A Gentle Introduction to Secure Computation

Eleftheria Makri| lunch talk – Digital Security group, Radboud University 19/01/2024

Universiteit Leiden

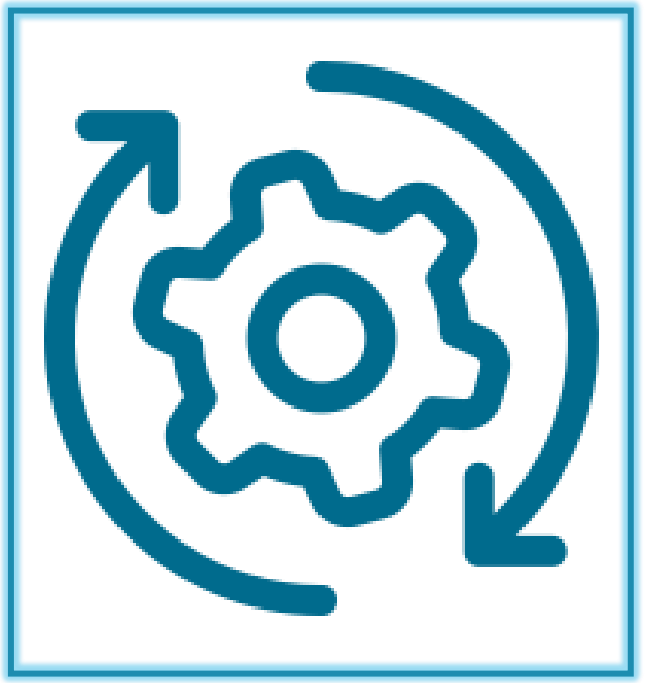
Privacy Enhancing Technologies

The Three States of Data

Data in Transit

Data at Rest

Data in Use



The Three States of Data

Data in Transit

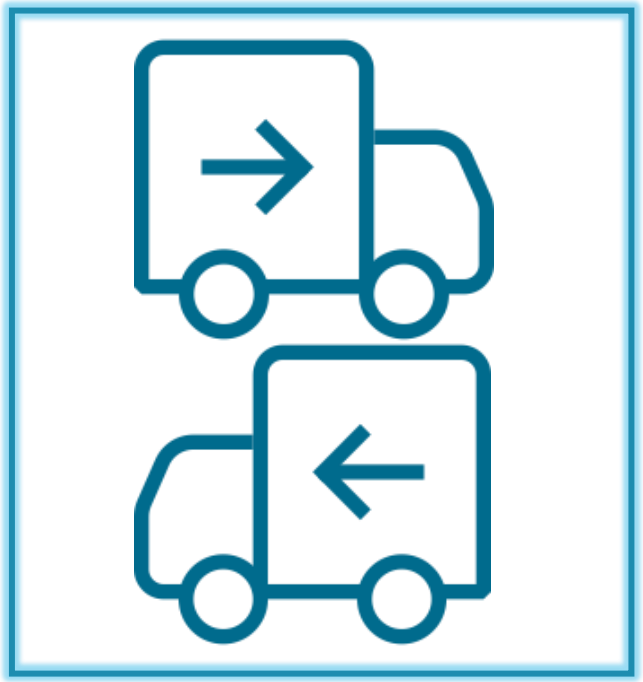
Data at Rest

Data in Use

Traditional Cryptography

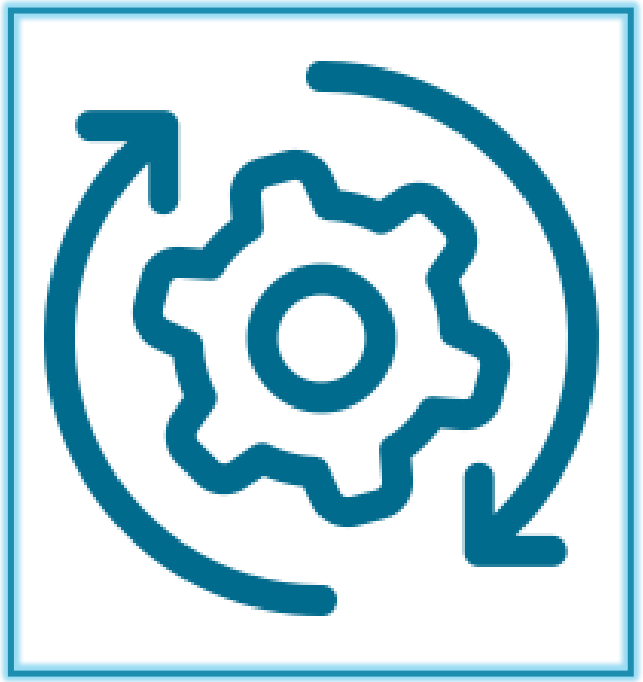
The Three States of Data

Data in Transit



Data at Rest

Data in Use



Traditional Cryptography

Secure Computation Technologies

Data in Use

Autonomous Driving

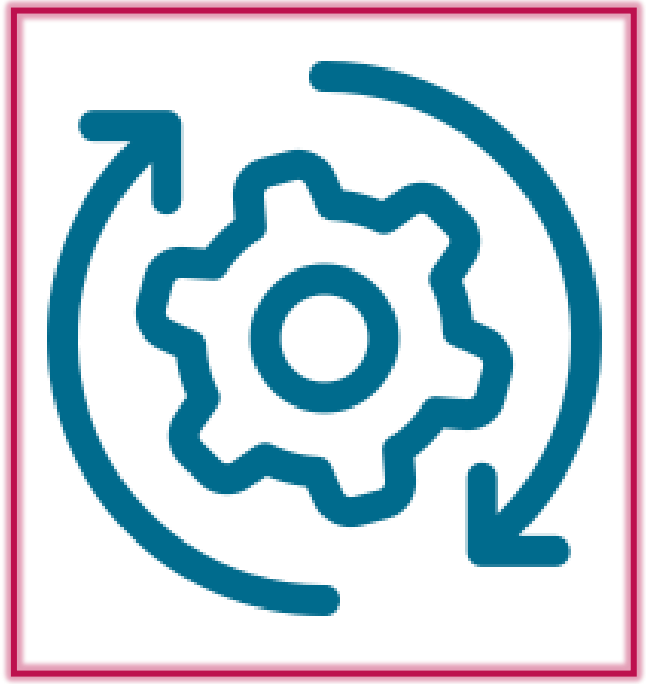
Internet of Things

Smart Cities

Online Social Networking

