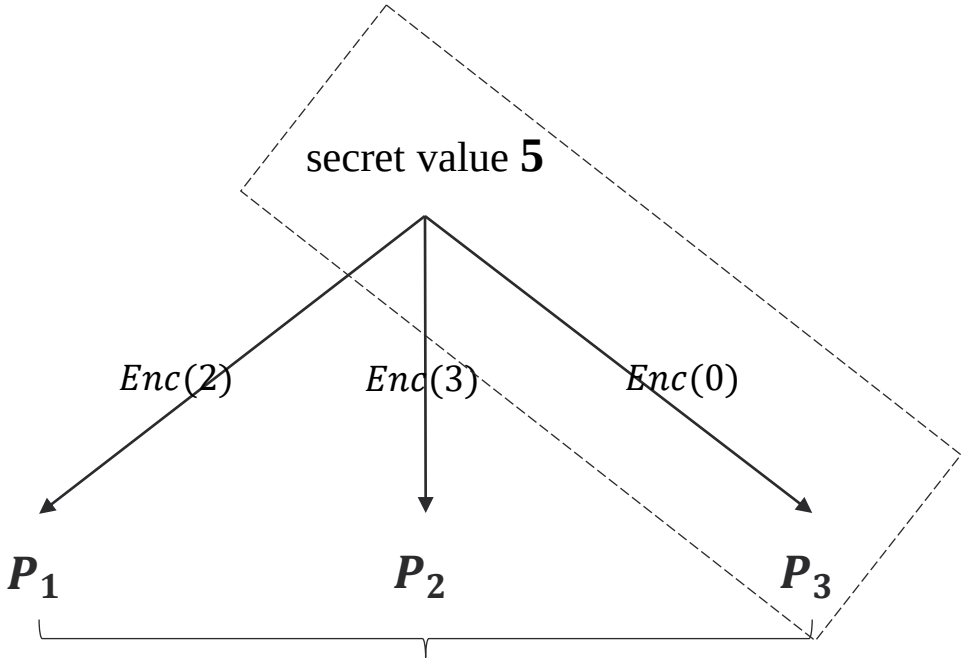
1.2 Research Topics

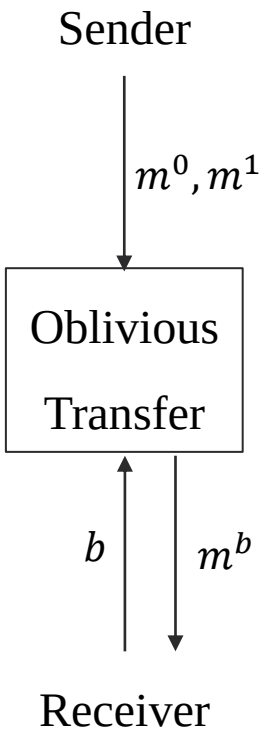


Homomorphic Encryption-based MPC Protocols

1 MPC

1.2 Research Topics





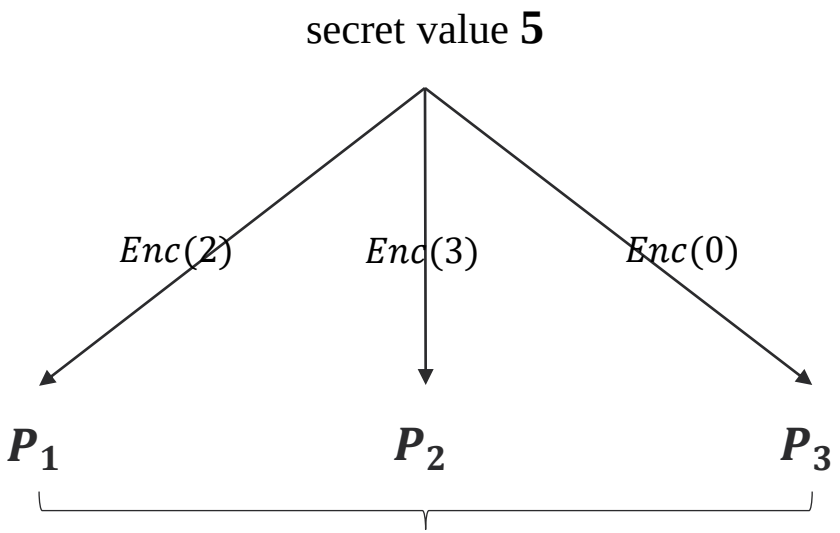
Receiver gains nothing but the piece he obtain.

