BLAZE: BLAZING FAST PRIVACY-PRESERVING MACHINE LEARNING

ARPITA PATRA AND **AJITH SURESH**

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

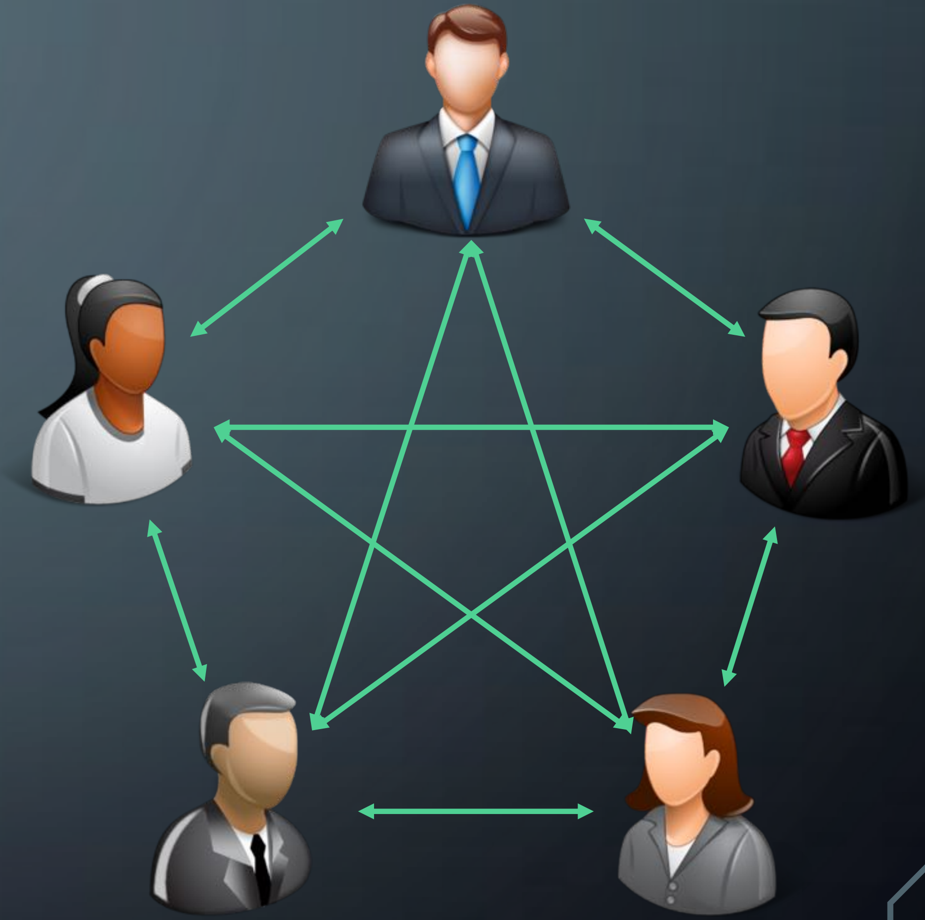
Outline

- Secure Multi-party Computation (MPC)
- MPC for small number of parties (3PC)
- Our Efficient BLAZE Protocol (Results)
- Privacy Preserving Machine Learning (PPML)

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

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

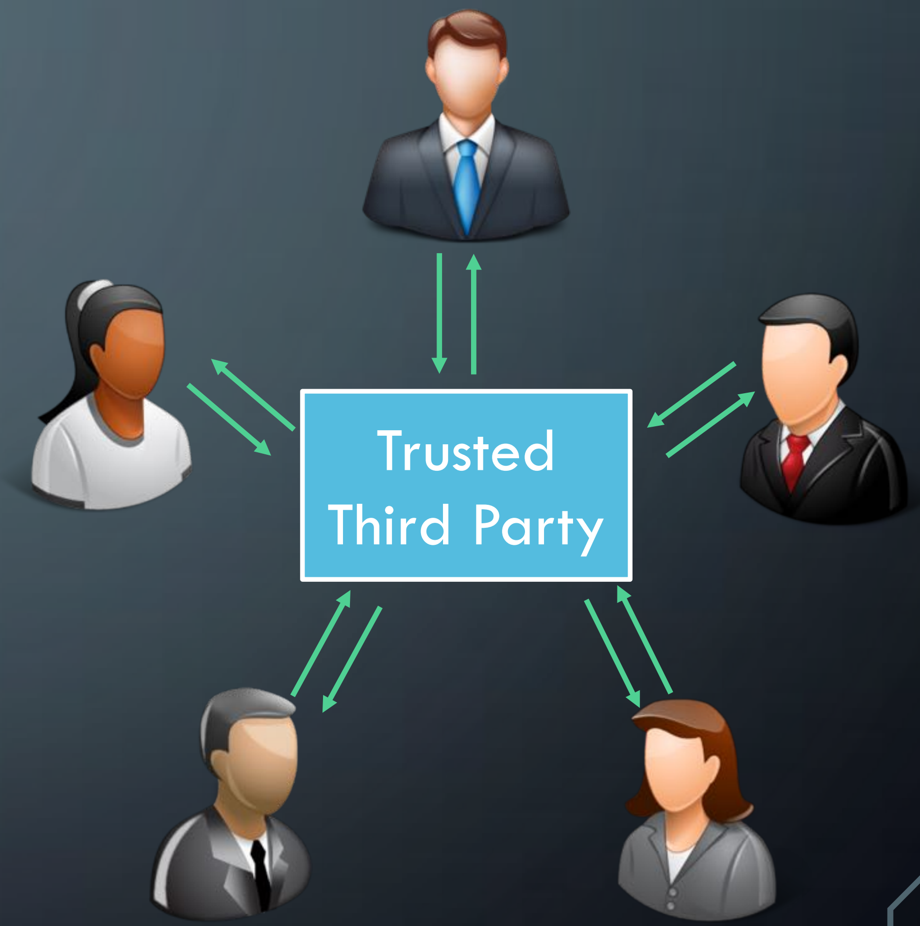
- ✓ Goals of MPC:
  - **Correctness** – Parties should correctly evaluate the function output.
  - **Privacy** – Nothing more than the function output should be revealed



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

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

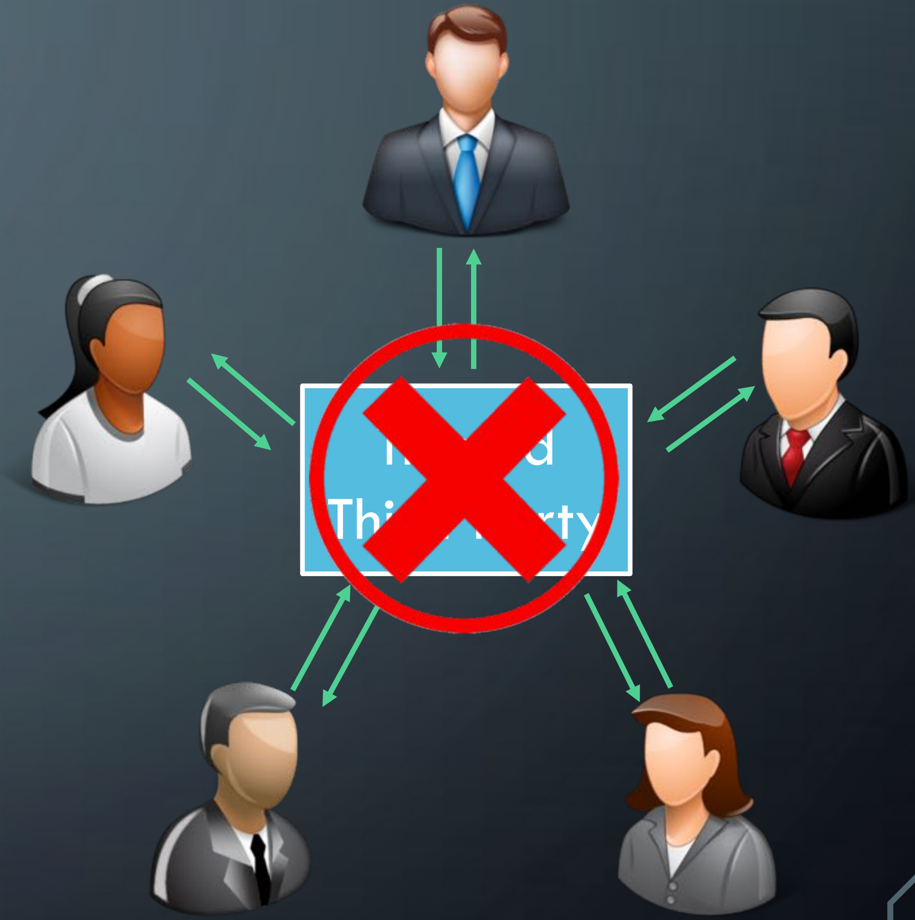
- ✓ Goals of MPC:
  - **Correctness** – Parties should correctly evaluate the function output.
  - **Privacy** – Nothing more than the function output should be revealed



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

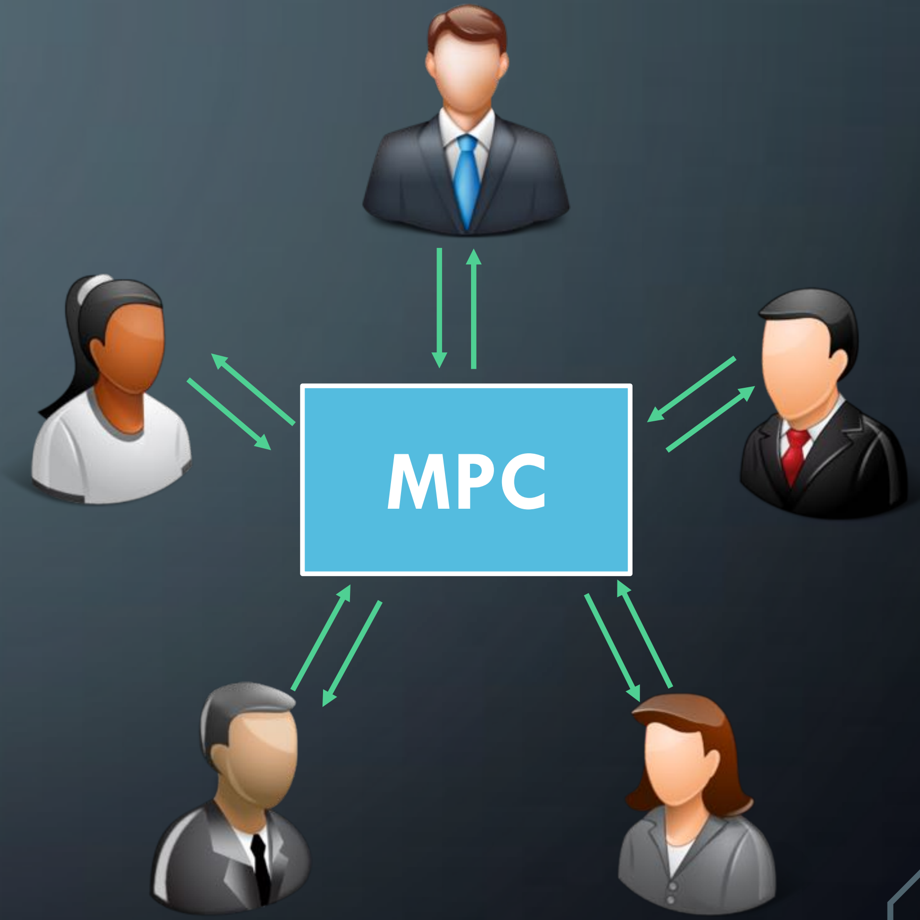
- ✓ A set of parties with private inputs wish to compute some joint function of their inputs.