Medical Research

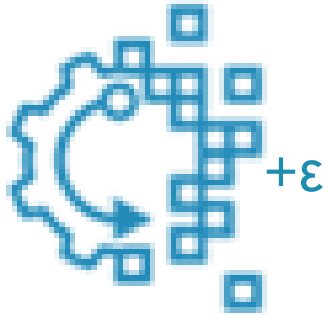
Data in Use



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

Securing Data in Use – PETs

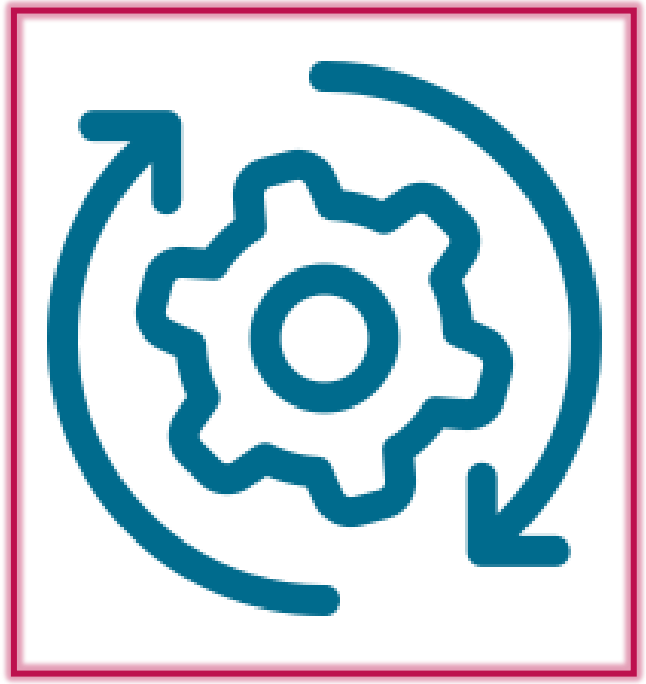
Data Anonymization



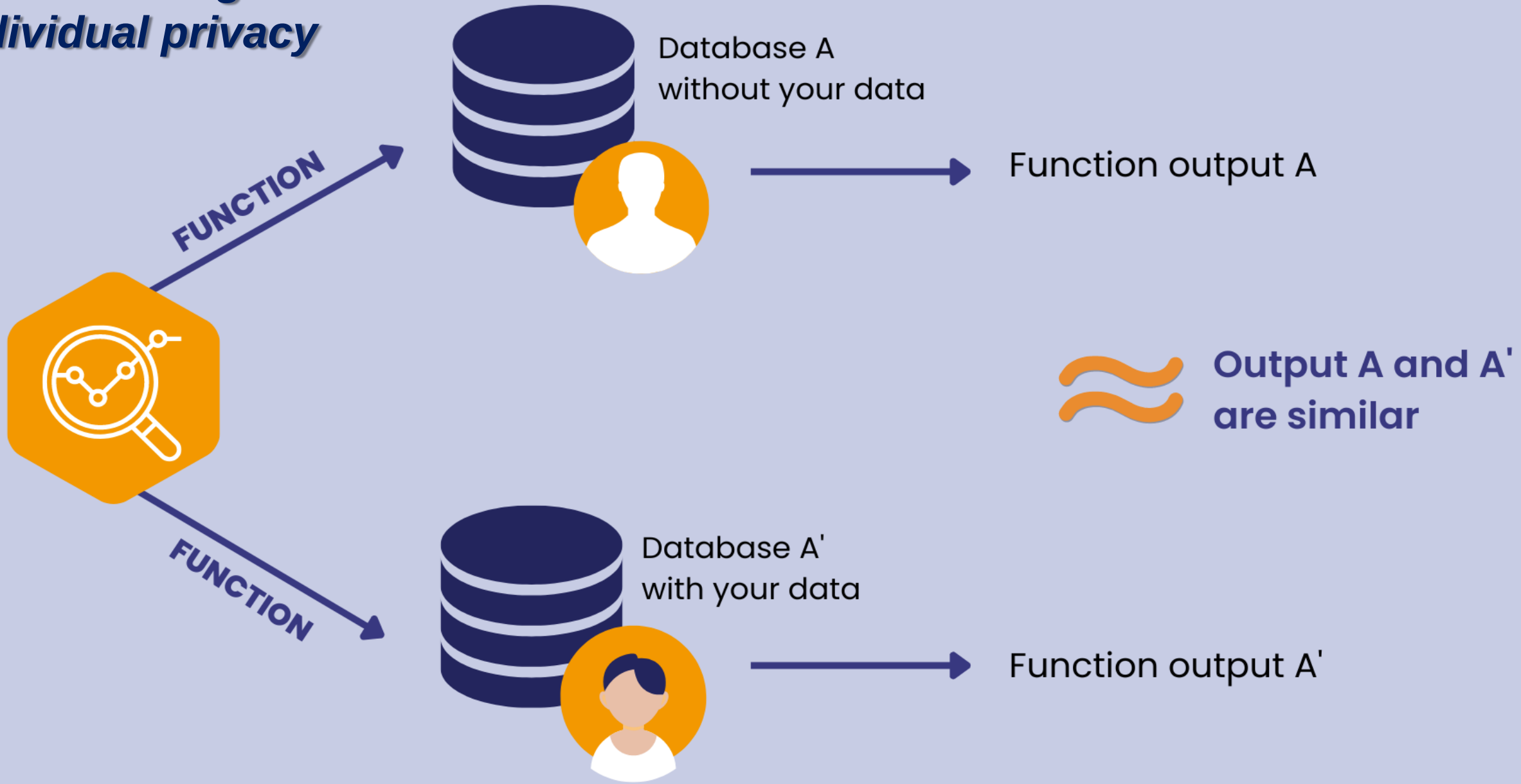
Differential Privacy

Cryptographic Techniques
for Secure Computation

Data in Use



DP – Ensuring individual privacy



DP – Ensuring individual privacy

FUNCTION

SENSITIVITY

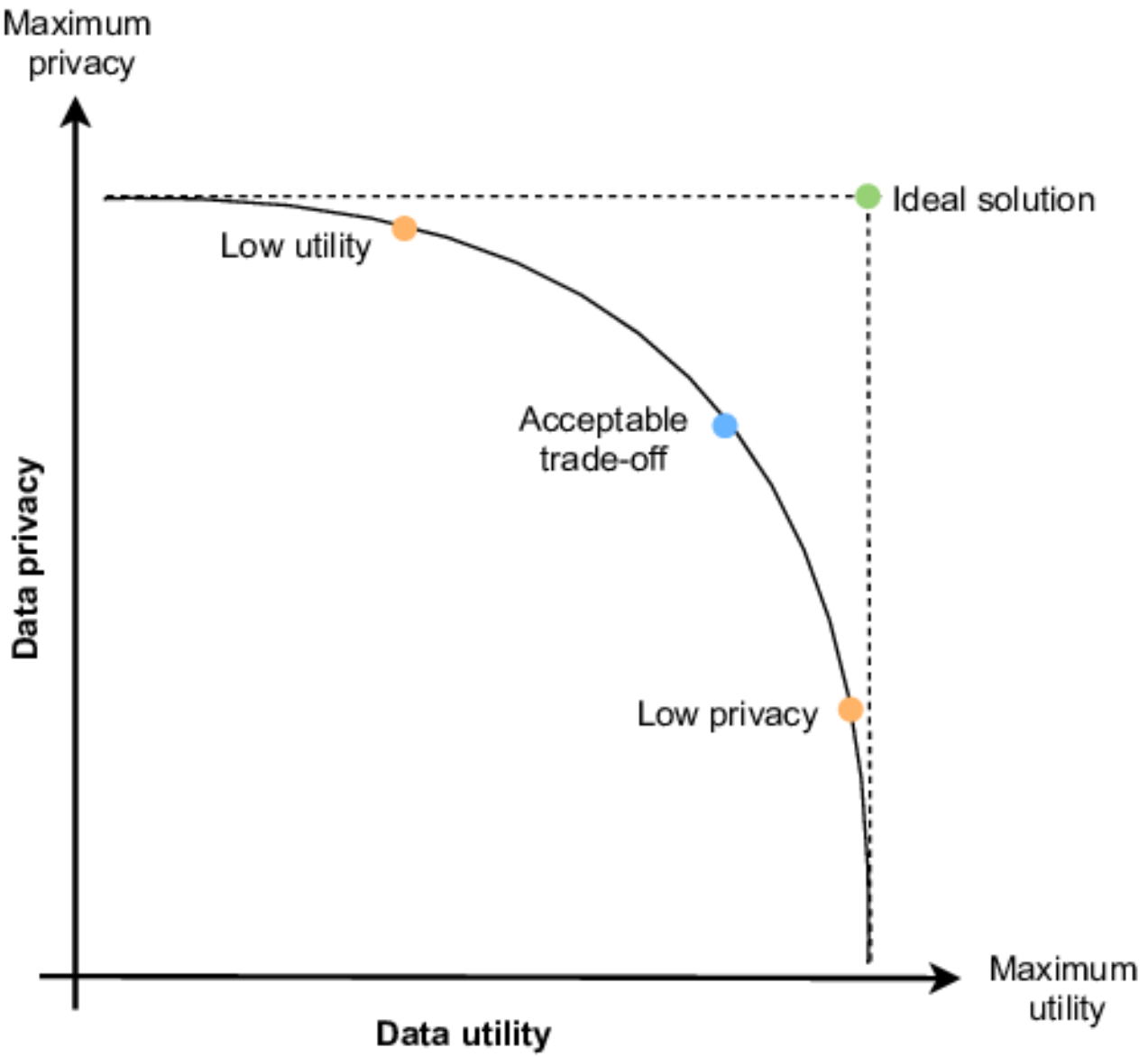
Determine the function sensitivity

Choose a noise addition mechanism

DATA WITH NOISE

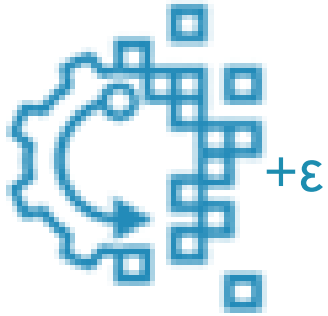
DP - The Penalties

- Inherent information leakage, called privacy budget in DP terms.
- Inherent tradeoff between data privacy and data utility



