# EDGE AI Academy

## Summer School

7-8 July 2025, Pisa, Italy

# Edge AI Academy Summer School

## PETs for dAIEDGE

**Aysajan Abidin, COSIC KU Leuven, Belgium**

**7-8 July 2025 Pisa, Italy**

# Outline

- Intro to MPC and FHE
- Intro to MPC- and FHE-based PPML
- Challenges

Copyright © 2025

# Privacy Enchancing Technologies

- PETs (in this lecture MPC and FHE) allow computation on encrypted data
  - training and evaluation of AI/ML models on encrypted data

- In general they are more expensive than performing operations in the clear

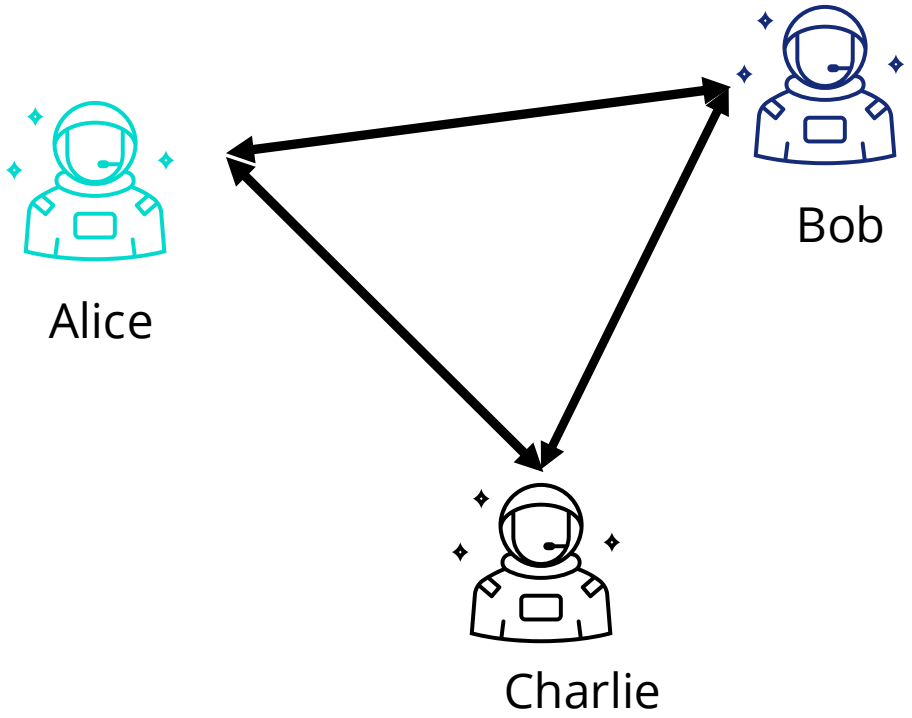
- In both cases the ML algorithm and the MPC/FHE protocol need joint development

- Companies such as Zama, Duality Tech, Cosmian, Enveil, Inpher, Nth Degree, Roseman Labs, etc., are deploying solutions using PETs

Copyright © 2025

# Multiparty Computation (MPC)

- MPC is a technique allowing a group of mutually distrustful parties to jointly compute a function without disclosing their private input