- ✓ 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]

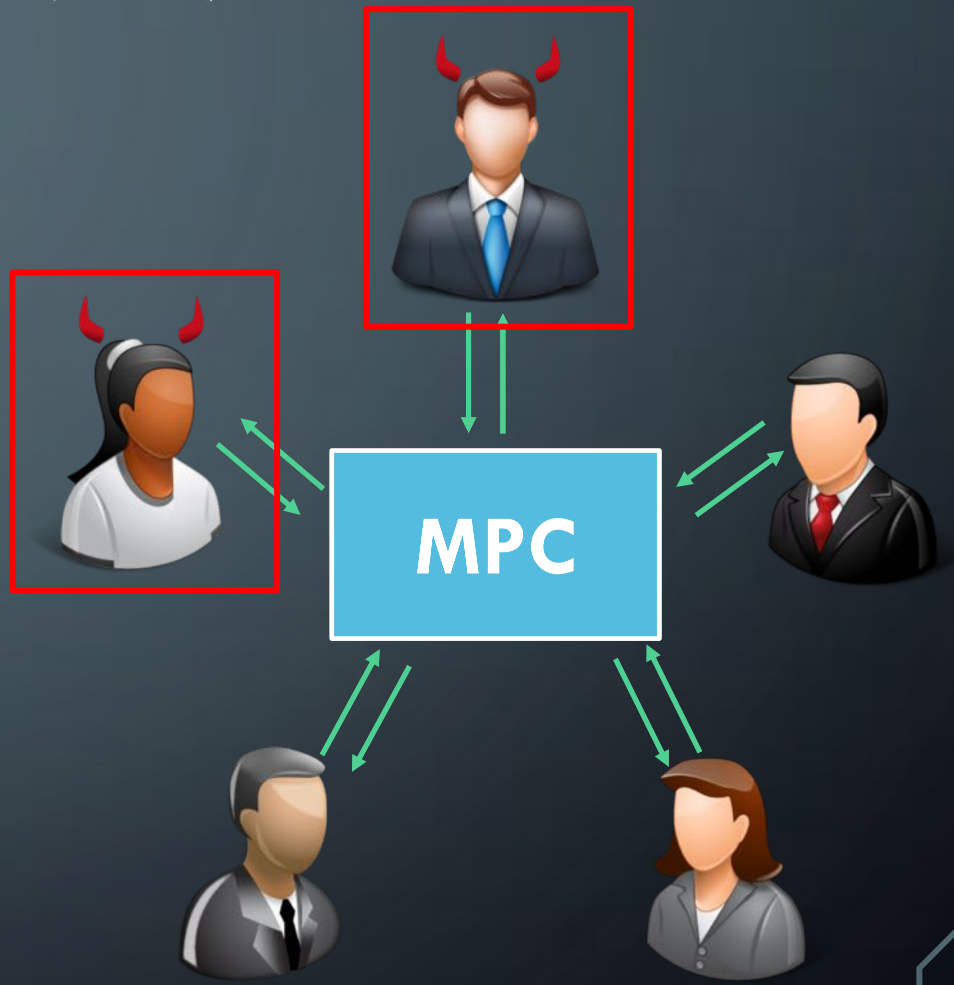
- ✓ A set of parties with private inputs wish to compute some joint function of their inputs.
- ✓ Goals of MPC:
  - **Correctness** – Parties should correctly evaluate the function output.
  - **Privacy** – Nothing more than the function output should be revealed



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

ADVERSARY

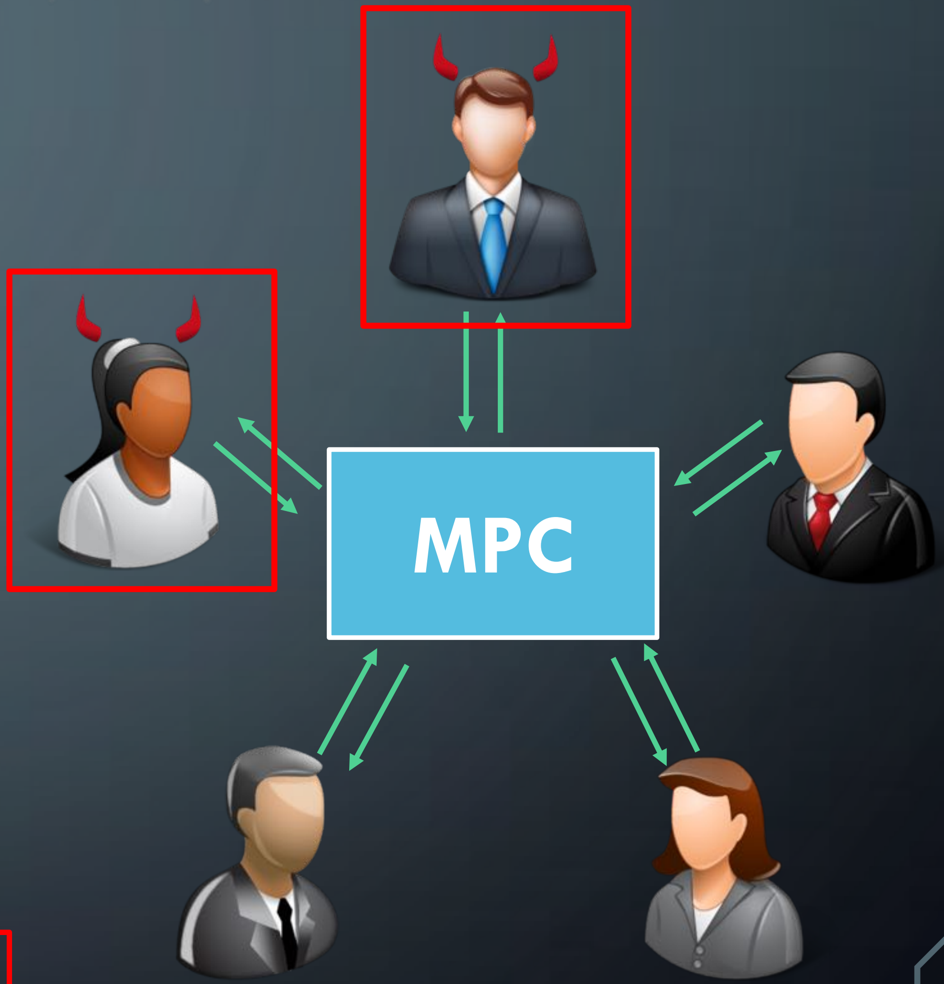
- Semi – honest:
  - Follows the protocol but tries to learn more
- Malicious:
  - Can arbitrarily deviate from the protocol



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

ADVERSARY

- Semi – honest:
  - Follows the protocol but tries to learn more
- Malicious:
  - Can arbitrarily deviate from the protocol



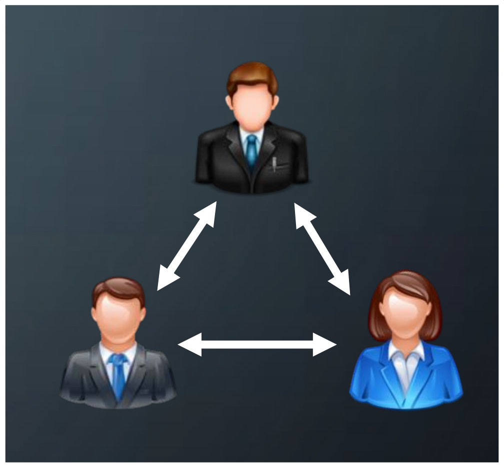
Malicious Corruption

MPC for small number of parties

- Efficiency and Simplicity [MRZ15,AFLNO16,FLNW17,CGMV17]

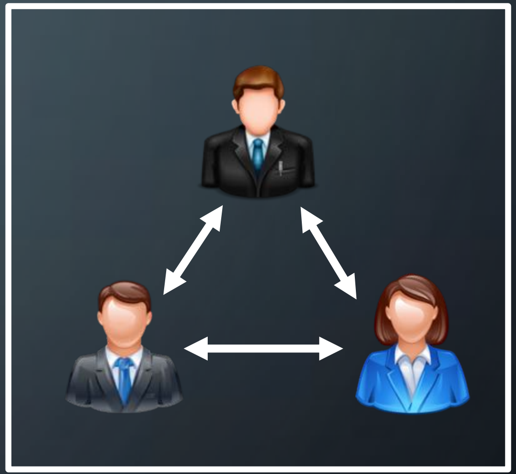
MPC for small number of parties

- **Efficiency** and **Simplicity** [MRZ15,AFLNO16,FLNW17,CGMV17]
- Our focus: MPC with 3 parties



MPC for small number of parties

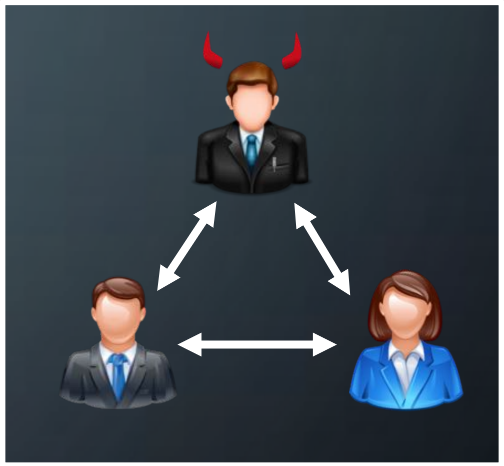
- **Efficiency** and **Simplicity** [MRZ15,AFLNO16,FLNW17,CGMV17]
- Our focus: MPC with 3 parties
- Corruption : **honest majority**