Securing Data in Use – PETs

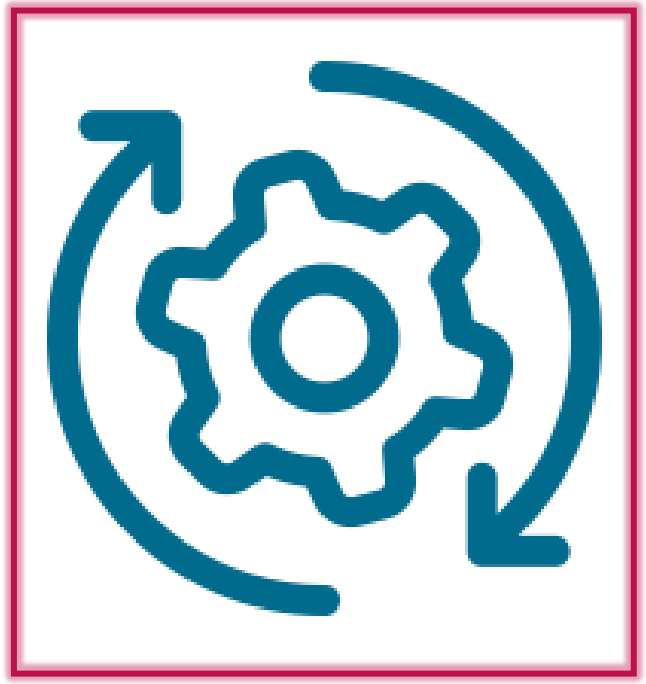
Data Anonymization



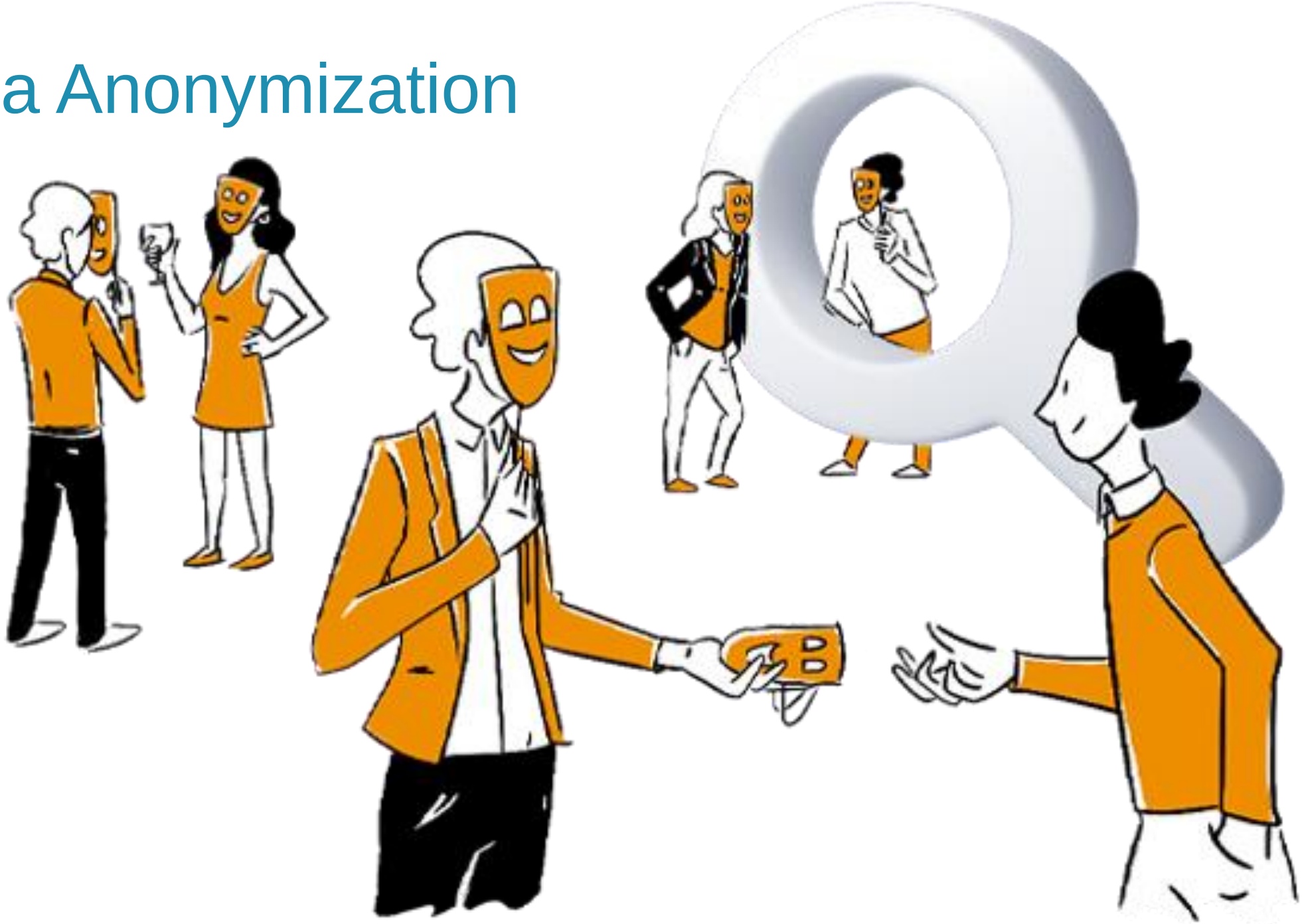
Differential Privacy

Cryptographic Techniques
for Secure Computation

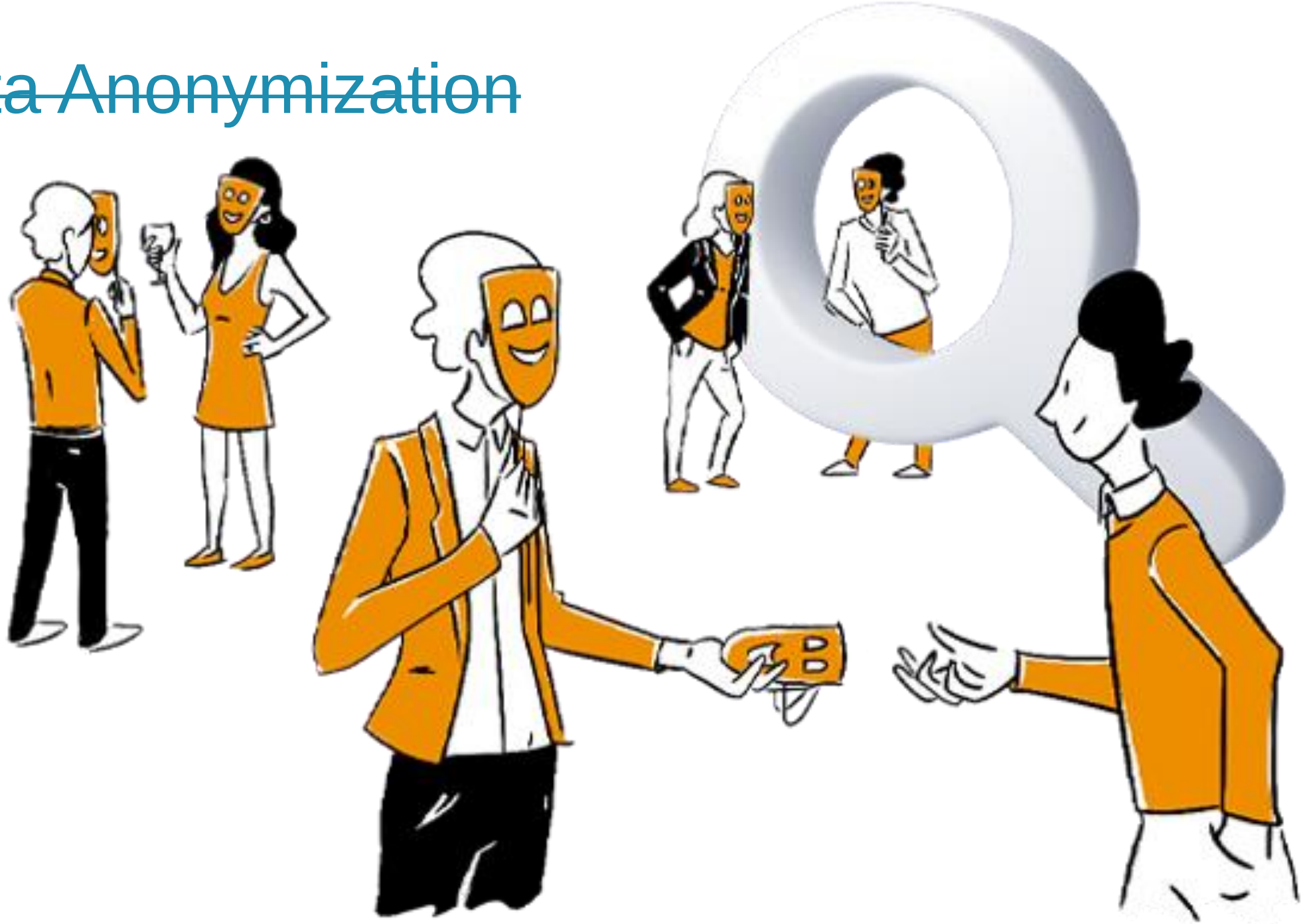
Data in Use



Data Anonymization

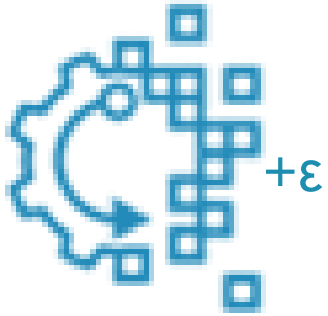


~~Data Anonymization~~



Securing Data in Use – PETs

Data Anonymization



Differential Privacy

Cryptographic Techniques for Secure Computation

Data in Use

Homomorphic Encryption

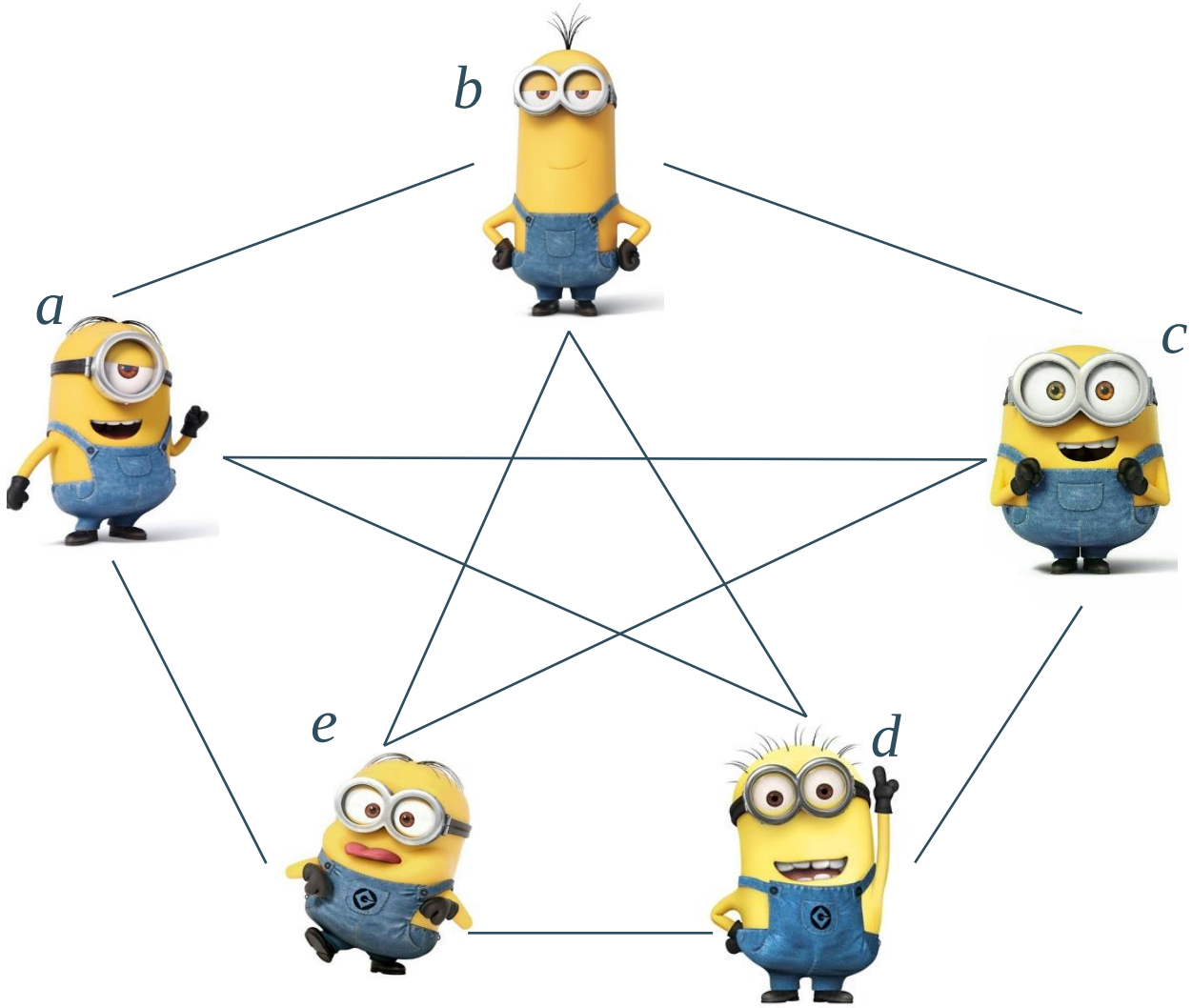
Types of Homomorphic Encryption

HE Type	Type of Operation	Number of Operations
Partially Homomorphic Encryption (PHE)	One (Addition OR Multiplication)	Unlimited