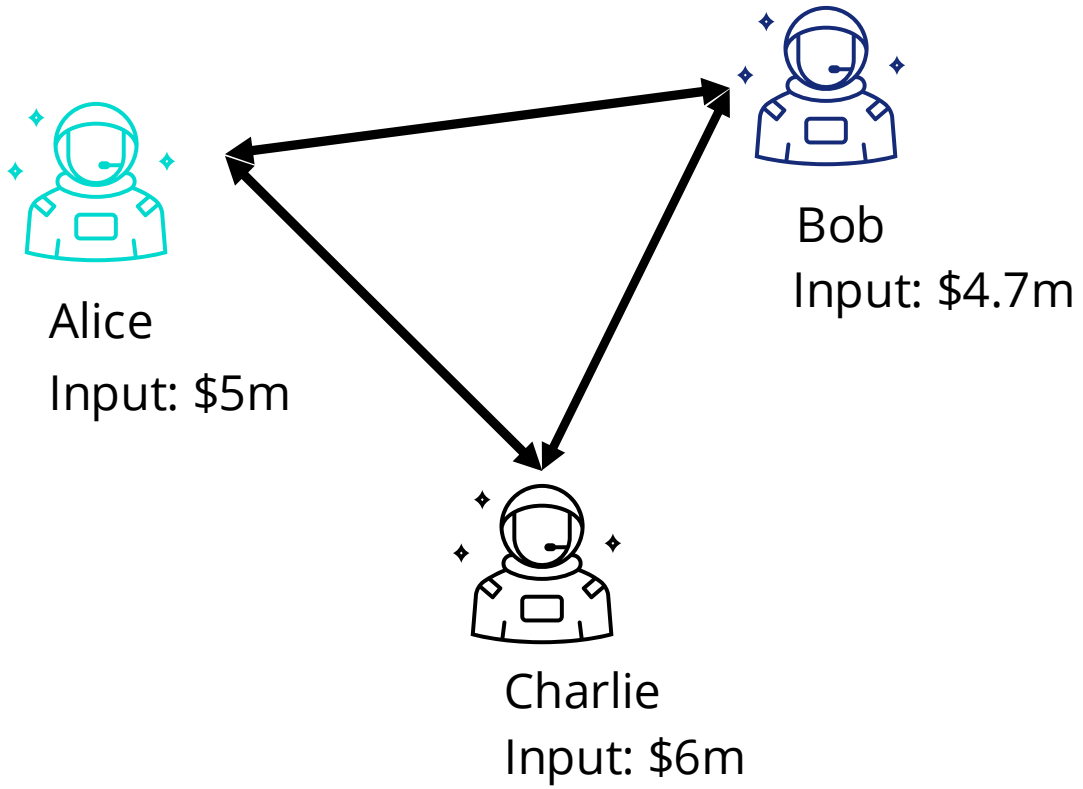



Who is wealthiest?

Copyright © 2025

# Multiparty Computation (MPC)

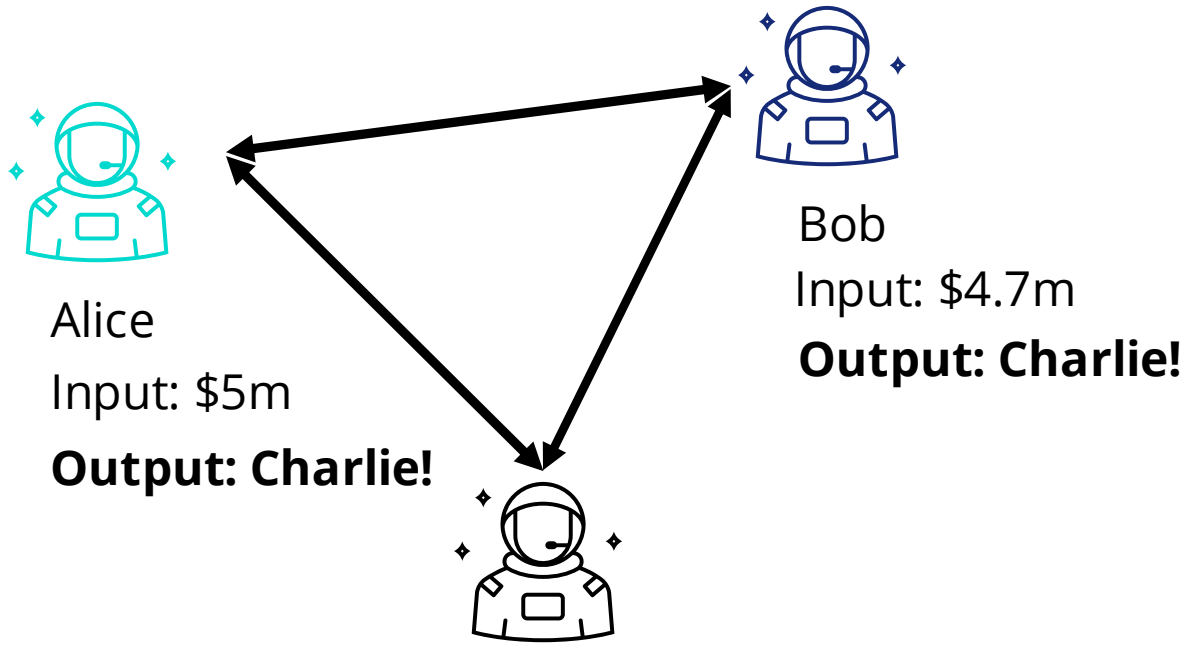
- MPC is a technique allowing a group of mutually distrustful parties to jointly compute a function without disclosing their private input




Copyright © 2025

# Multiparty Computation (MPC)

- MPC is a technique allowing a group of mutually distrustful parties to jointly compute a function without disclosing their private input




Copyright © 2025

# MPC

- Let $f: D \rightarrow R$ be an arbitrary function in $n$-variables $x_1, \ldots, x_n$, s.t.