MPC for small number of parties

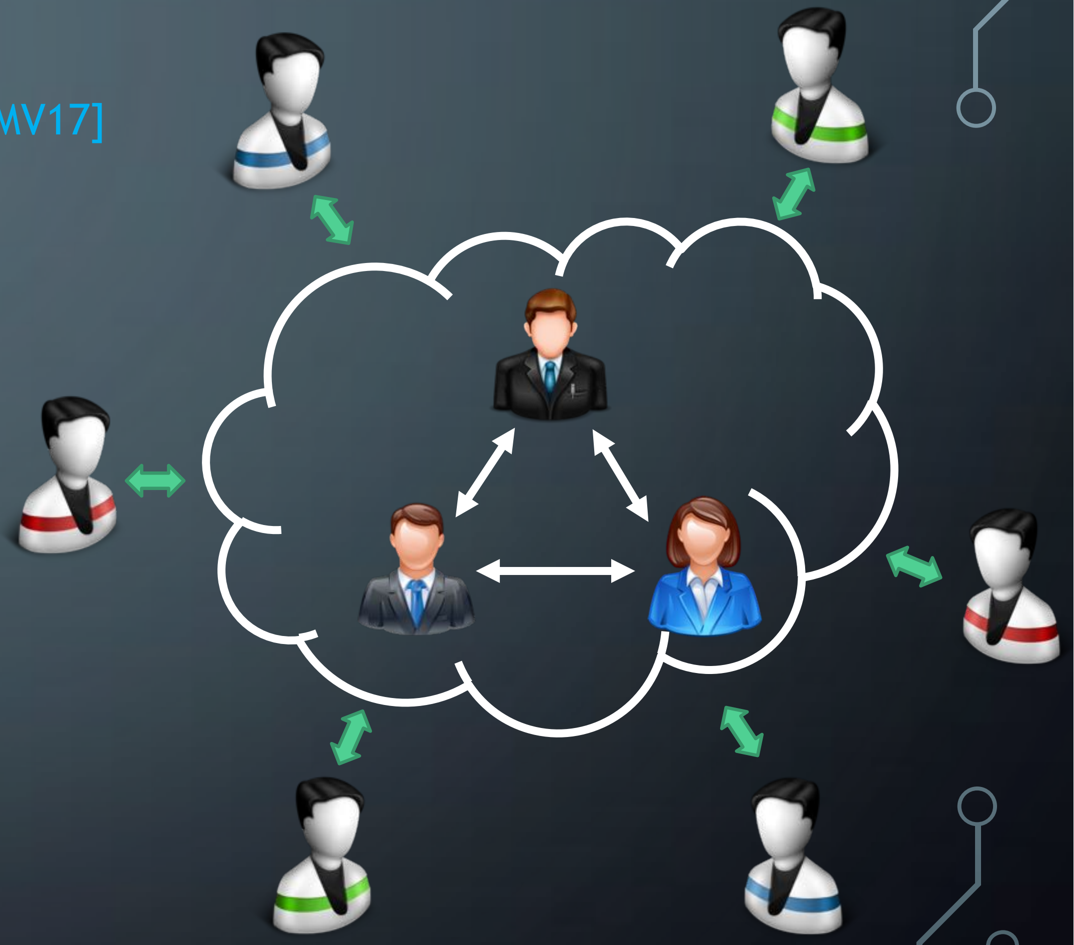
- **Efficiency** and **Simplicity** [MRZ15,AFLNO16,FLNW17,CGMV17]
- Our focus: MPC with 3 parties
- Corruption : **honest majority**

  - Majority of the parties are honest
  - 3PC - at most 1 corruption



MPC for small number of parties

- **Efficiency and Simplicity** [MRZ15,AFLNO16,FLNW17,CGMV17]
- Our focus: MPC with 3 parties
- Corruption : **honest majority**
- **Outsourced Computation**



MPC for small number of parties

- **Efficiency** and **Simplicity** [MRZ15,AFLNO16,FLNW17,CGMV17]
- Our focus: MPC with 3 parties
- Corruption : **honest majority**
- **Outsourced Computation**
- **Pre-processing Model**

MPC for small number of parties

- **Efficiency** and **Simplicity** [MRZ15,AFLNO16,FLNW17,CGMV17]
- Our focus: MPC with 3 parties
- Corruption : **honest majority**
- **Outsourced Computation**
- **Pre-processing Model**
  - **Pre-processing phase**

MPC for small number of parties

- **Efficiency** and **Simplicity** [MRZ15,AFLNO16,FLNW17,CGMV17]
- Our focus: MPC with 3 parties
- Corruption : **honest majority**
- **Outsourced Computation**
- **Pre-processing Model**
  - **Pre-processing phase**

- Data-independent Computation
- Relatively slow and expensive

MPC for small number of parties

- **Efficiency** and **Simplicity** [MRZ15,AFLNO16,FLNW17,CGMV17]
- Our focus: MPC with 3 parties
- Corruption : **honest majority**
- **Outsourced Computation**
- **Pre-processing Model**
  - **Pre-processing phase**
  - **Online Phase**

MPC for small number of parties

- **Efficiency** and **Simplicity** [MRZ15,AFLNO16,FLNW17,CGMV17]
- Our focus: MPC with 3 parties
- Corruption : **honest majority**
- **Outsourced Computation**
- **Pre-processing Model**
  - **Pre-processing phase**
  - **Online Phase**