Somewhat Homomorphic Encryption (SHE)	Two (Addition AND Multiplication)	Limited
Fully Homomorphic Encryption (FHE)	Two (Addition AND Multiplication)	Unlimited

Homomorphic Encryption Context

- Outsourcing the computation to ***one single party*** (server)
- Inherently ***trust*** the server to perform the computation correctly and honestly
- ***One round*** of communication: Query – Response
- ***Communication and computational cost*** is considerably larger than plaintext computations

Multiparty Computation – MPC



→ Securely compute $f(a, b, c, d, e)$.

“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?”

-Andrew Yao, 1982

Multiparty Computation Context

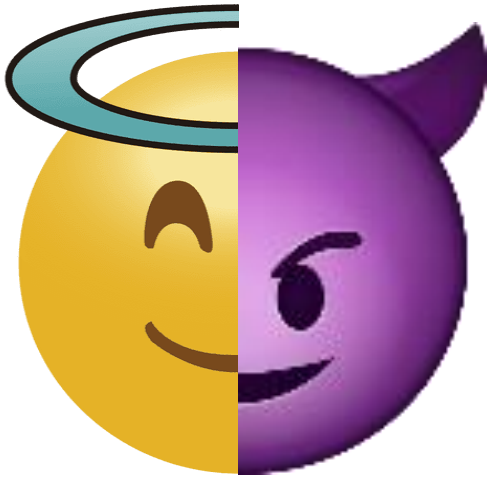
- A ***minimum of two parties*** (servers) is required to perform computation