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

- Suppose there are $n$ parties $P_1$, ..., $P_n$ and each $P_i$ has input $x_i$
- MPC allows $P_1$, ..., $P_n$ to jointly compute $y$ without revealing anything about their private inputs
- Put differently, MPC emulates a *trusted authority* computing $y$

Copyright © 2025

# How does MPC work?

- Garbled Circuits (GC)
- Oblivious Transfer (OT)
- Secret Sharing

Copyright © 2025

# GC

- A GC is an encryption of a binary circuit $C_f$ representing the function $f$ to be evaluated

| $u$ | $v$ | $w$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

$\Longrightarrow$

| $u$ | $v$ | $w$ |
|---|---|---|
| $k_u^0$ | $k_v^0$ | $k_w^0$ |
| $k_u^0$ | $k_v^1$ | $k_w^0$ |
| $k_u^1$ | $k_v^0$ | $k_w^0$ |
| $k_u^1$ | $k_v^1$ | $k_w^1$ |

| |
|---|
| $E^s_{k_u^1,k_v^1}(k_w^1)$ |
| $E^s_{k_u^1,k_v^0}(k_w^0)$ |
| $E^s_{k_u^0,k_v^0}(k_w^0)$ |
| $E^s_{k_u^0,k_v^1}(k_w^0)$ |

Copyright © 2025

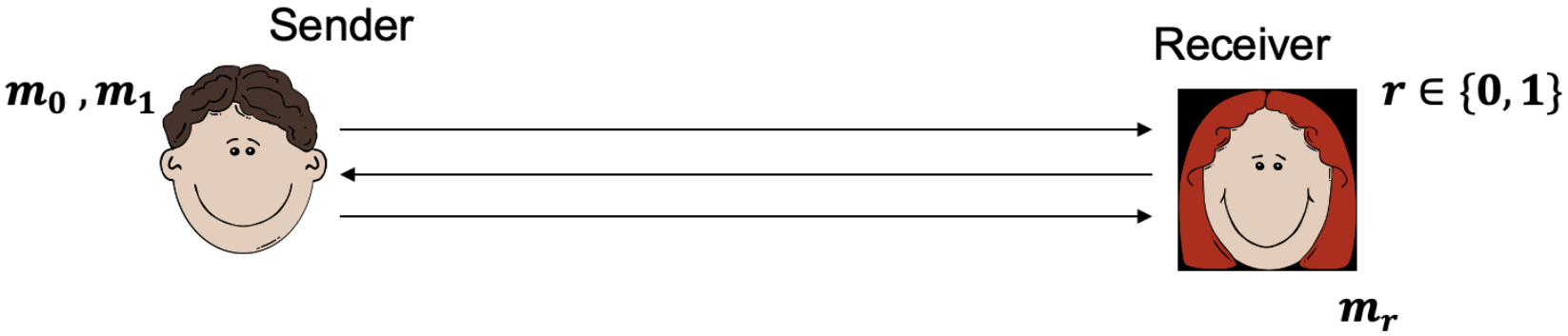
# MPC from GC

- Yao introduced GC as 2PC (1982)
  - Garbler – picks garbled values $(k_u^0, k_u^1)$, for all wires $u$ of $C_f$, creates a garbled circuit $C_f'$ using these garbled values, sends $C_f'$ and $k_u^x$
  - Evaluator – evaluates $C_f'$ using $k_u^x$ and $k_u^y$, after obtaining $k_u^y$ from the Garbler via OT