Sender does not learn anything about which pieces of information were actually transferred to the receiver.

Oblivious Transfer-based MPC Protocols

1 MPC

1.2 Research Topics



MPC protocols blend multiple cryptographic techniques to achieve varied functionalities

2 MPC in Preprocessing Model

Preprocessing Model

- The most common way to construct MPC protocols, increases efficiency
- Preprocessing/offline phase, online phase
- The preprocessing phase:

  data independent, any time prior to protocol execution,

  prepare random materials for input sharing and computation
- The online phase

  data dependent, consume preprocessed materials for computation

2 MPC in Preprocessing Model

Online Phase

P_2

x

P_1

$z = x \cdot y$?

P_3

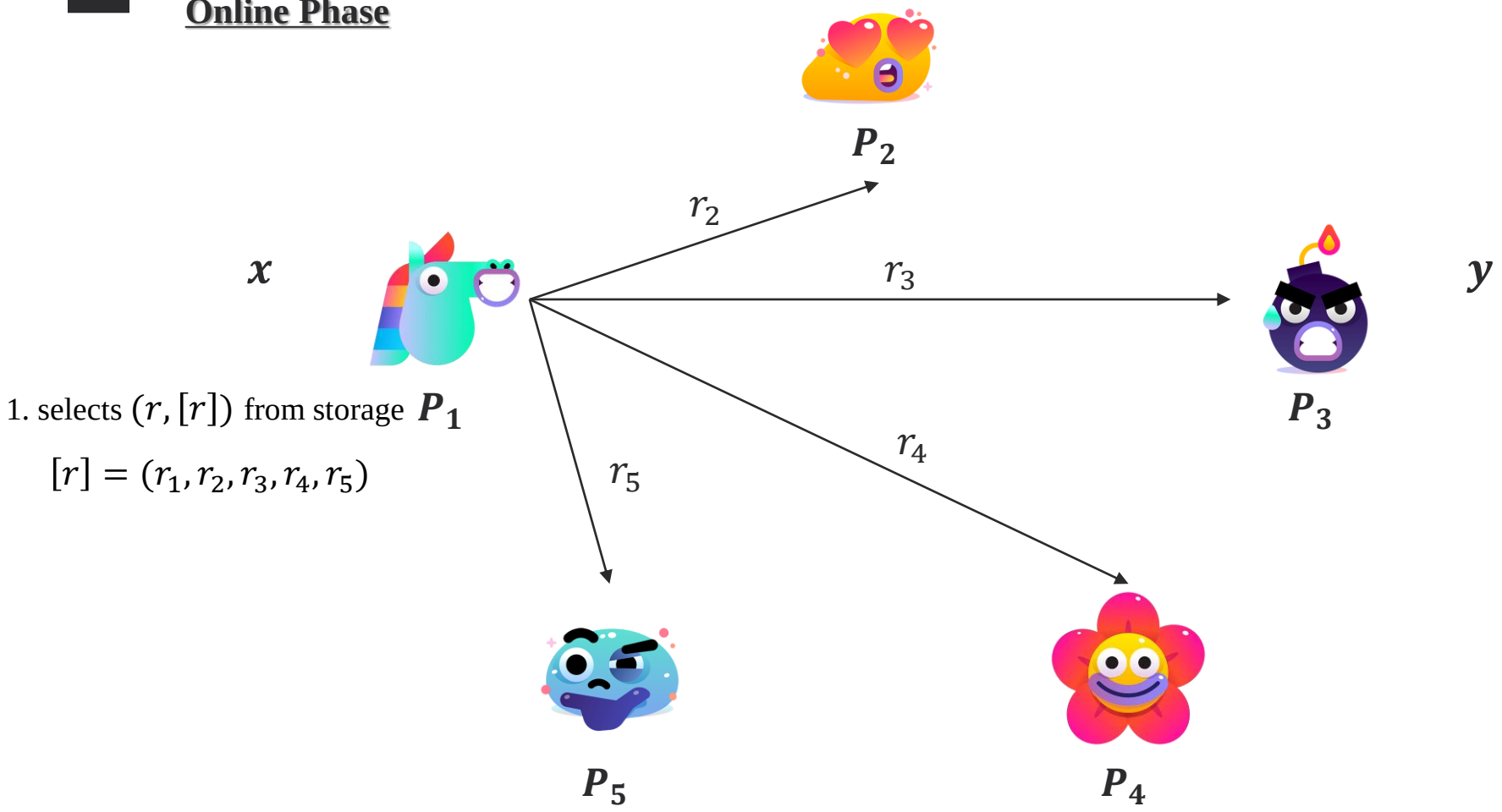
y

P_5

P_4

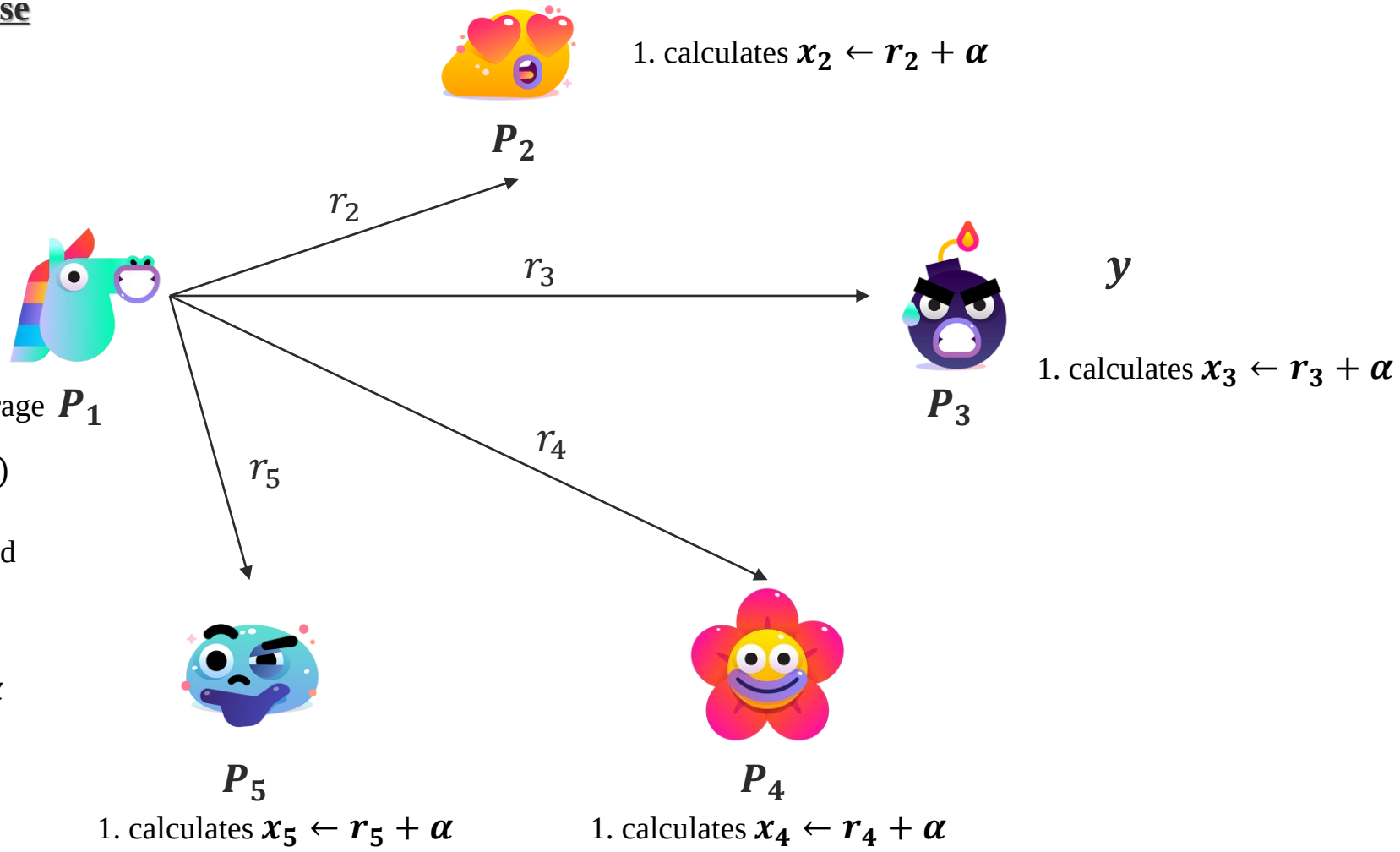
2 MPC in Preprocessing Model

Online Phase



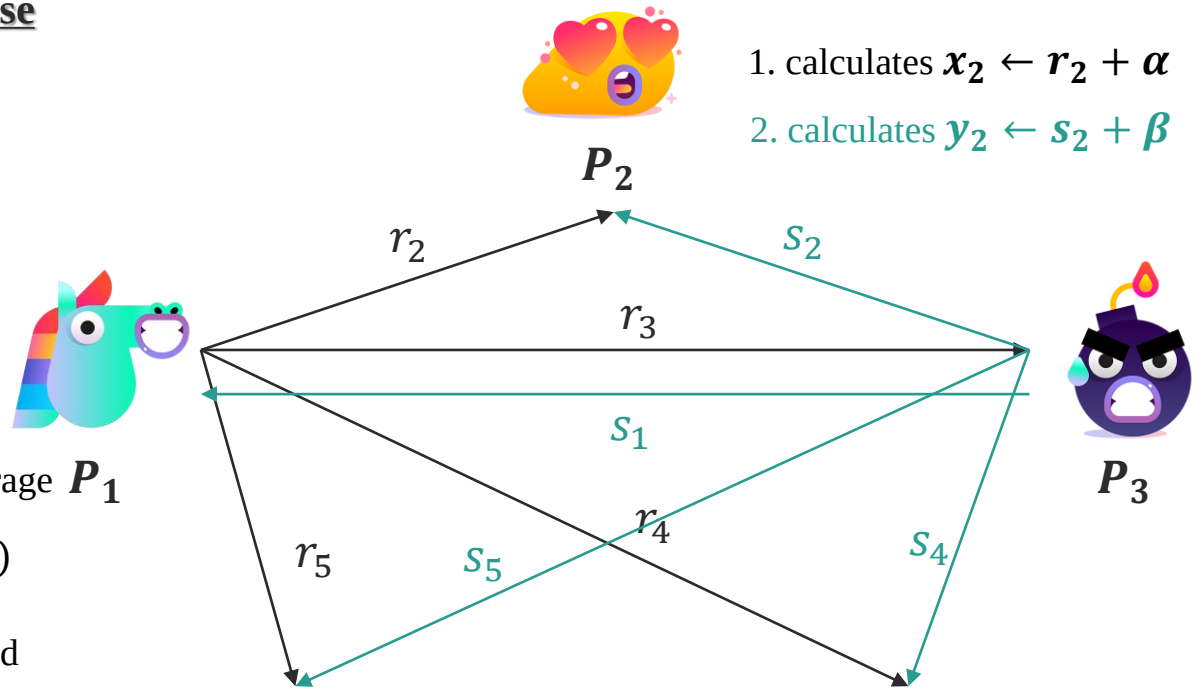
2 MPC in Preprocessing Model

Online Phase



2 MPC in Preprocessing Model

Online Phase



P_2

1. calculates $\boldsymbol{x_2 \leftarrow r_2 + \alpha}$
2. calculates $\boldsymbol{y_2 \leftarrow s_2 + \beta}$

$\boldsymbol{x}$

P_1

1. selects $(r, [r])$ from storage

$[r] = (r_1, r_2, r_3, r_4, r_5)$

2. calculates $\alpha \leftarrow x - r$ and then broadcast α
3. calculates $\boldsymbol{x_1 \leftarrow r_1 + \alpha}$
4. calculates $\boldsymbol{y_1 \leftarrow s_1 + \beta}$

$\boldsymbol{y}$

P_3

1. calculates $\boldsymbol{x_3 \leftarrow r_3 + \alpha}$
2. selects $(s, [s])$ from storage

$[s] = (s_1, s_2, s_3, s_4, s_5)$

3. calculates $\beta \leftarrow y - s$ and then broadcast β
4. calculates $\boldsymbol{y_3 \leftarrow s_3 + \beta}$

P_5

1. calculates $\boldsymbol{x_5 \leftarrow r_5 + \alpha}$
2. calculates $\boldsymbol{y_5 \leftarrow s_5 + \beta}$