- ***Trust*** is distributed and there are various security models one can consider
- ***Multiple rounds*** of communication required in an interactive protocol
- ***Communication and computational cost*** is considerably larger than plaintext computations (yet ***more efficient*** than HE solutions!)

Security Models

- Active Security

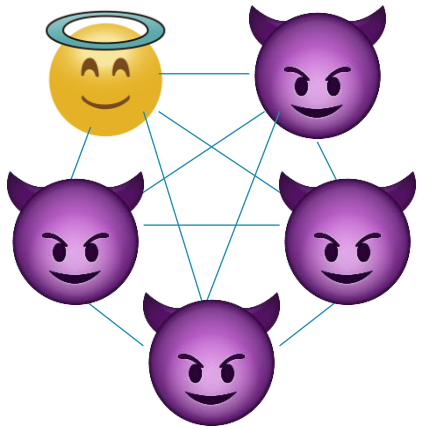
vs.

- Passive Security



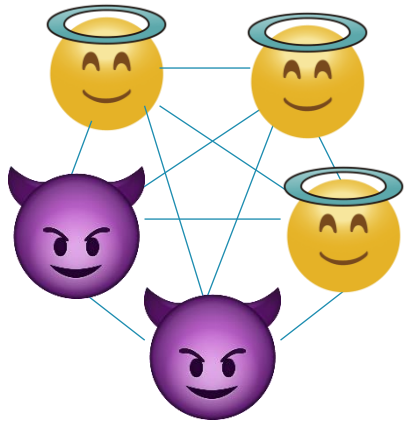
Corruption Thresholds

- Dishonest Majority



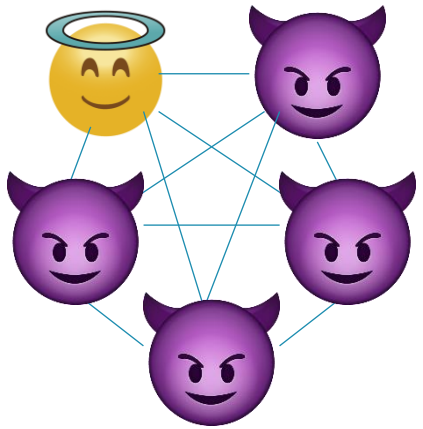
vs.

- Honest Majority



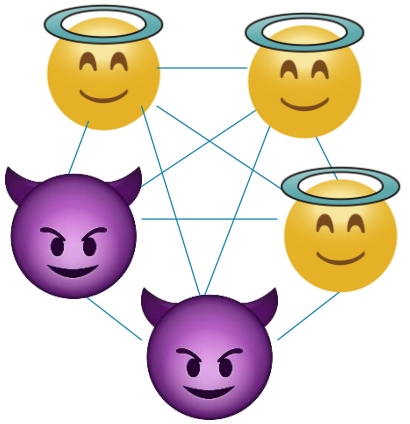
Corruption Thresholds

- Dishonest Majority



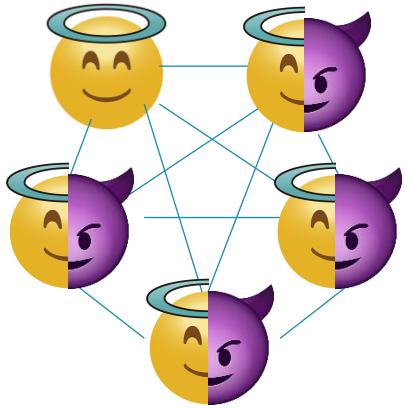
vs.