Copyright © 2025

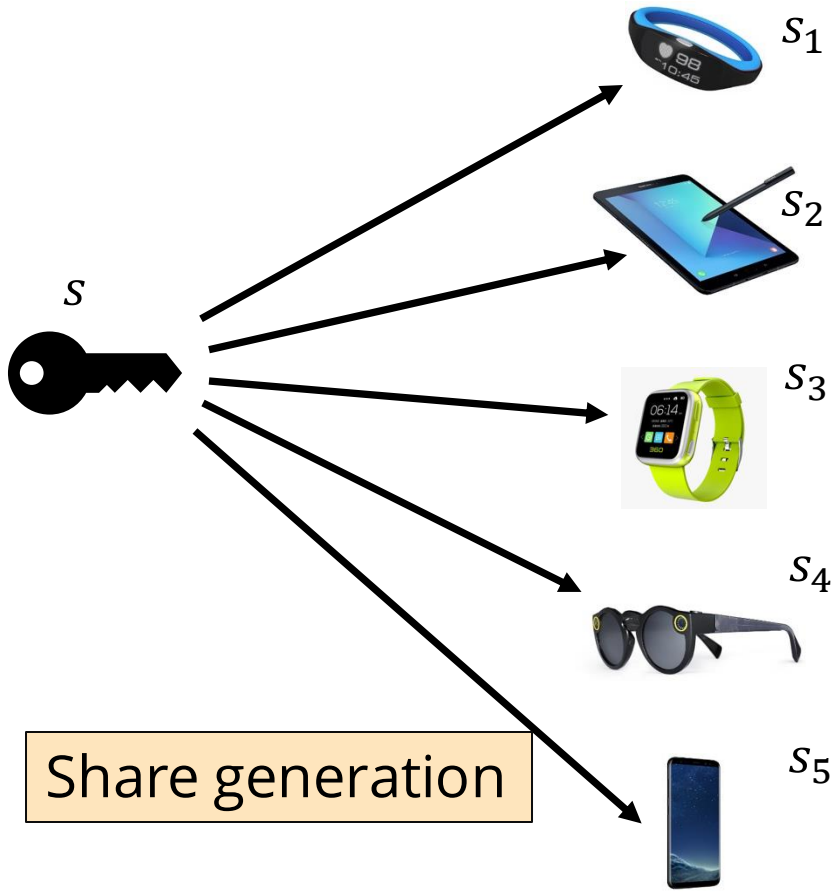
# OT

- OT is a cryptographic primitive designed to transfer specific data based on the receivers choice
- No other information can be learned by any party