- Minimized communication
- Blazing fast

BLAZE PROTOCOL

BLAZE Protocol

S_0

S_1

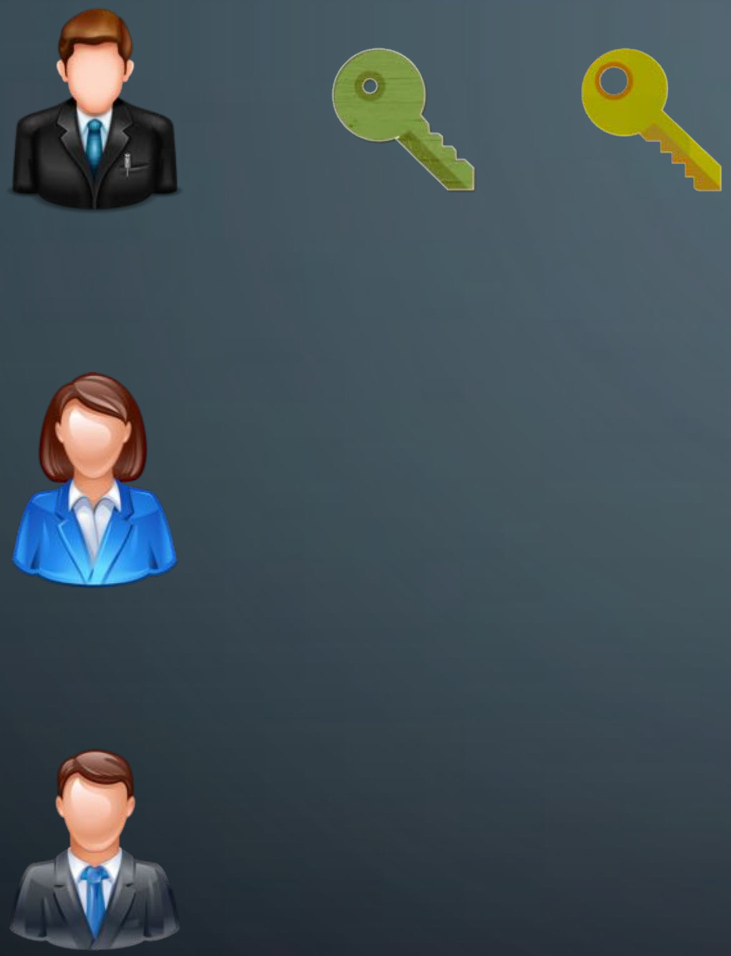
S_2

BLAZE Protocol

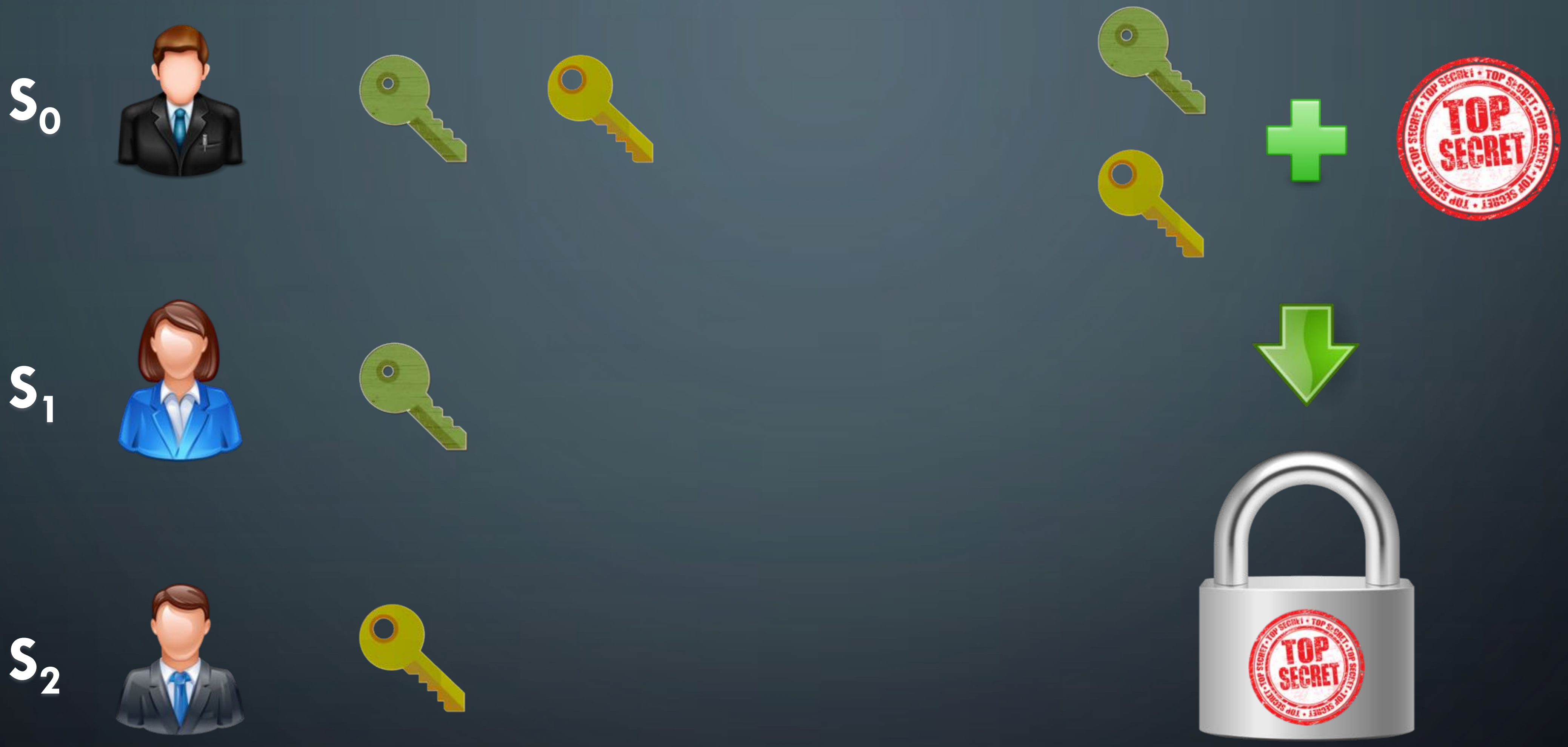
S_0

S_1

S_2

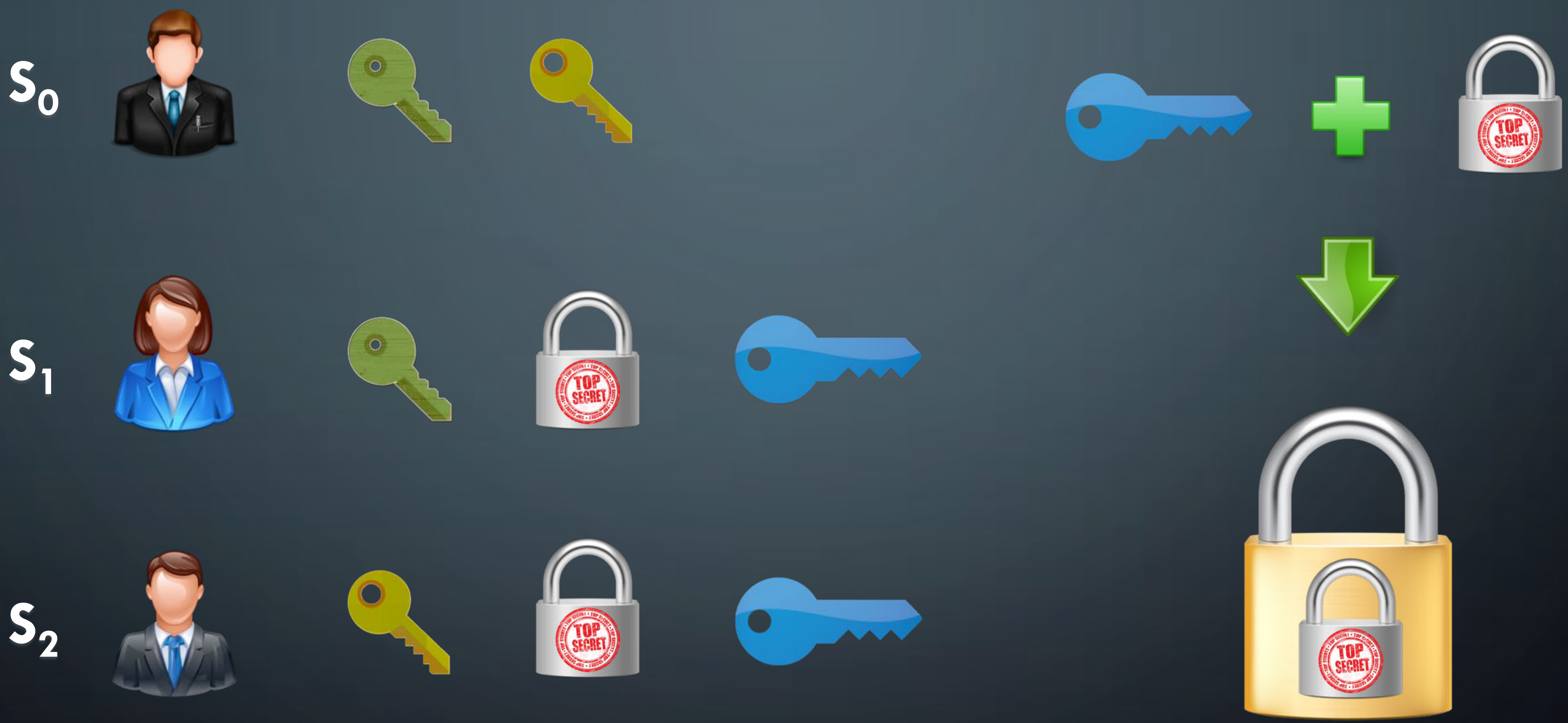


BLAZE Protocol

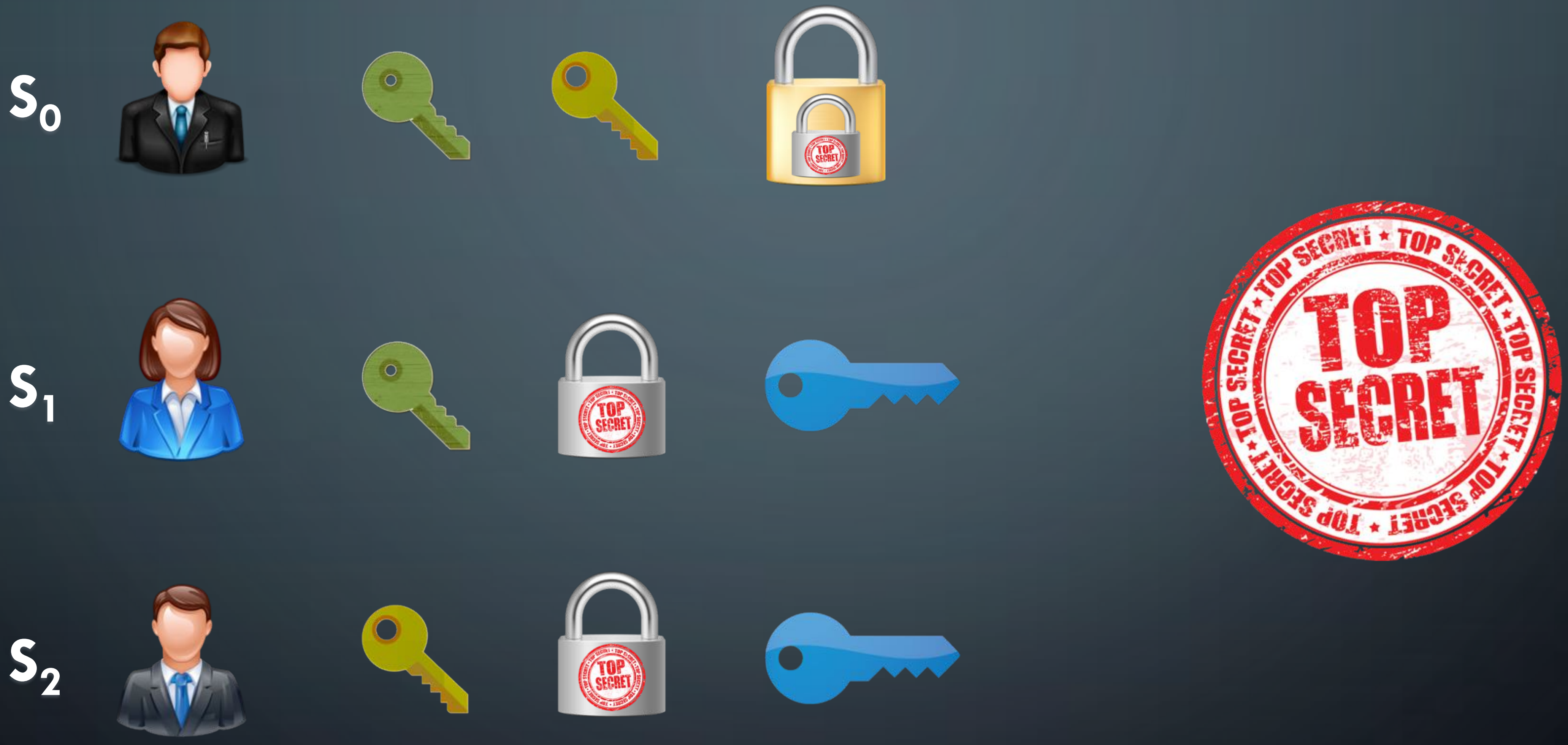


BLAZE Protocol

BLAZE Protocol



BLAZE Protocol



BLAZE Protocol

Communication Cost per
Multiplication Gate (malicious)

$Mult: x.y$

BLAZE : https://eprint.iacr.org/2020/042

BLAZE Protocol

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

Communication Cost per
Multiplication Gate (malicious)

$Mult: x.y$

BLAZE : https://eprint.iacr.org/2020/042

BLAZE Protocol

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

Communication Cost per
Multiplication Gate (malicious)

$Mult: x.y$

BLAZE : https://eprint.iacr.org/2020/042

BLAZE Protocol

Ref	Pre-processing (#elements)	Online (#elements)	Security
Araki et al'17	12	9	Abort
ASTRA	21	4	Fair
Boneh et al'19	0	3	Abort

Communication Cost per Multiplication Gate (malicious)

$$Mult: x.y$$

BLAZE : https://eprint.iacr.org/2020/042

BLAZE Protocol

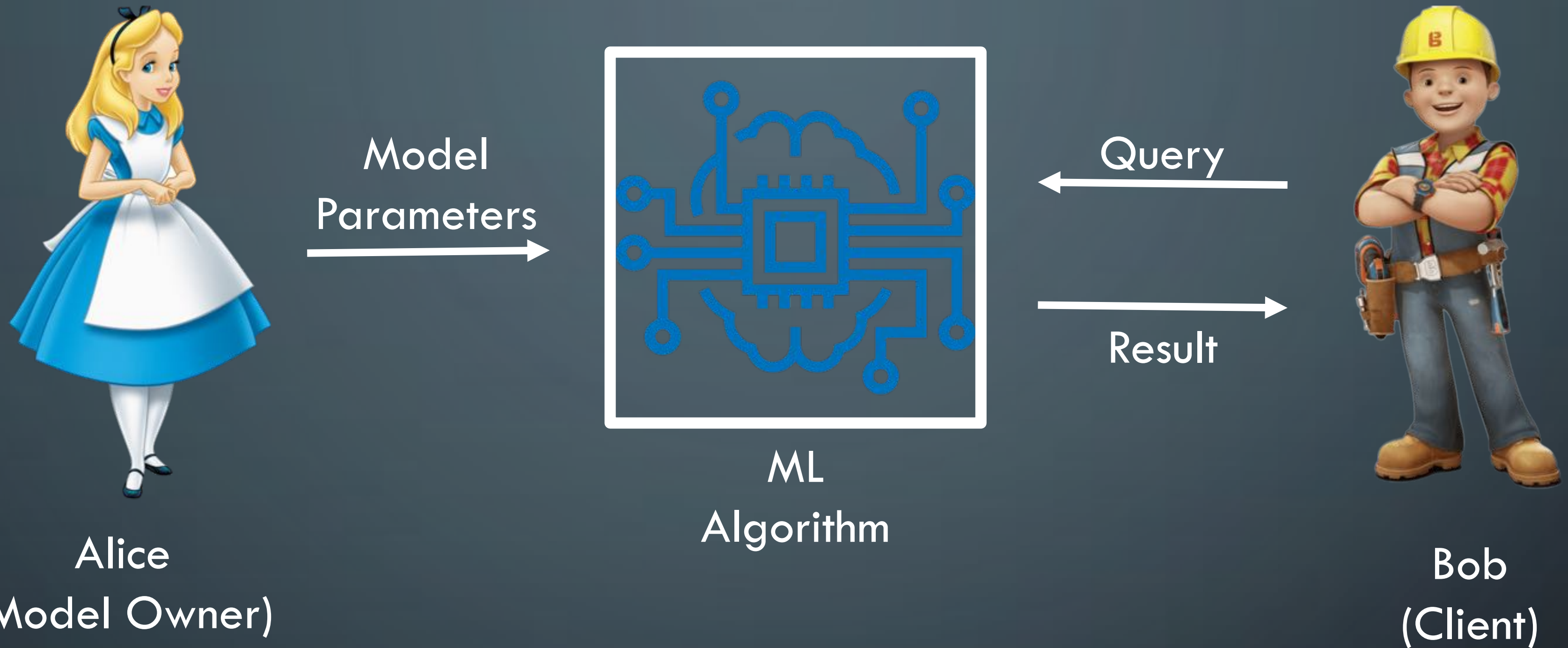
Ref	Pre-processing (#elements)	Online (#elements)	Security
Araki et al'17	12	9	Abort
ASTRA	21	4	Fair
Boneh et al'19	0	3	Abort
BLAZE	**3**	**3**	**Fair**

Communication Cost per
Multiplication Gate (malicious)

$Mult: x.y$

BLAZE : https://eprint.iacr.org/2020/042

Privacy Preserving Machine Learning (PPML)

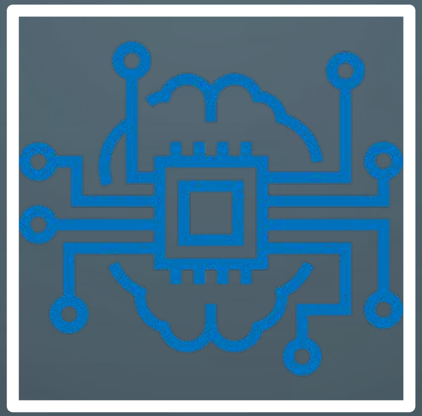


Privacy ??