- Honest Majority

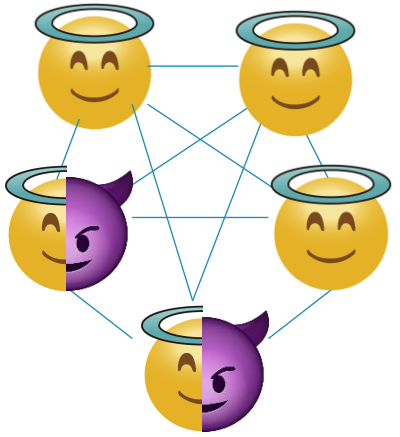


in the active model

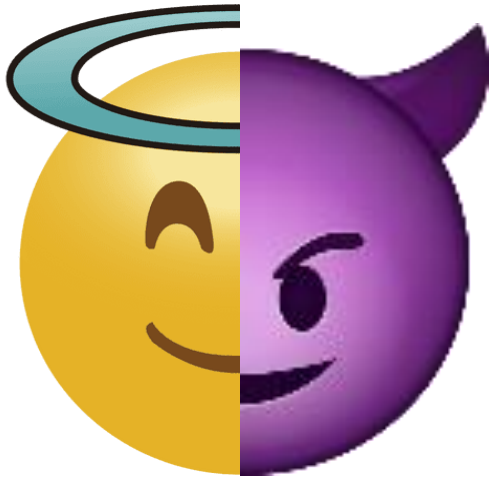
OR



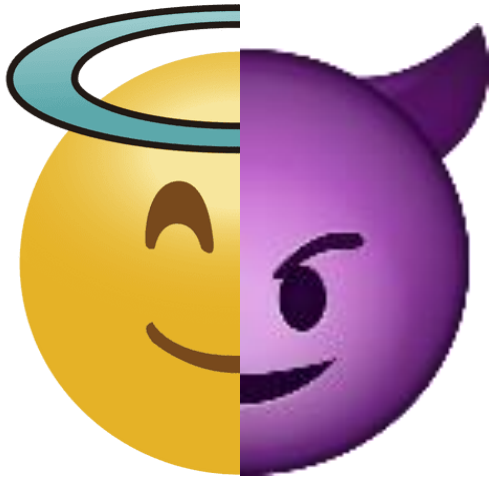
in the passive model

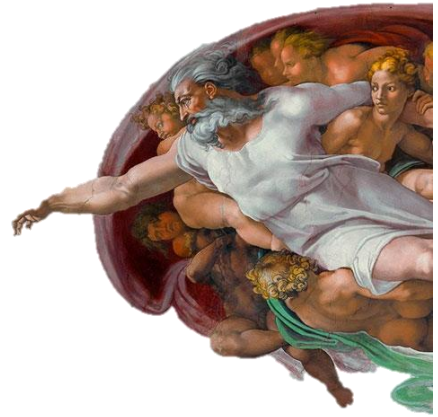


Types of Parties



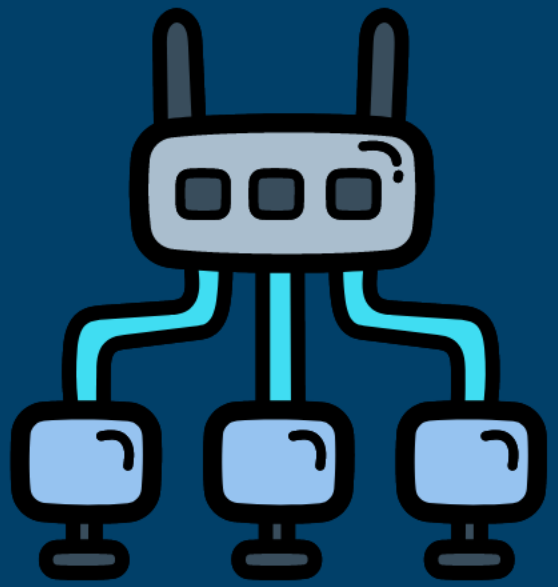
Types of Parties





Computational Power of Parties

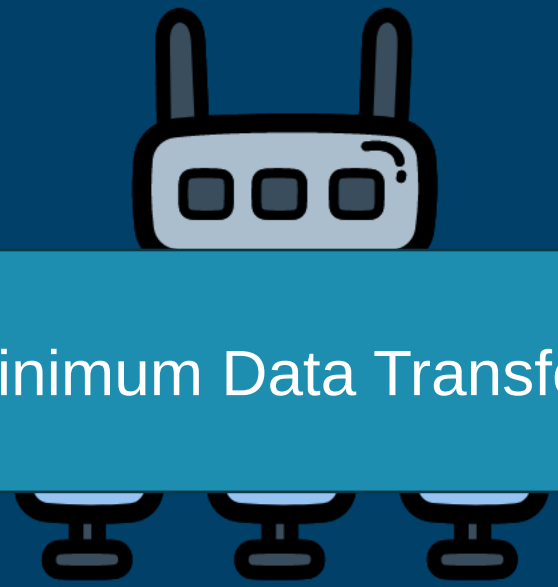
Available Network Setting/Resources



LAN

WAN