Copyright © 2025

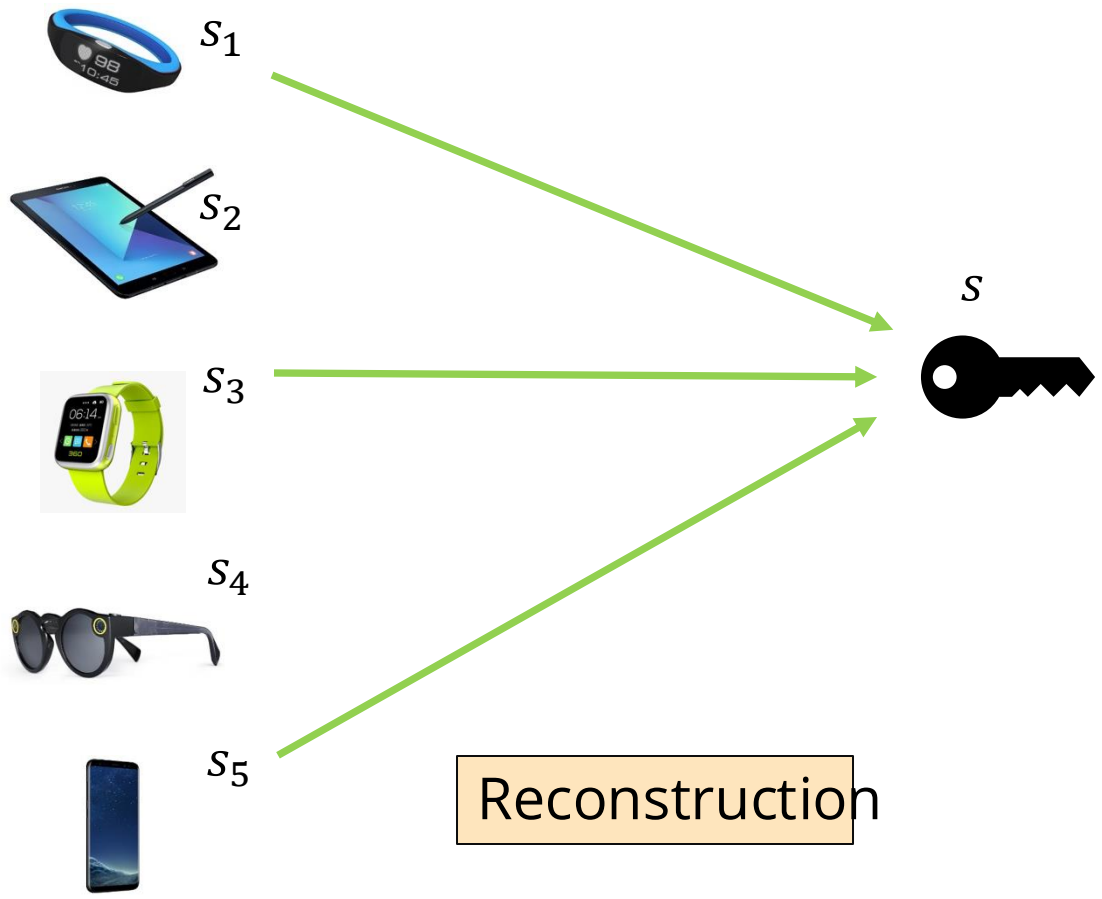
# Secret Sharing




3 out of 5 secret sharing

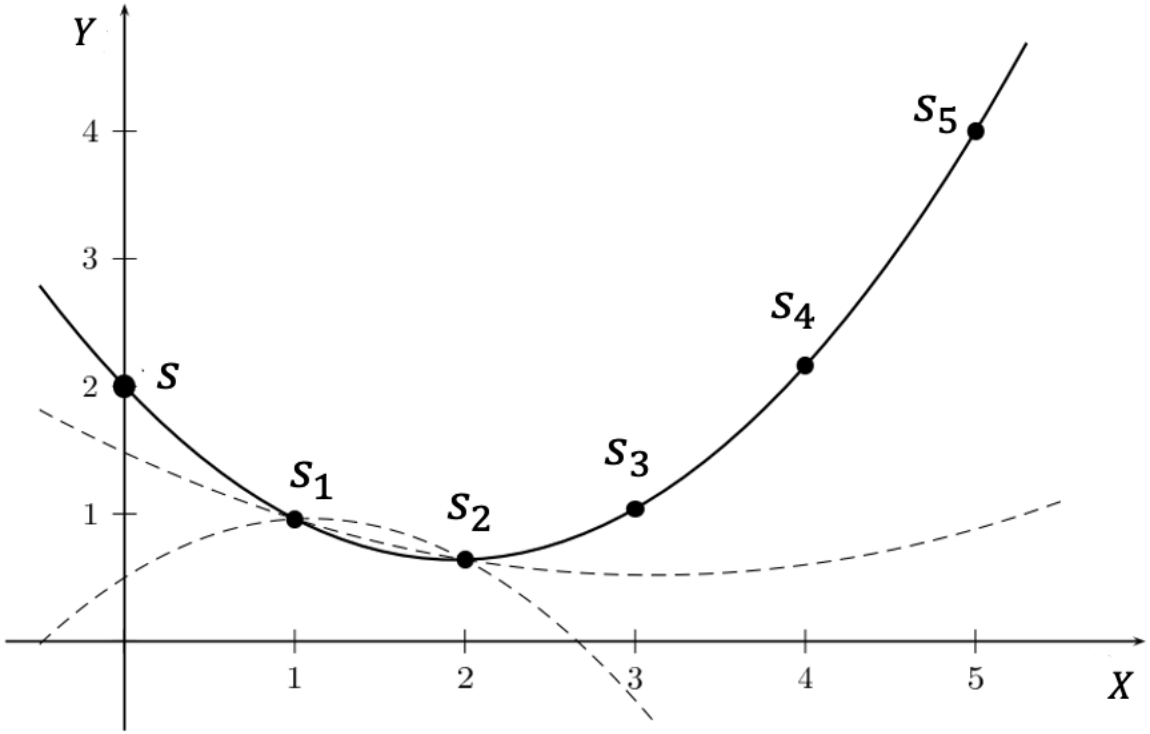
Copyright © 2025

# Secret Sharing




Copyright © 2025

# Secret Sharing




Copyright © 2025

# MPC adversary model

- Two types of adversaries
  - Semi-honest, a.k.a., honest-but-curious or passive
    - Follows the protocol, but attempts to learn private information
  - Dishonest, a.k.a., malicious or active
    - Arbitrarily deviates from the protocol

- Adversarial strategies
  - Static – corrupted parties fixed throughout the protocol execution
  - Adaptive – adversary chooses which party to corrup during the protocol execution

Copyright © 2025

# MPC – computation model

- Works over
  - Rings
  - Fields
  - Field Extensions
- Online (function dependent/independent) & Offline
- Online only

Copyright © 2025

# MPC security

- Adversarial power
  - Unconditional
  - Computational
- Corruption
  - Honest majority
  - Dishonest majority
- Semi-honest security
- Dishonest security
- Covert security