Privacy Preserving Machine Learning (PPML)

Alice
(Model Owner)

Model Parameters



ML Algorithm

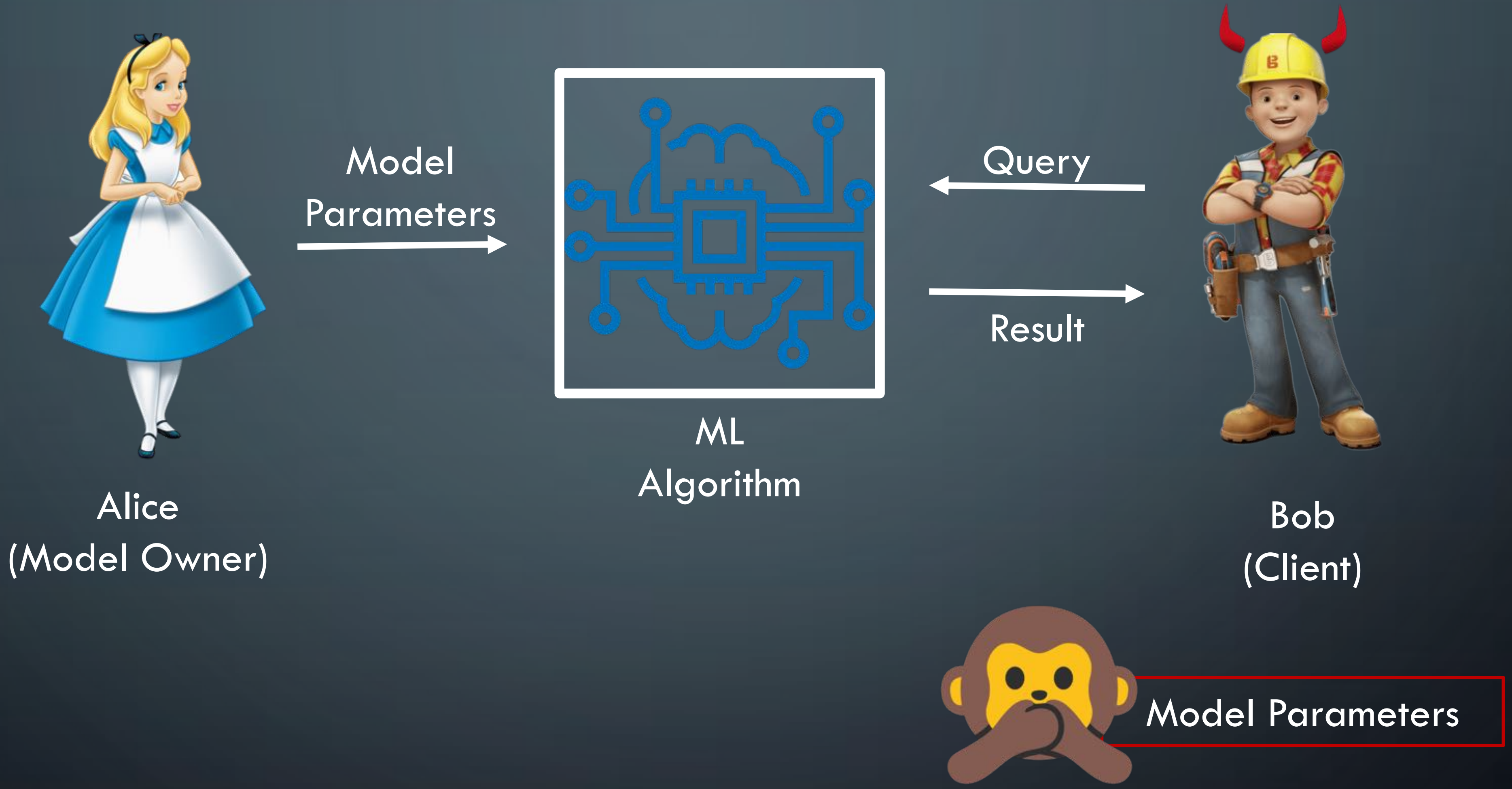
Query

Result

Bob
(Client)

Query

Privacy Preserving Machine Learning (PPML)

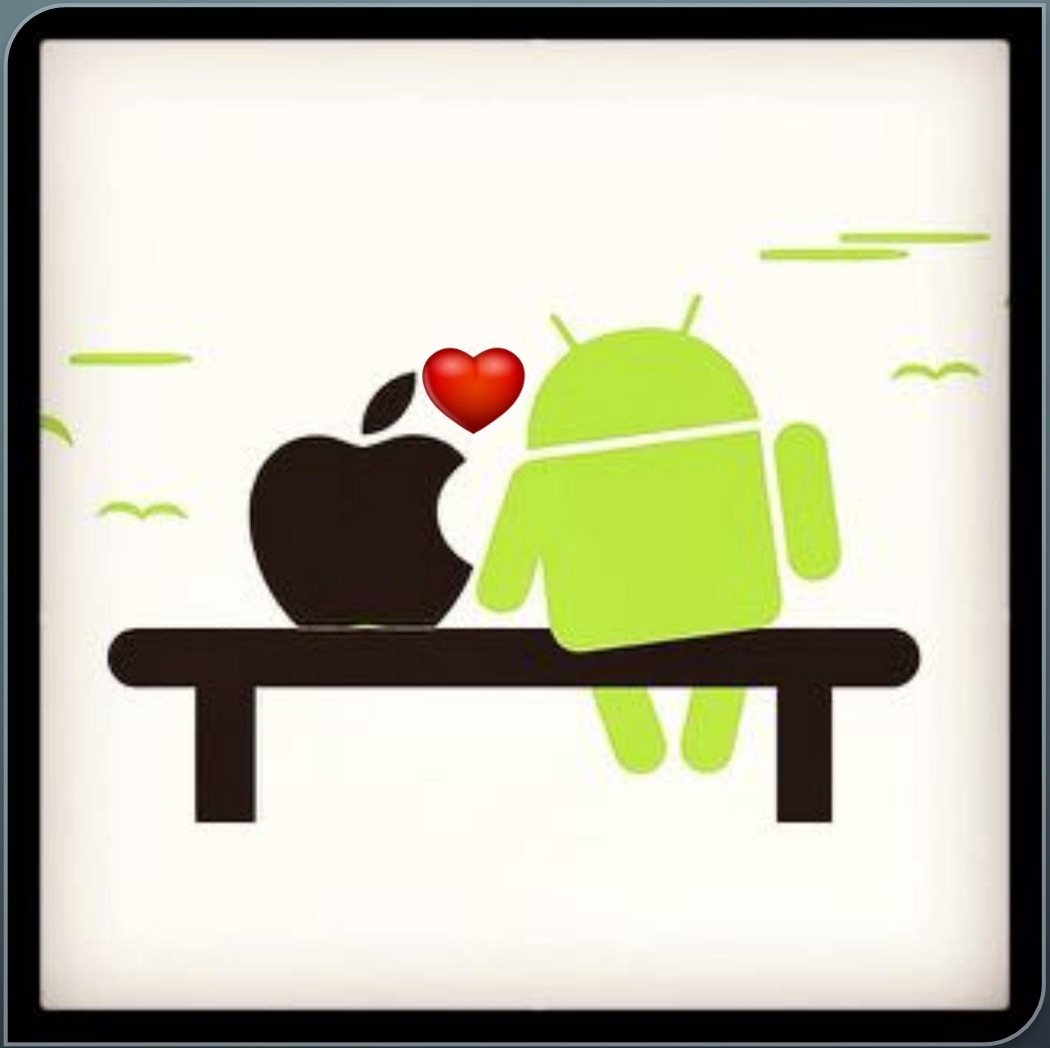


Solution ??