P_4

1. calculates $\boldsymbol{x_4 \leftarrow r_4 + \alpha}$
2. calculates $\boldsymbol{y_4 \leftarrow s_4 + \beta}$

2 MPC in Preprocessing Model

Online Phase

P_2

1. calculates $x_2 \leftarrow r_2 + \alpha$
2. calculates $y_2 \leftarrow s_2 + \beta$

P_1

1. selects $(r, [r])$ from storage

$[r] = (r_1, r_2, r_3, r_4, r_5)$

2. calculates $\alpha \leftarrow x - r$ and then broadcast α
3. calculates $x_1 \leftarrow r_1 + \alpha$
4. calculates $y_1 \leftarrow s_1 + \beta$

Random materials are generated in preprocessing phase

P_3

1. calculates $x_3 \leftarrow r_3 + \alpha$
2. selects $(s, [s])$ from storage

$[s] = (s_1, s_2, s_3, s_4, s_5)$

3. calculates $\beta \leftarrow y - s$ and then broadcast β
4. calculates $y_3 \leftarrow s_3 + \beta$

P_5

1. calculates $x_5 \leftarrow r_5 + \alpha$
2. calculates $y_5 \leftarrow s_5 + \beta$

P_4

1. calculates $x_4 \leftarrow r_4 + \alpha$
2. calculates $y_4 \leftarrow s_4 + \beta$

2 MPC in Preprocessing Model

Online Phase

$P_2 \quad (x_2, y_2)$

x

$P_1 \quad (x_1, y_1)$

y

$P_3 \quad (x_3, y_3)$

$P_5 \quad (x_5, y_5)$

$P_4 \quad (x_4, y_4)$

2 MPC in Preprocessing Model

Online Phase

$P_2 \quad (x_2, y_2)$

x

$P_1 \quad (x_1, y_1)$

Each party takes a share of Beaver Triple

$([\![a]\!], [\![b]\!], [\![c]\!])$

Random $\quad c = a \cdot b$

y

$P_3 \quad (x_3, y_3)$

$P_5 \quad (x_5, y_5)$

$P_4 \quad (x_4, y_4)$

2 MPC in Preprocessing Model

Online Phase

$P_2 \quad (x_2, y_2) \quad (a_2, b_2, c_2)$

x

P_1

$(x_1, y_1) \quad (a_1, b_1, c_1)$

Each party takes a share of Beaver Triple

$$([\![a]\!], [\![b]\!], [\![c]\!])$$

$$[\![a]\!] = \{a_i\}_{i=1}^n$$

$$[\![b]\!] = \{b_i\}_{i=1}^n$$

$$[\![c]\!] = \{c_i\}_{i=1}^n$$

y

$P_3 \quad (x_3, y_3) \quad (a_3, b_3, c_3)$

(x_5, y_5)

$P_5 \quad (a_5, b_5, c_5)$

$P_4 \quad (x_4, y_4) \quad (a_4, b_4, c_4)$

2 MPC in Preprocessing Model

Online Phase

$$\begin{cases}\alpha_2 = x_2 - a_2 \\ \beta_2 = y_2 - b_2\end{cases}$$

$\boldsymbol{P_2}$ $(\boldsymbol{x_2}, \boldsymbol{y_2})$ $(\boldsymbol{a_2}, \boldsymbol{b_2}, \boldsymbol{c_2})$

$\boldsymbol{x}$

$$\begin{cases}\alpha_1 = x_1 - a_1 \\ \beta_1 = y_1 - b_1\end{cases}$$

$\boldsymbol{P_1}$

$(\boldsymbol{x_1}, \boldsymbol{y_1})$ $(\boldsymbol{a_1}, \boldsymbol{b_1}, \boldsymbol{c_1})$

Each party locally calculates:

$$\begin{cases}\alpha_i = x_i - a_i \\ \beta_i = y_i - b_i\end{cases}, \quad i = 1, \ldots, n$$