Copyright © 2025

# MPC output guarantees

- Guaranteed output delivery (GOD)
- Security with abort
- Fairness

Copyright © 2025

# MPC

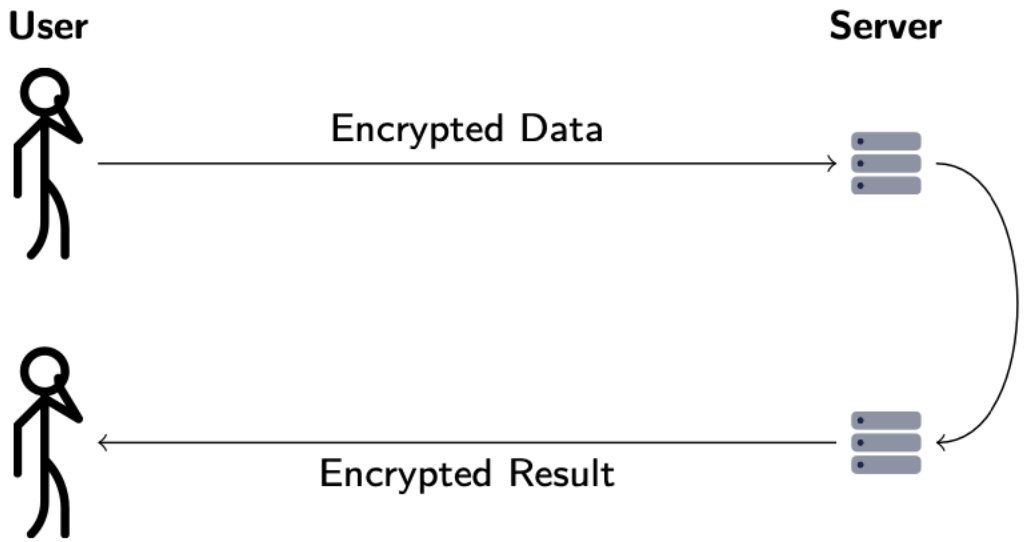
- Properties (or goals)
  - Correctness
  - Privacy

- Requires communication among the parties
  - How many rounds of communication?
  - How much data is exchanged?

Copyright © 2025

# FHE

- FHE allows meaningful computations on encrypted data
- It enables secure outsourcing of computations to untrusted parties
  - PPML




[Credit to Leonard Schild]

Copyright © 2025

# (Partially) Homomorphic encryption

- **RSA (1977)**:
  - Key generation: Pick primes $p$, $q$, $N = pq$ and choose $e$ and $d$ such that
    - $d = e^{-1} \pmod{(p-1)(q-1)}$
  - Encryption: $c = m^e \ mod \ N$
  - Decryption: $m = c^d \ mod \ N$
  - Homomorphic property:
    - $Enc(m_1) \cdot Enc(m_2) = m_1^e \cdot m_2^e = (m_1 \cdot m_2)^e = Enc(m_1 \cdot m_2)$

- Others
  - **Paillier Cryptosystem (1999)** – additive
  - **ElGamal (1985)** – multiplicative

Copyright © 2025

# FHE

- Gentry introduced the first FHE construction in 2009
  - Impractical

- There are a number of well-established schemes since then
  - **TFHE/FHEW**: suitable for small messages
  - **BFV/BGV**: Exact arithmetic
  - **CKKS**: Supports approximate arithmetic