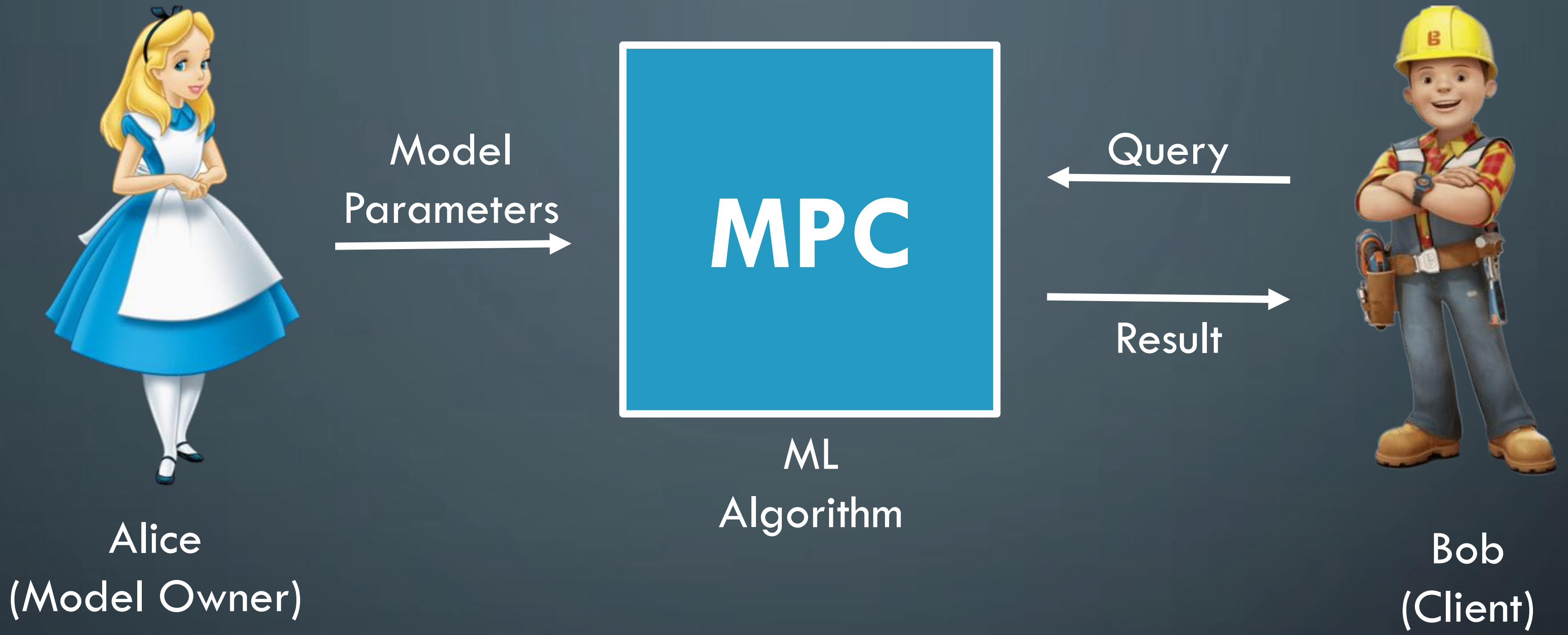
ML

MPC

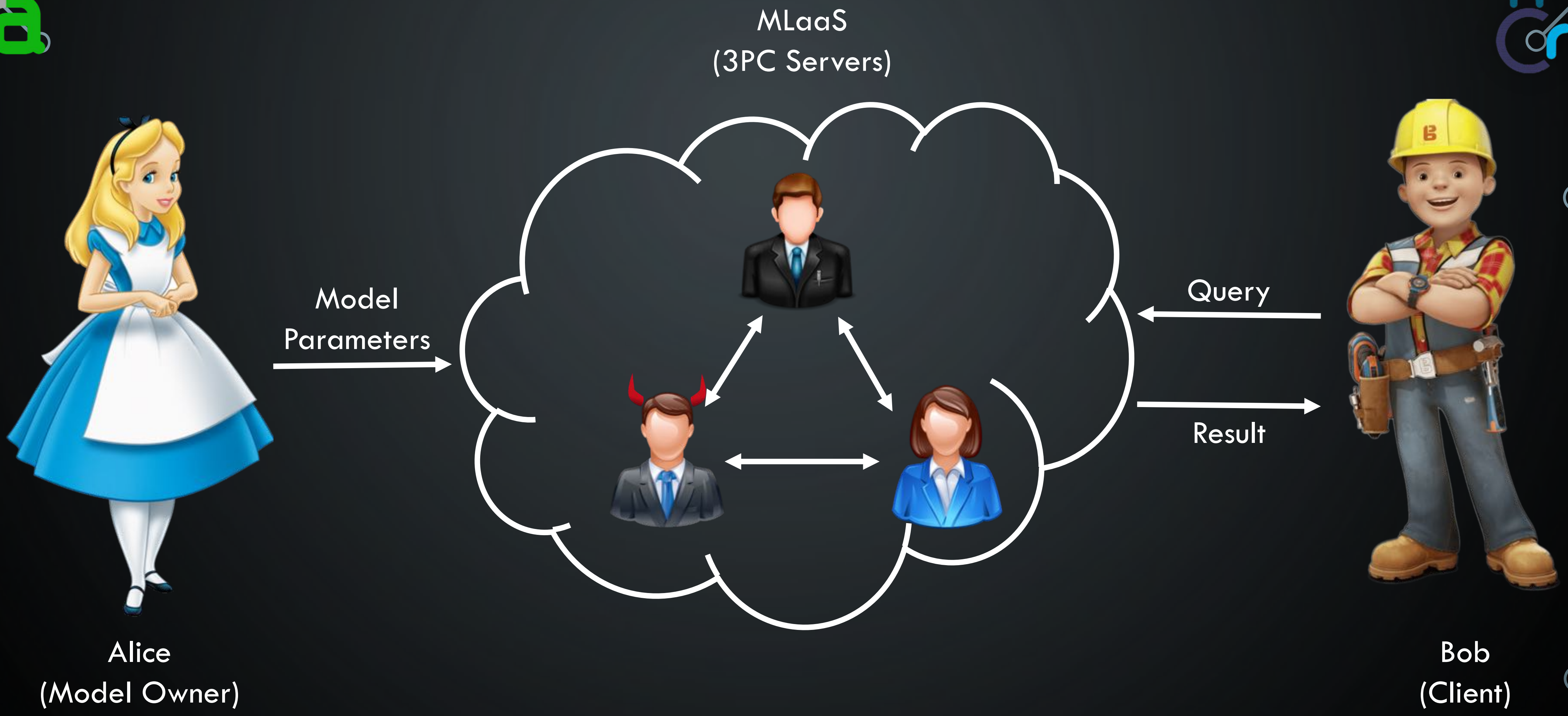
MPC MEETS ML



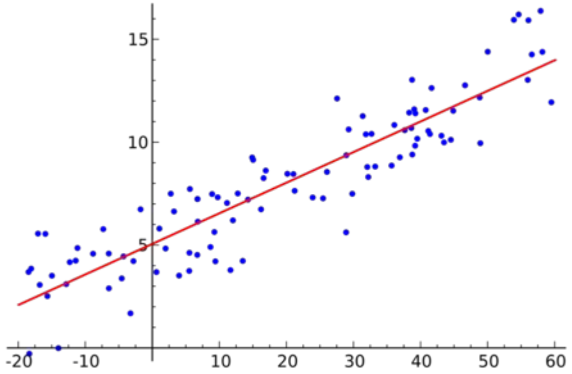
Privacy Preserving Machine Learning (PPML)



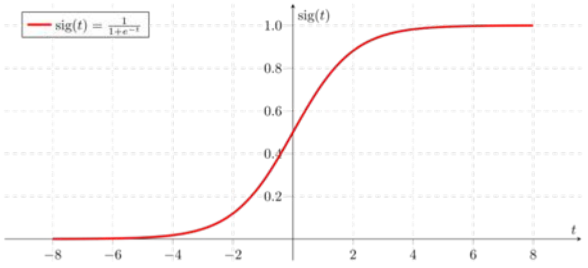
Use MPC to achieve privacy



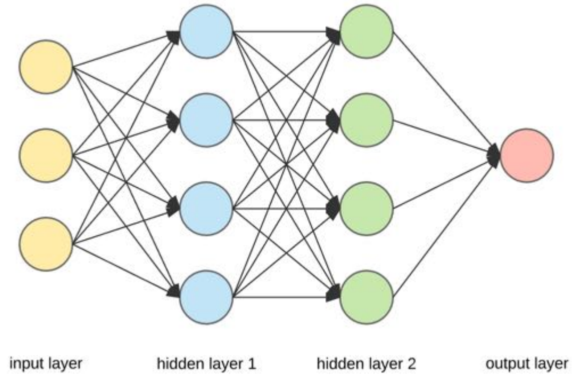
SECURE OUTSOURCED SETTING (SOC)