Available Network Setting/Resources



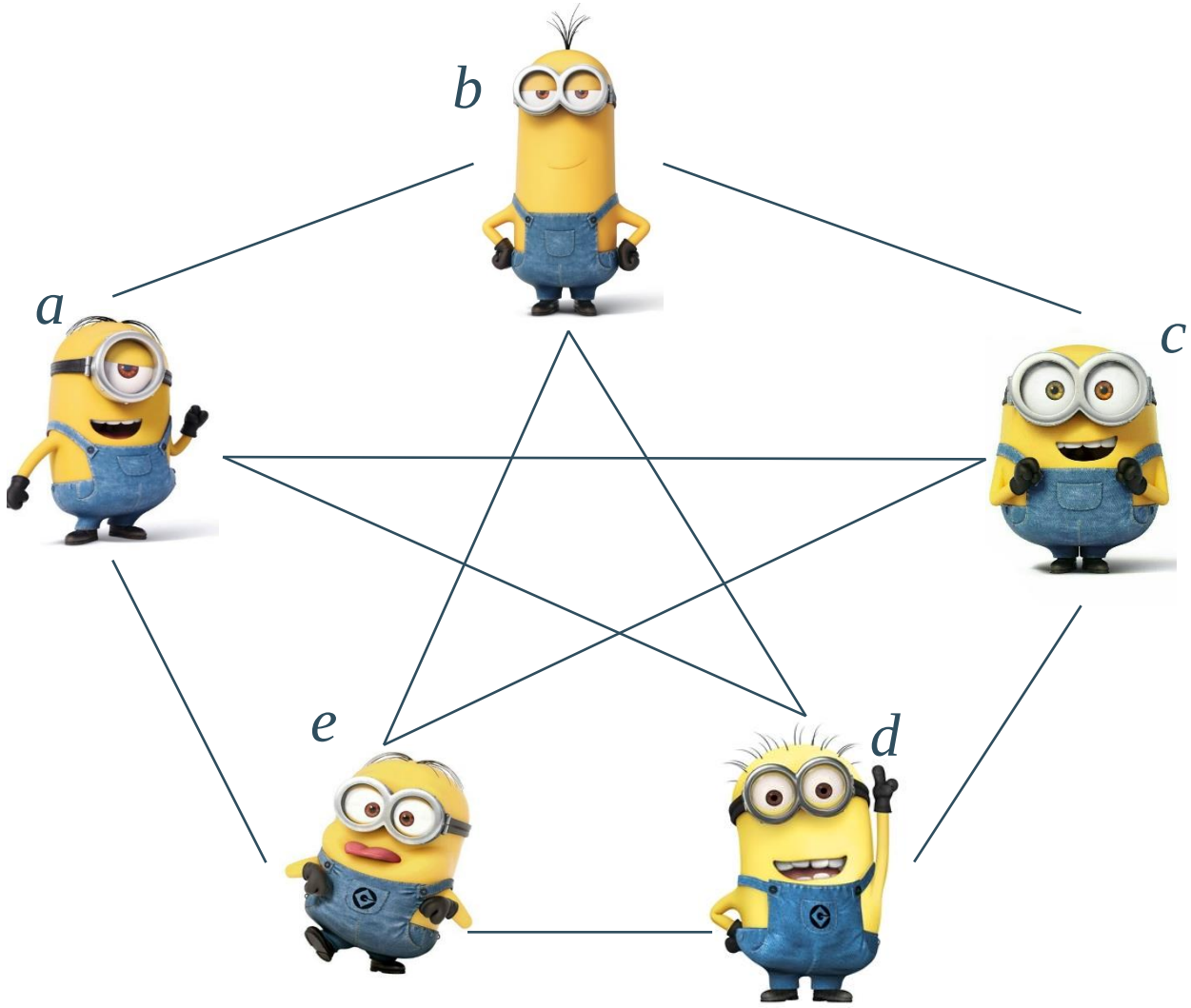
Minimum Data Transfer

Minimum Number of Rounds

LAN

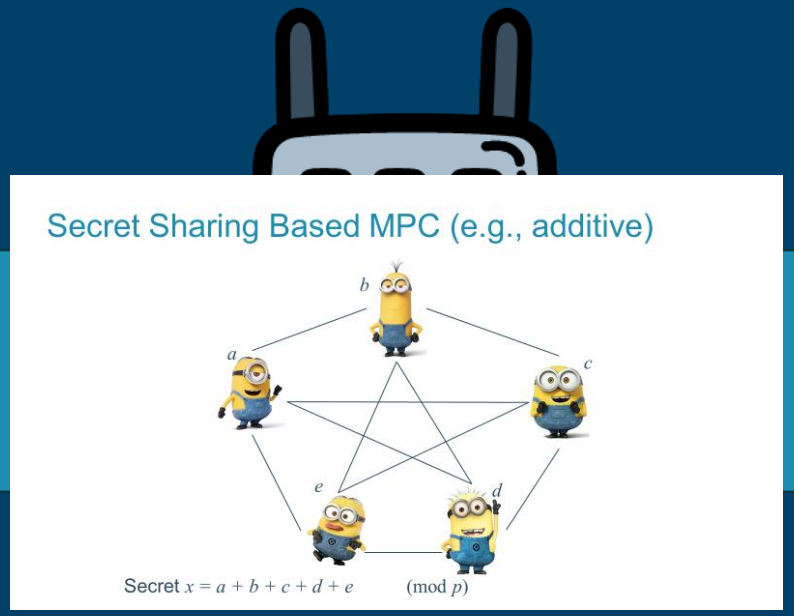
WAN

Secret Sharing Based MPC (e.g., additive)



Secret $x = a + b + c + d + e \pmod{p}$

Available Network Setting/Resources

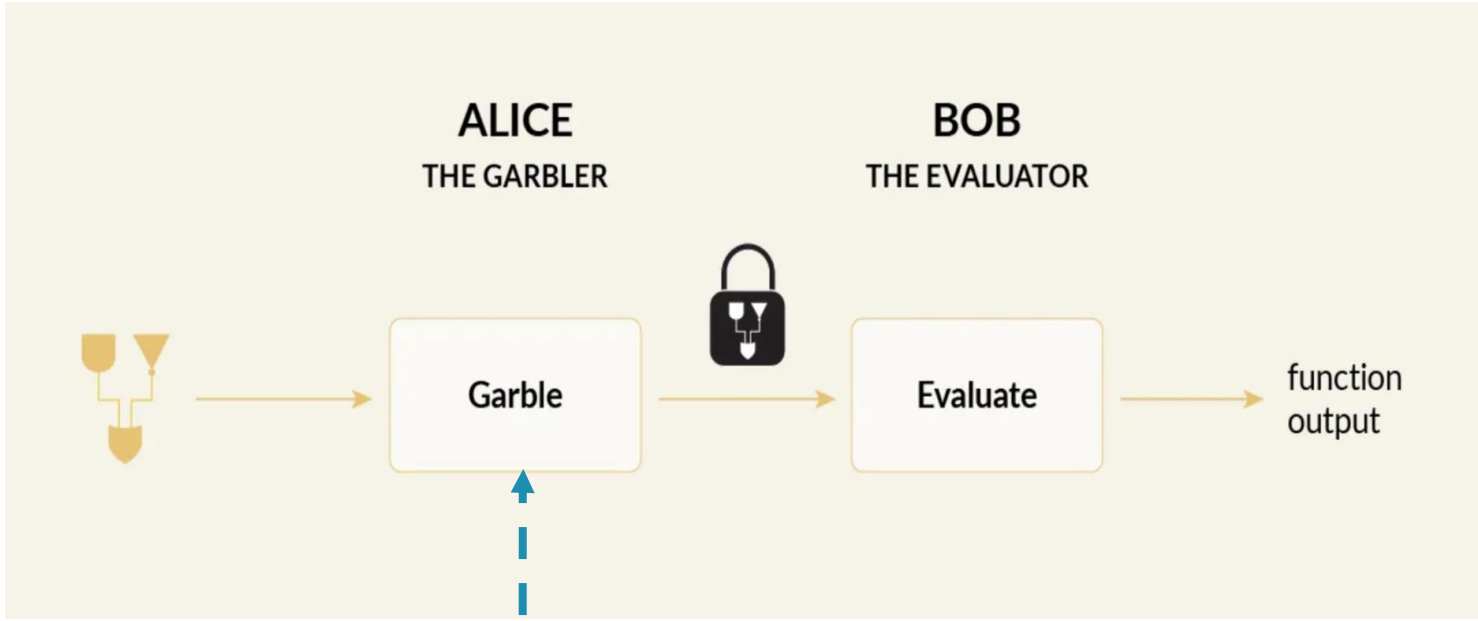


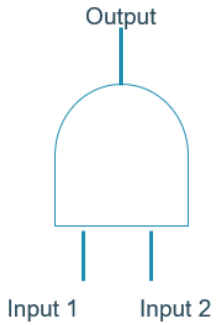
Minimum Number of Rounds

LAN

WAN

Garbling Based (MPC)