- Current research focuses
  - reducing the key size
  - improving performance

Copyright © 2025

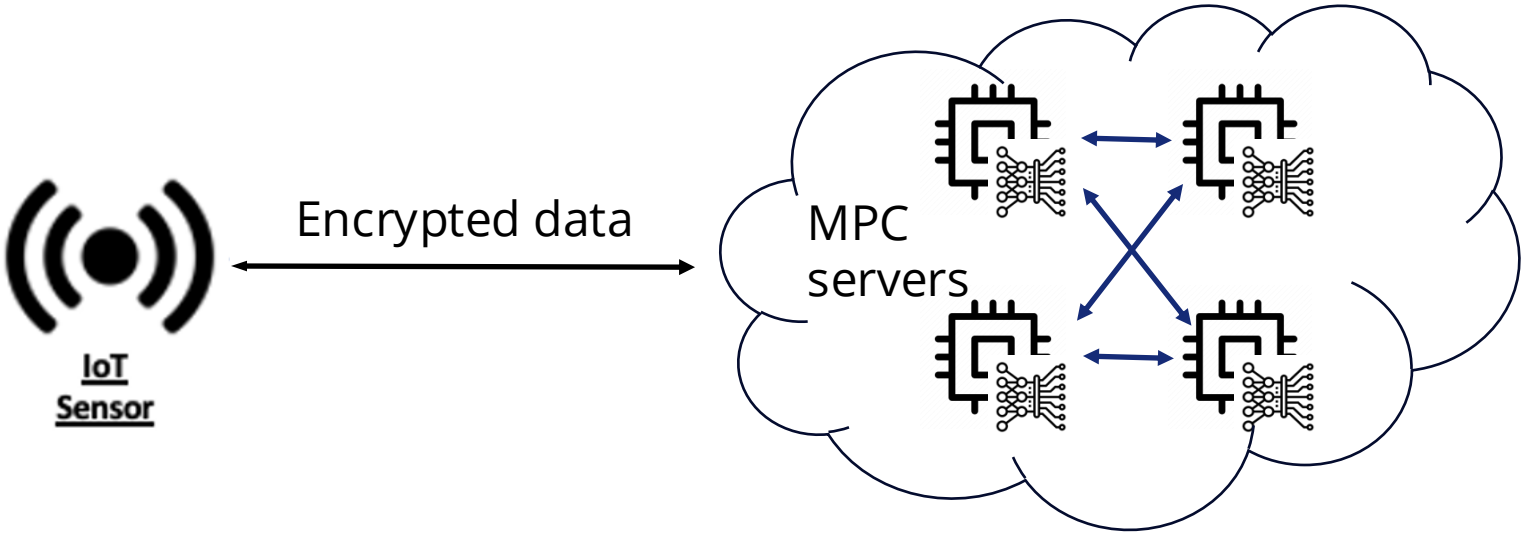
# MPC-based PPML

- Secure training
  - Multiple parties with their own data train a model on the combined dataset
  - Goal: no party learns another party's data