$\boldsymbol{y}$

$$\begin{cases}\alpha_3 = x_3 - a_3 \\ \beta_3 = y_3 - b_3\end{cases}$$

$\boldsymbol{P_3}$ $(\boldsymbol{x_3}, \boldsymbol{y_3})$ $(\boldsymbol{a_3}, \boldsymbol{b_3}, \boldsymbol{c_3})$

$$\begin{cases}\alpha_5 = x_5 - a_5 \\ \beta_5 = y_5 - b_5\end{cases}$$

$(\boldsymbol{x_5}, \boldsymbol{y_5})$

$\boldsymbol{P_5}$ $(\boldsymbol{a_5}, \boldsymbol{b_5}, \boldsymbol{c_5})$

$$\begin{cases}\alpha_4 = x_4 - a_4 \\ \beta_4 = y_4 - b_4\end{cases}$$

$\boldsymbol{P_4}$ $(\boldsymbol{x_4}, \boldsymbol{y_4})$ $(\boldsymbol{a_4}, \boldsymbol{b_4}, \boldsymbol{c_4})$

2 MPC in Preprocessing Model

Online Phase

$$\begin{cases}\alpha_2 = x_2 - a_2 \\ \beta_2 = y_2 - b_2\end{cases}$$

$\boldsymbol{P_2}$ $(\boldsymbol{x_2}, \boldsymbol{y_2})$ $(\boldsymbol{a_2}, \boldsymbol{b_2}, \boldsymbol{c_2})$

$\boldsymbol{x}$

$$\begin{cases}\alpha_1 = x_1 - a_1 \\ \beta_1 = y_1 - b_1\end{cases}$$

$\boldsymbol{P_1}$

$(\boldsymbol{x_1}, \boldsymbol{y_1})$ $(\boldsymbol{a_1}, \boldsymbol{b_1}, \boldsymbol{c_1})$

Each party locally calculates:

$$z_i = c_i + \alpha \cdot b_i + \beta \cdot a_i + \alpha \cdot \beta$$

$$(i = 1, \ldots, n)$$

$\boldsymbol{y}$

$$\begin{cases}\alpha_3 = x_3 - a_3 \\ \beta_3 = y_3 - b_3\end{cases}$$

$\boldsymbol{P_3}$ $(\boldsymbol{x_3}, \boldsymbol{y_3})$ $(\boldsymbol{a_3}, \boldsymbol{b_3}, \boldsymbol{c_3})$

$$\begin{cases}\alpha_5 = x_5 - a_5 \\ \beta_5 = y_5 - b_5\end{cases}$$

$(\boldsymbol{x_5}, \boldsymbol{y_5})$

$\boldsymbol{P_5}$ $(\boldsymbol{a_5}, \boldsymbol{b_5}, \boldsymbol{c_5})$

$$\begin{cases}\alpha_4 = x_4 - a_4 \\ \beta_4 = y_4 - b_4\end{cases}$$

$\boldsymbol{P_4}$ $(\boldsymbol{x_4}, \boldsymbol{y_4})$ $(\boldsymbol{a_4}, \boldsymbol{b_4}, \boldsymbol{c_4})$

2 MPC in Preprocessing Model

Online Phase

$$\begin{cases}\alpha_2 = x_2 - a_2 \\ \beta_2 = y_2 - b_2\end{cases}$$

P_2 (x_2, y_2) (a_2, b_2, c_2)

x

$$\begin{cases}\alpha_1 = x_1 - a_1 \\ \beta_1 = y_1 - b_1\end{cases}$$

P_1

(x_1, y_1) (a_1, b_1, c_1)

$$z_1 = c_1 + \alpha \cdot b_1 + \beta \cdot a_1 + \alpha \cdot \beta$$

$$z_2 = c_2 + \alpha \cdot b_2 + \beta \cdot a_2 + \alpha \cdot \beta$$

$$z_3 = c_3 + \alpha \cdot b_3 + \beta \cdot a_3 + \alpha \cdot \beta$$

$$z_4 = c_4 + \alpha \cdot b_4 + \beta \cdot a_4 + \alpha \cdot \beta$$

$$z_5 = c_5 + \alpha \cdot b_5 + \beta \cdot a_5 + \alpha \cdot \beta$$

y

$$\begin{cases}\alpha_3 = x_3 - a_3 \\ \beta_3 = y_3 - b_3\end{cases}$$

P_3 (x_3, y_3) (a_3, b_3, c_3)

$$\begin{cases}\alpha_5 = x_5 - a_5 \\ \beta_5 = y_5 - b_5\end{cases}$$

(x_5, y_5)

P_5 (a_5, b_5, c_5)

$$\begin{cases}\alpha_4 = x_4 - a_4 \\ \beta_4 = y_4 - b_4\end{cases}$$

P_4 (x_4, y_4) (a_4, b_4, c_4)