Linear Regression



Logistic Regression

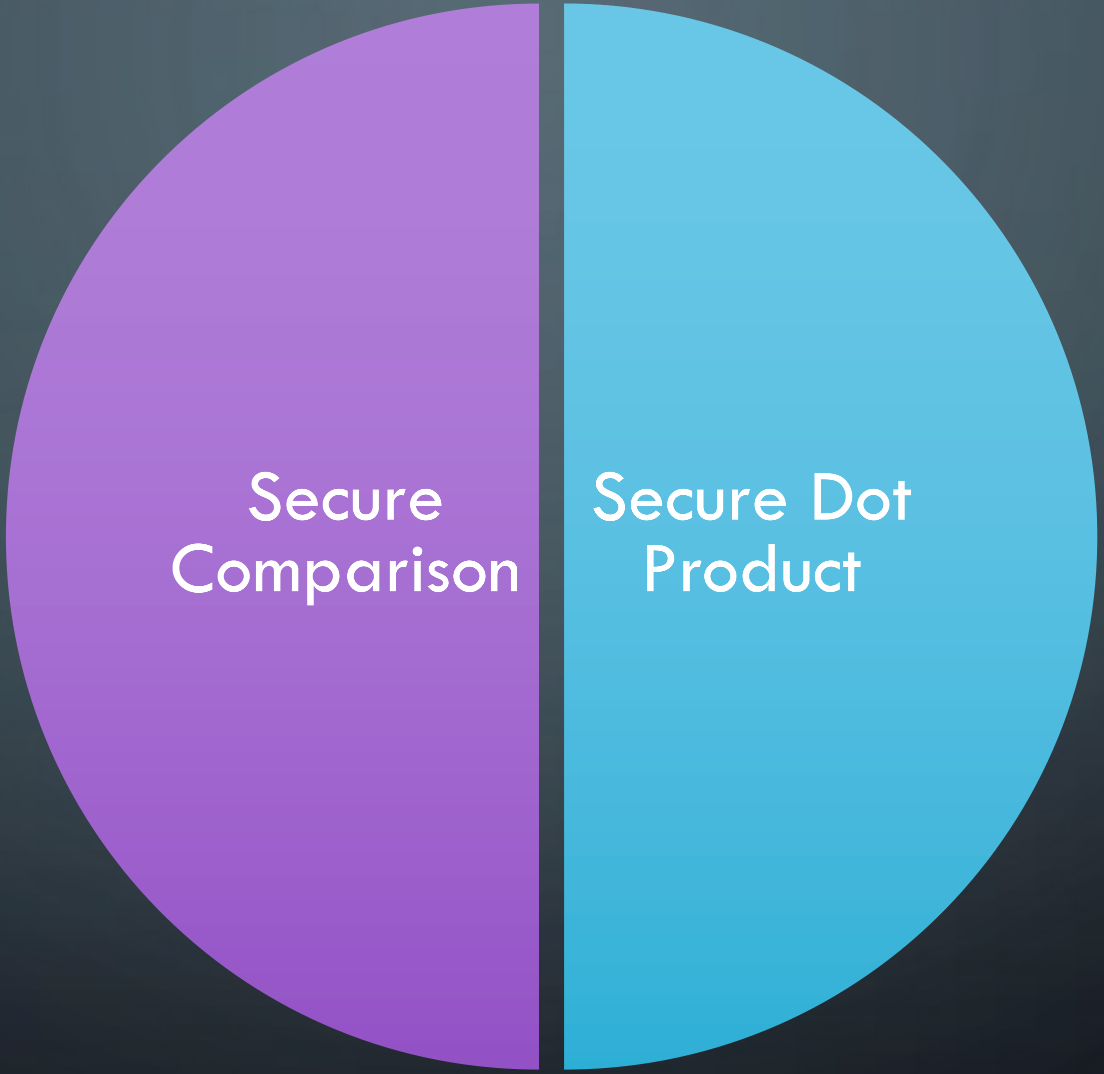


Neural Networks

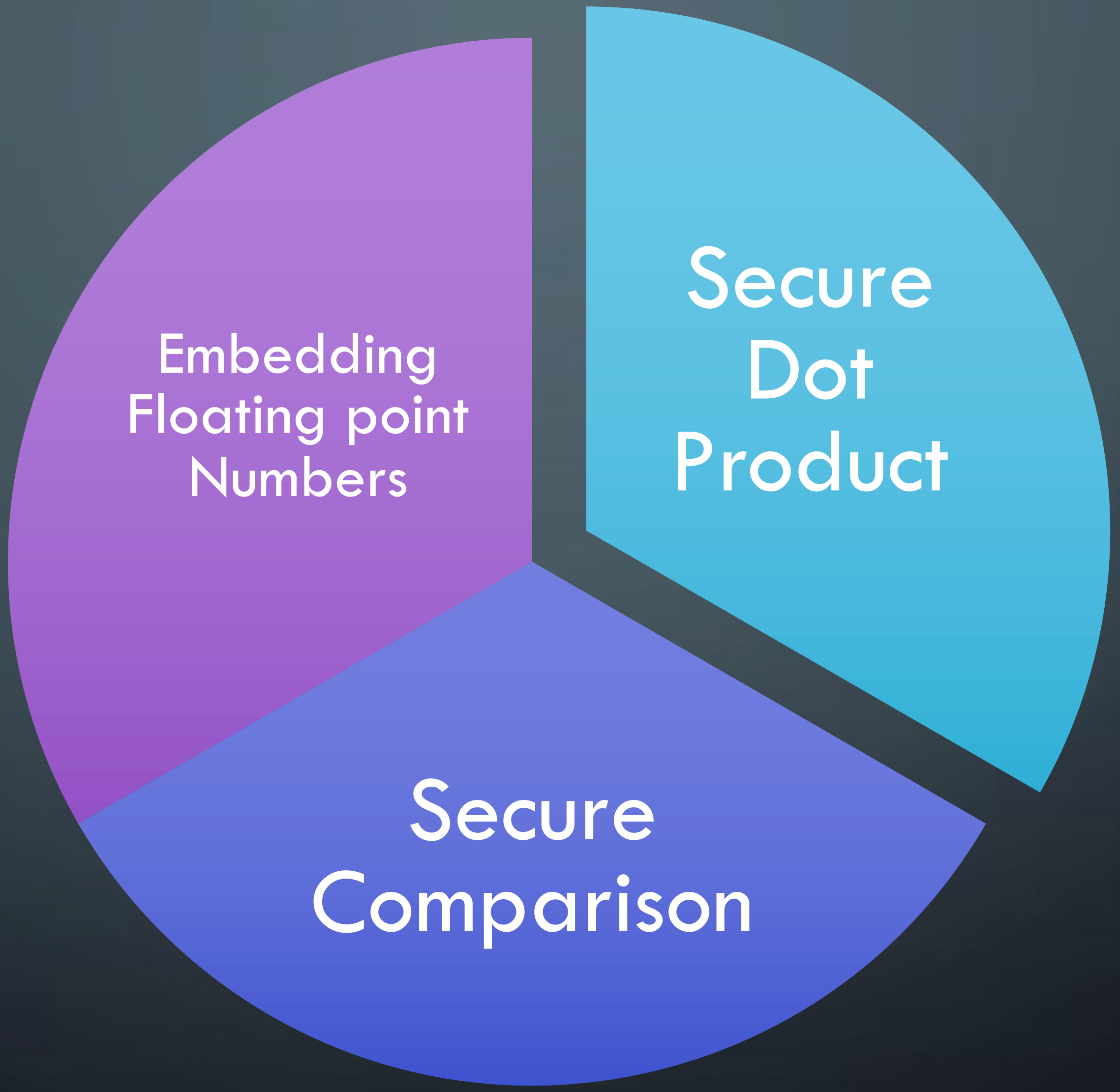
ML ALGORITHMS CONSIDERED

Secure Dot Product

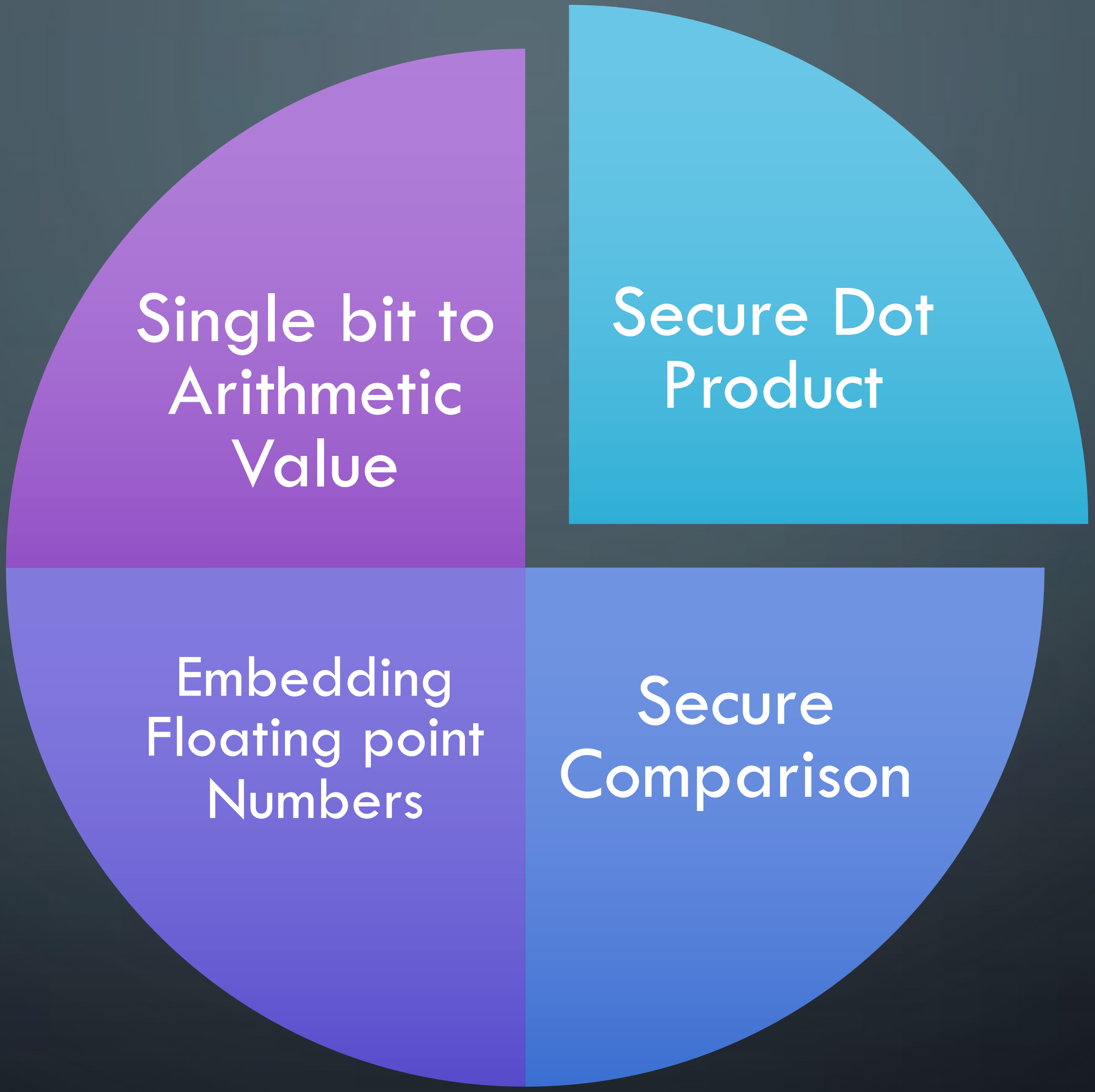
PPML using MPC: Hurdles to Clear



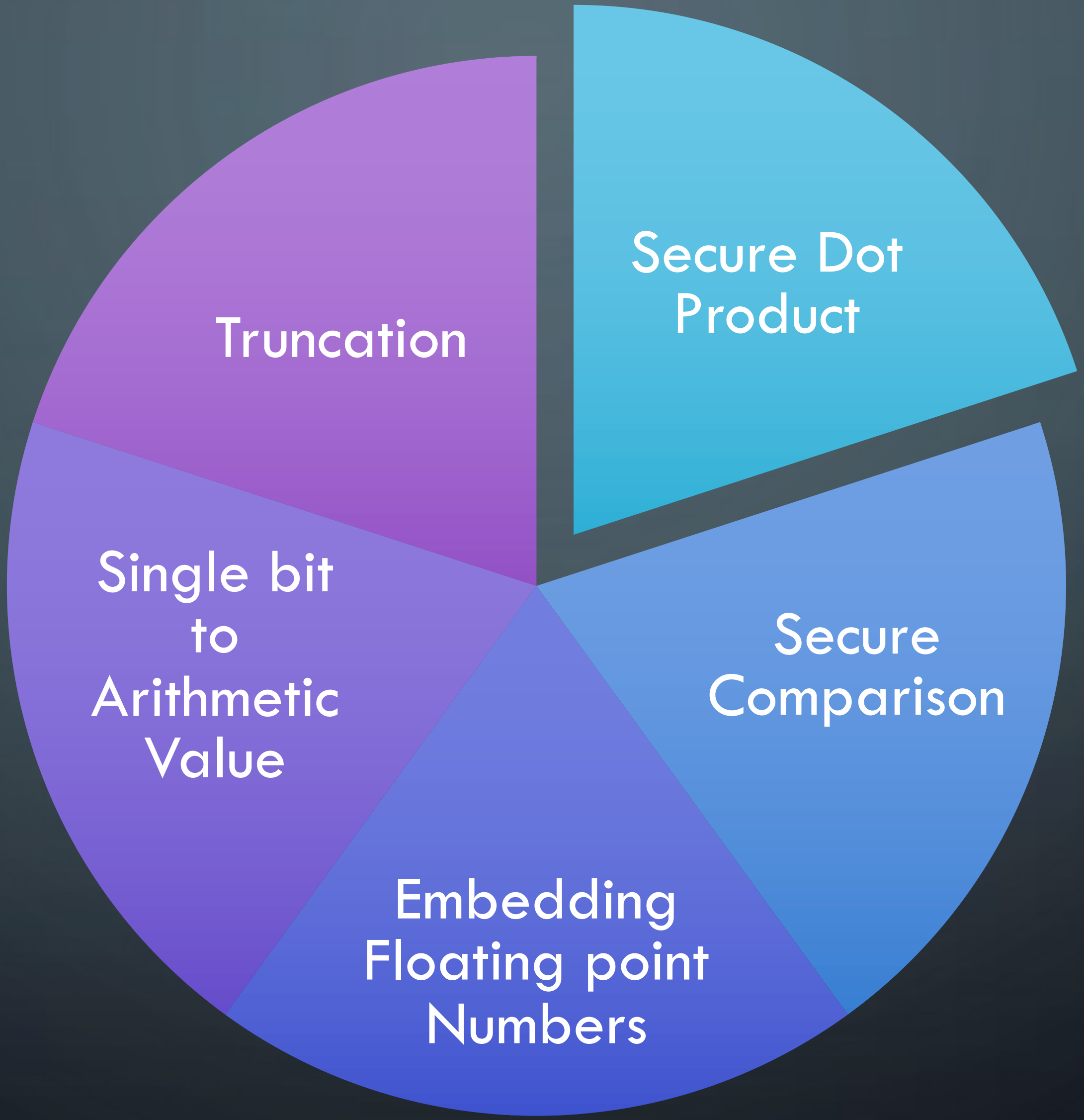
PPML using MPC: Hurdles to Clear



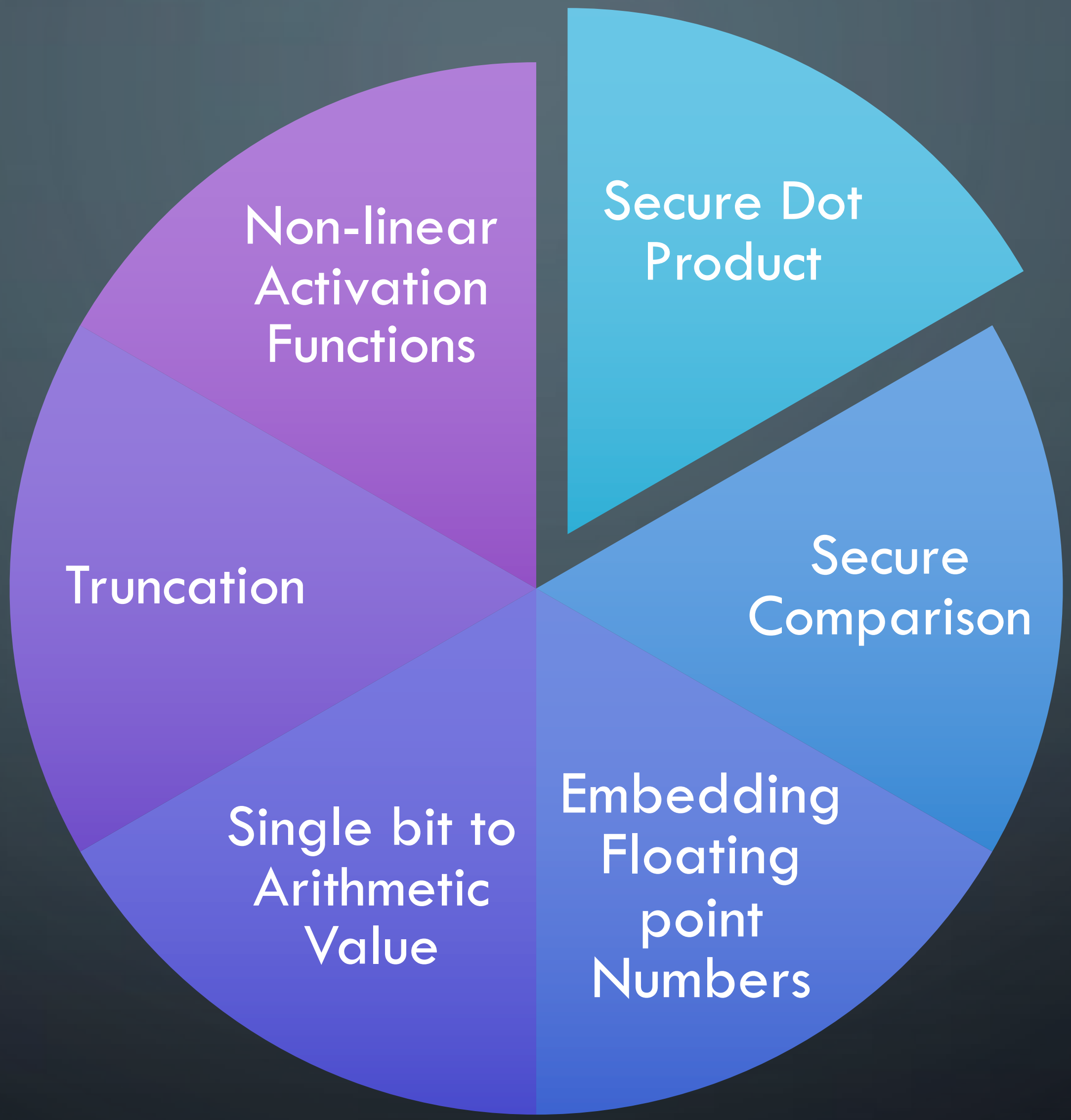
PPML using MPC: Hurdles to Clear



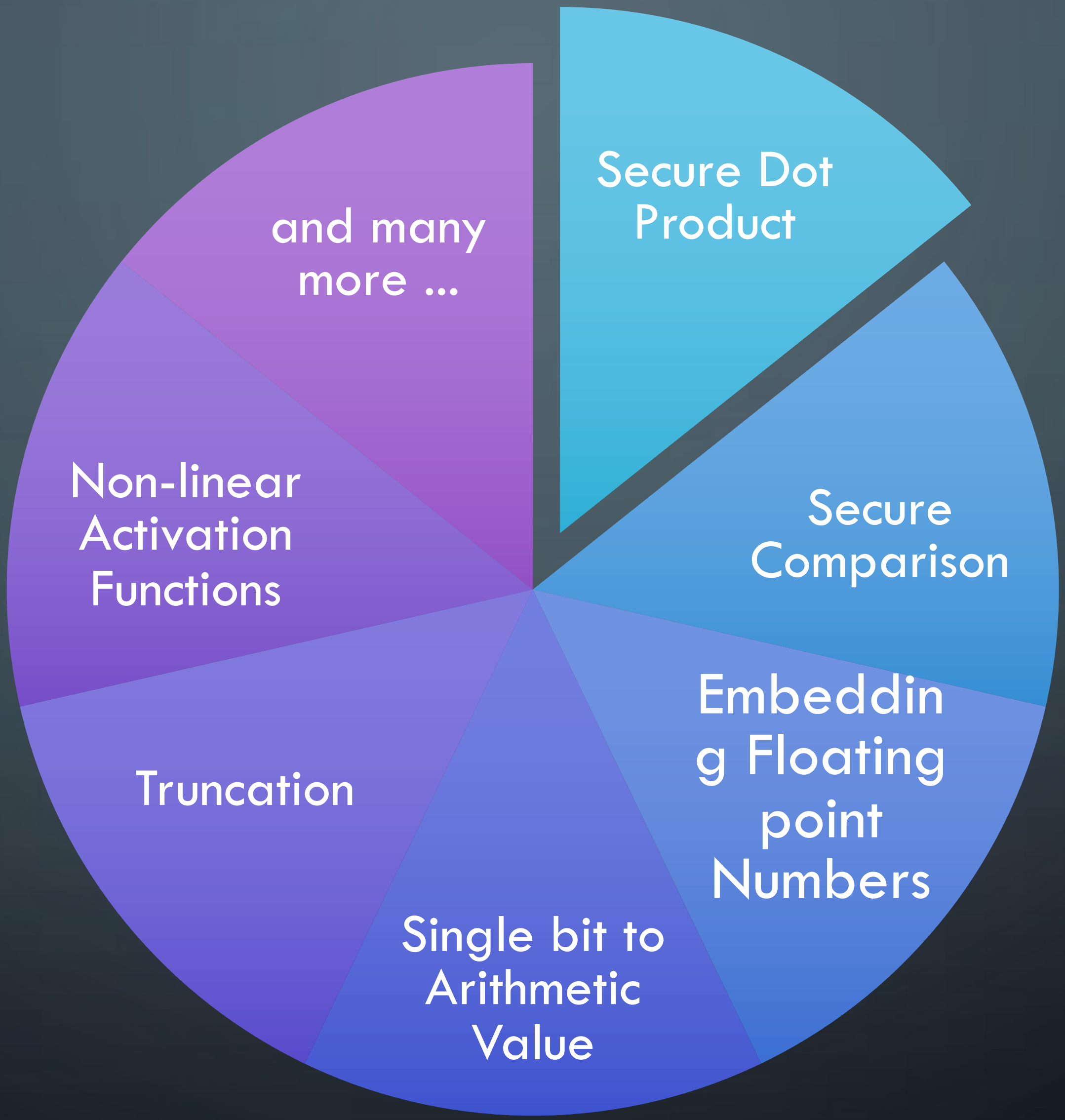
PPML using MPC: Hurdles to Clear



PPML using MPC: Hurdles to Clear



PPML using MPC: Hurdles to Clear



BLAZE Protocol

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

Communication Cost per Dot Product

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

BLAZE : https://eprint.iacr.org/2020/042

d – #elements in each vector

BLAZE Protocol

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

Communication Cost per Dot Product

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

BLAZE : https://eprint.iacr.org/2020/042

d – #elements in each vector

BLAZE Protocol

Ref	Pre-processing (#elements)	Online (#elements)	Security
ABY3	12d	9d	Abort
ASTRA	21d	2d+2	Fair
Boneh et al'19*	0	3d	Abort

Communication Cost per Dot Product

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

BLAZE : https://eprint.iacr.org/2020/042

d – #elements in each vector

BLAZE Protocol

Ref	Pre-processing (#elements)	Online (#elements)	Security
ABY3	12d	9d	Abort
ASTRA	21d	2d+2	Fair
Boneh et al'19*	0	3d	Abort
BLAZE	**3d**	**3**	**Fair**