- Secure inference
  - ML inference on encrypted queries
  - ML-as-a-Service

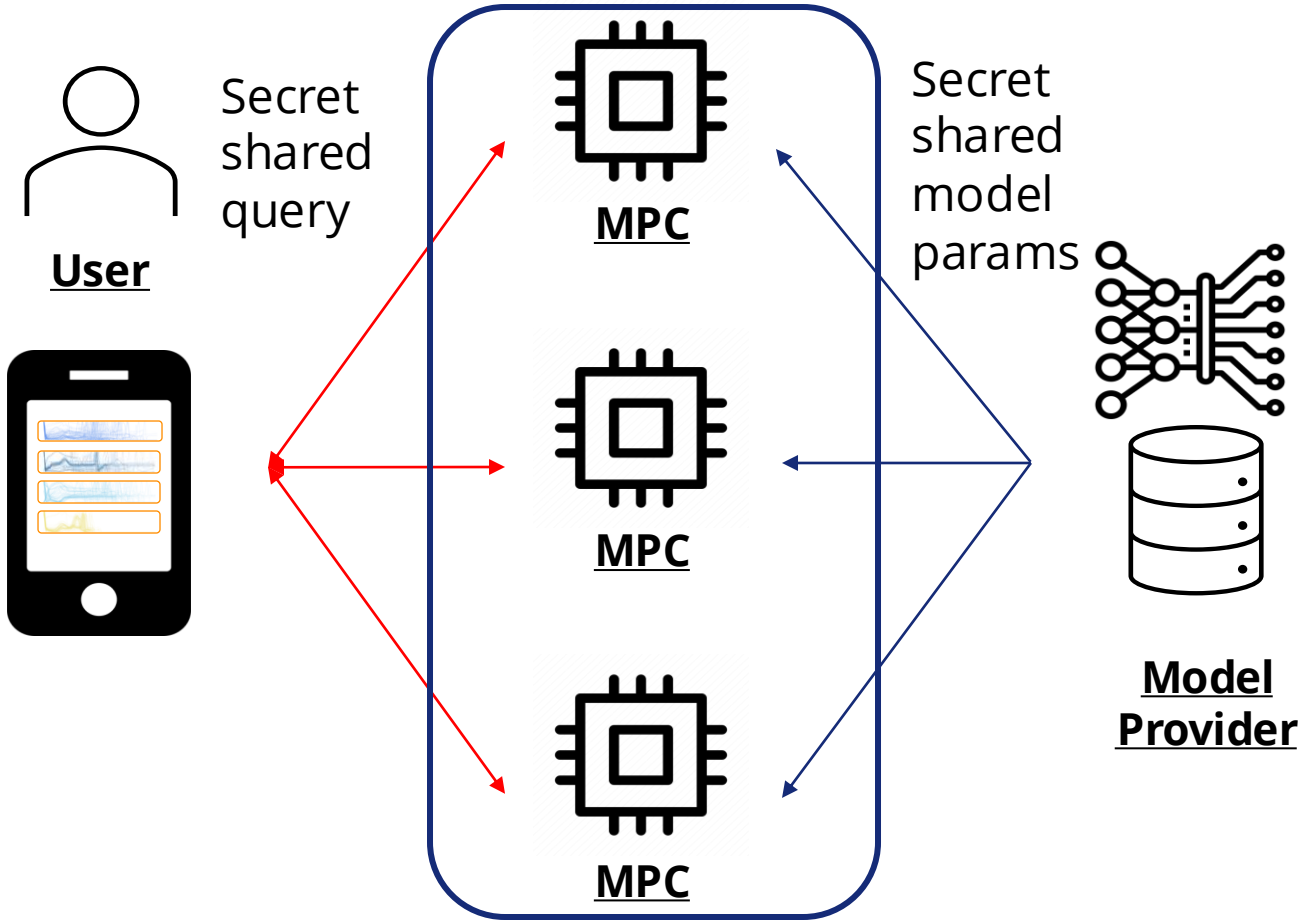
Copyright © 2025

# MPC-based PPML: secure training




Copyright © 2025

# MPC-based PPML: secure inference




Copyright © 2025

# MPC-based PPML: challenges

- Handling real numbers
  - Fixed-point arithmetic vs floating-point arithmetic
- Field vs Ring
- Efficient protocols for
  - Matrix multiplication
  - Truncation
  - Activation functions
  - Secure comparison
  - Dot-product
  - Share conversion
  - Oblivious selection
  - …

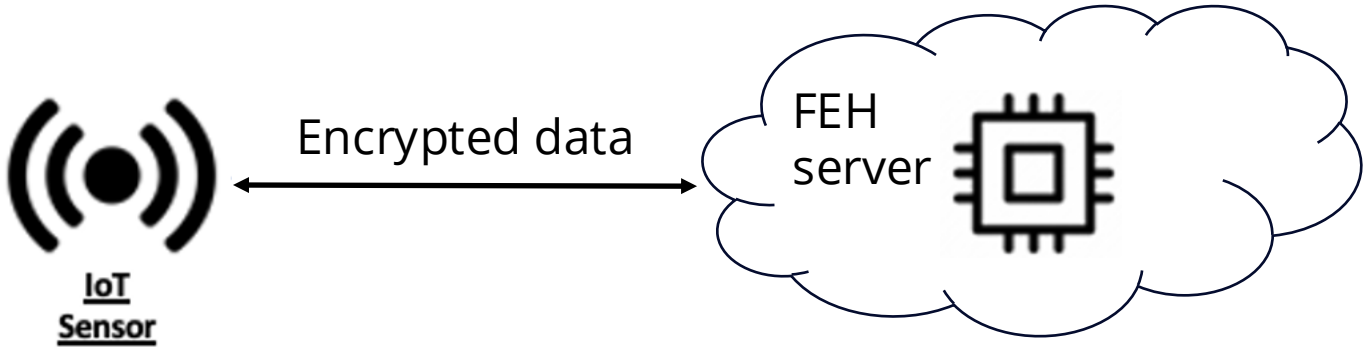
Copyright © 2025

# MPC-based PPML: challenges

- Handling real numbers
  - Fixed-point arithmetic vs floating-point arithmetic
- Field vs Ring
- Efficient protocols
- Cost
  - Communication
  - Computation
- Performance

Copyright © 2025

# FHE-based PPML




Copyright © 2025

# FHE-based PPML: challenges

- Model representation
  - FHE deals with modular arithmetic operations for integers
  - Fixed- and floating-point arithmetic
- Matrix multiplications (or tensor operations)
- Dot-product
- Non-linear functions
  - Actication functions
  - Max pooling
- Scheme switching
  - Different FHE schemes for linear and non-linear layers for better efficiency

Copyright © 2025

# Conclusions

- PETs are crucial for secure AI at the edge
  - MPC → collaborative computation
  - FHE → encrypted inference
- Real-world tools exist, but trade-offs remain
- Ongoing research focus on making PETs practical and scalable
- FHE/MPC in combination with a judicious choice of AI/ML algorithms
  - Pros: feasible and privacy can be guaranteed
  - Cons: computational and communication costs are higher


Copyright © 2025

# Thank You

@ Name.Name@name.eu

https://edge-ai-tech.eu/

The two-day innovative educational initiative is designed for students, young researchers, and professionals eager to expand their understanding and skills in these cutting-edge technologies.

Participants will engage in interactive discussions, hands-on sessions, and lectures covering foundational concepts and innovative applications of edge AI across various domains with leading experts, gain insights into real-world applications, and work on team-based projects to foster collaboration and innovation.

Copyright © 2025

# EDGE AI Academy 2025

## Summer School Objectives

- The EDGE AI Academy Summer School aims to empower participants with advanced knowledge, hands-on experience and an in-depth understanding of edge AI, which combines Artificial Intelligence (AI) with edge computing and the Internet of Things (IoT) to process data closer to its source.
- Edge AI technology is gaining prominence due to its ability to enhance real-time decision-making, reduce latency, improve data privacy, and diminish reliance on continuous internet connectivity.
- The topics will extend to RISC-V architectures as ultra-low-power high-performance RISC-V-based processors and ultra-low-power vector-based accelerators are advancing smart IoT and edge AI computing capabilities.

Copyright © 2025