2 MPC in Preprocessing Model

Online Phase

$$z_1 = c_1 + \alpha \cdot b_1 + \beta \cdot a_1 + \alpha \cdot \beta$$
$$z_2 = c_2 + \alpha \cdot b_2 + \beta \cdot a_2 + \alpha \cdot \beta$$
$$z_3 = c_3 + \alpha \cdot b_3 + \beta \cdot a_3 + \alpha \cdot \beta$$
$$z_4 = c_4 + \alpha \cdot b_4 + \beta \cdot a_4 + \alpha \cdot \beta$$
$$z_5 = c_5 + \alpha \cdot b_5 + \beta \cdot a_5 + \alpha \cdot \beta$$

$$\alpha = x - a$$
$$\beta = y - b$$
$$c = a \cdot b$$

$$z_1 + z_2 + z_3 + z_4 + z_5 = \boldsymbol{c} + \alpha \cdot \boldsymbol{b} + \beta \cdot \boldsymbol{a} + \alpha \cdot \beta$$

2 MPC in Preprocessing Model

Online Phase

$$
\begin{aligned}
z_1 &= c_1 + \alpha \cdot b_1 + \beta \cdot a_1 + \alpha \cdot \beta \\
z_2 &= c_2 + \alpha \cdot b_2 + \beta \cdot a_2 + \alpha \cdot \beta \\
z_3 &= c_3 + \alpha \cdot b_3 + \beta \cdot a_3 + \alpha \cdot \beta \\
z_4 &= c_4 + \alpha \cdot b_4 + \beta \cdot a_4 + \alpha \cdot \beta \\
z_5 &= c_5 + \alpha \cdot b_5 + \beta \cdot a_5 + \alpha \cdot \beta
\end{aligned}
$$

$$
\begin{aligned}
z_1 + z_2 + z_3 + z_4 + z_5 &= \boldsymbol{c} + \alpha \cdot \boldsymbol{b} + \beta \cdot \boldsymbol{a} + \alpha \cdot \beta \\
&= \cancel{ab} + b\cancel{x} - \cancel{ab} + a\cancel{y} - \cancel{ab} + xy - b\cancel{x} - a\cancel{y} + \cancel{ab} \\
&= xy
\end{aligned}
$$

2 MPC in Preprocessing Model

Online Phase

$$\begin{cases}\alpha_2 = x_2 - a_2 \\ \beta_2 = y_2 - b_2\end{cases}$$

P_2 (x_2, y_2) (a_2, b_2, c_2)

$$\begin{cases}\alpha_1 = x_1 - a_1 \\ \beta_1 = y_1 - b_1\end{cases}$$

P_1

(x_1, y_1) (a_1, b_1, c_1)

$$z = z_1 + z_2 + z_3 + z_4 + z_5 = x \cdot y$$

$$\begin{cases}\alpha_3 = x_3 - a_3 \\ \beta_3 = y_3 - b_3\end{cases}$$

P_3 (x_3, y_3) (a_3, b_3, c_3)

$$\begin{cases}\alpha_5 = x_5 - a_5 \\ \beta_5 = y_5 - b_5\end{cases}$$

(x_5, y_5)

P_5 (a_5, b_5, c_5)

$$\begin{cases}\alpha_4 = x_4 - a_4 \\ \beta_4 = y_4 - b_4\end{cases}$$

P_4 (x_4, y_4) (a_4, b_4, c_4)

2 MPC in Preprocessing Model

Preprocessing Model

MAC
Message Authentication Code

GCs
Garbled Circuits

OT Extension
Oblivious Transfer Extension

OPE
Oblivious Product Evaluation

PRF
Pseudo Random Function

FSS
Functional Secret Sharing

[1] M. Keller, E. Orsini, and P. Scholl, ‘MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer’

[2] I. Damgard, V. Pastro, N. P. Smart, and S. Zakarias, ‘Multiparty Computation from Somewhat Homomorphic Encryption’

[3] R. Bendlin, I. Damgård, C. Orlandi, and S. Zakarias, ‘Semi-Homomorphic Encryption and Multiparty Computation’

Thank You

Welcome to communication and collaboration

s.sun@liacs.leidenuniv.nl

Shuang Sun

PhD candidate