Communication Cost per Dot Product

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

BLAZE : https://eprint.iacr.org/2020/042

d – #elements in each vector

Summary of Our Benchmarking Results

Algorithm	Improvement in terms of Online Throughput over State-of-the-art protocols over WAN	
	Training	**Prediction**
Linear Regression	333.22 x	194.86 x
Logistic Regression	53.19 x	27.52 x
Neural Networks	-	276.31x

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

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

Summary of Our Benchmarking Results

Algorithm	Ref.	Preprocessing		Online	
		TP	Gain	TP	Gain
Linear Regression	ABY3	61.02		30.61	
	BLAZE	**244.74**	**4.01×**	**4449.55**	**145.35×**
Logistic Regression	ABY3	60.71		60.99	
	BLAZE	**243.81**	**4.02×**	**1945.24**	**31.89×**

TABLE VI: Throughput (TP) for ML Training for a batch size B-128 and feature size n-784

Algorithm	Ref.	Preprocessing		Online	
		TP ($\times 10^3$)	Gain	TP ($\times 10^3$)	Gain
Linear Regression	ABY3	15.57		15.67	
	BLAZE	**62.61**	**4.02×**	**2660.53**	**169.75×**
Logistic Regression	ABY3	15.41		15.55	
	BLAZE	**62.13**	**4.03×**	**366.68**	**23.57×**
Neural Networks	ABY3	0.10		0.14	
	BLAZE	**0.41**	**4.01×**	**33.74**	**245.74×**

TABLE VII: Throughput (TP) for ML Inference for a feature size of n-784

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. D. Boneh, E. Boyle, H. Corrigan{-}Gibbs, N. Gilboa and Y. Ishai. Zero-Knowledge Proofs on Secret-Shared Data via Fully Linear PCPs. In CRYPTO, 2019.