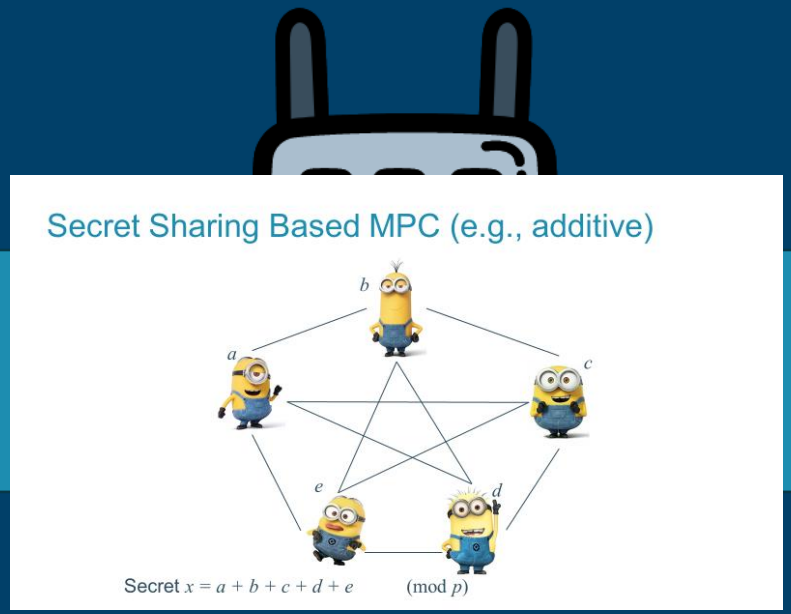


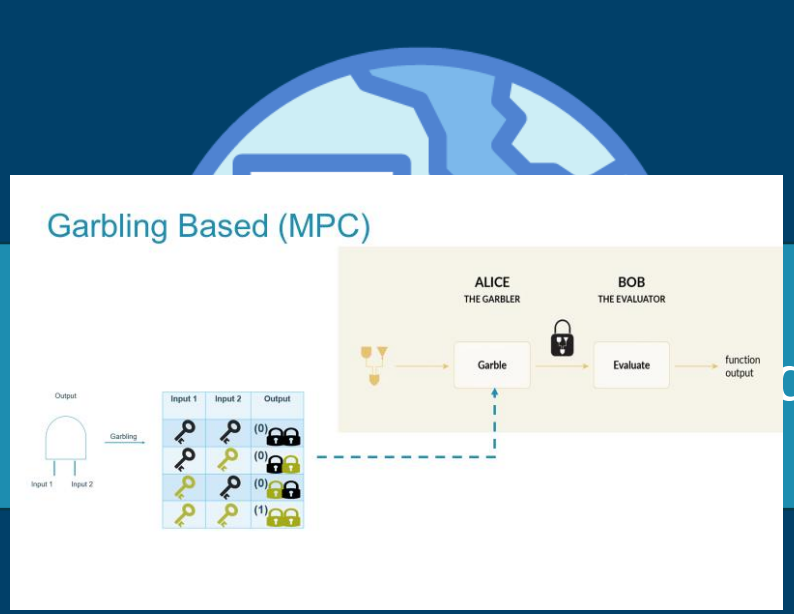


Garbling

Input 1	Input 2	Output
		(0)
		(0)
		(0)
		(1)

Available Network Setting/Resources





ds

LAN

WAN

The Preprocessing Model

Offline Phase

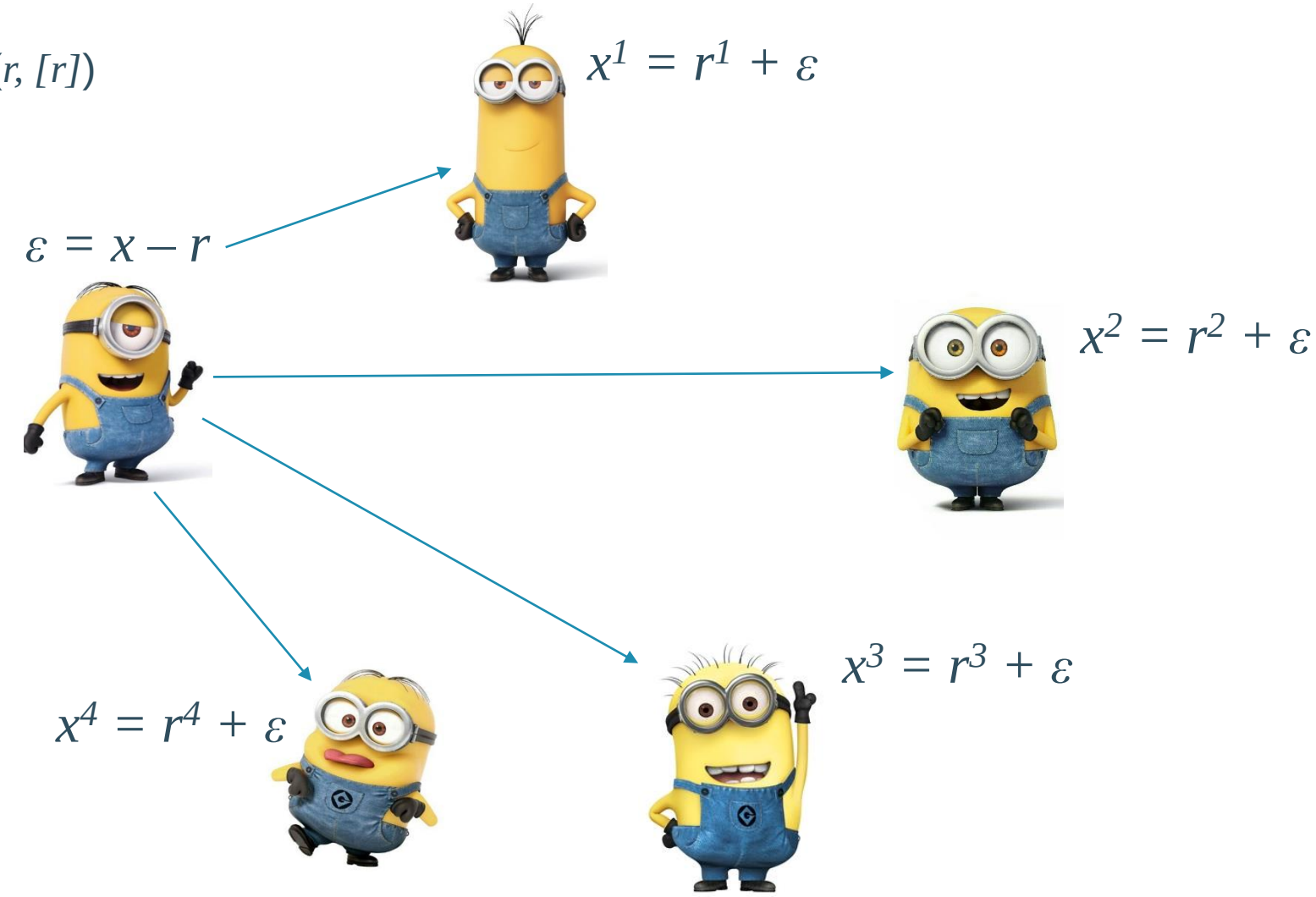
- Data independent
- Any time prior to protocol execution
- Prepare (random) material for input sharing and multiplication computations

Online Phase

- Data dependent
- Synchronous protocol execution with all parties online
- Consume preprocessed material to (more efficiently) complete the computation at hand

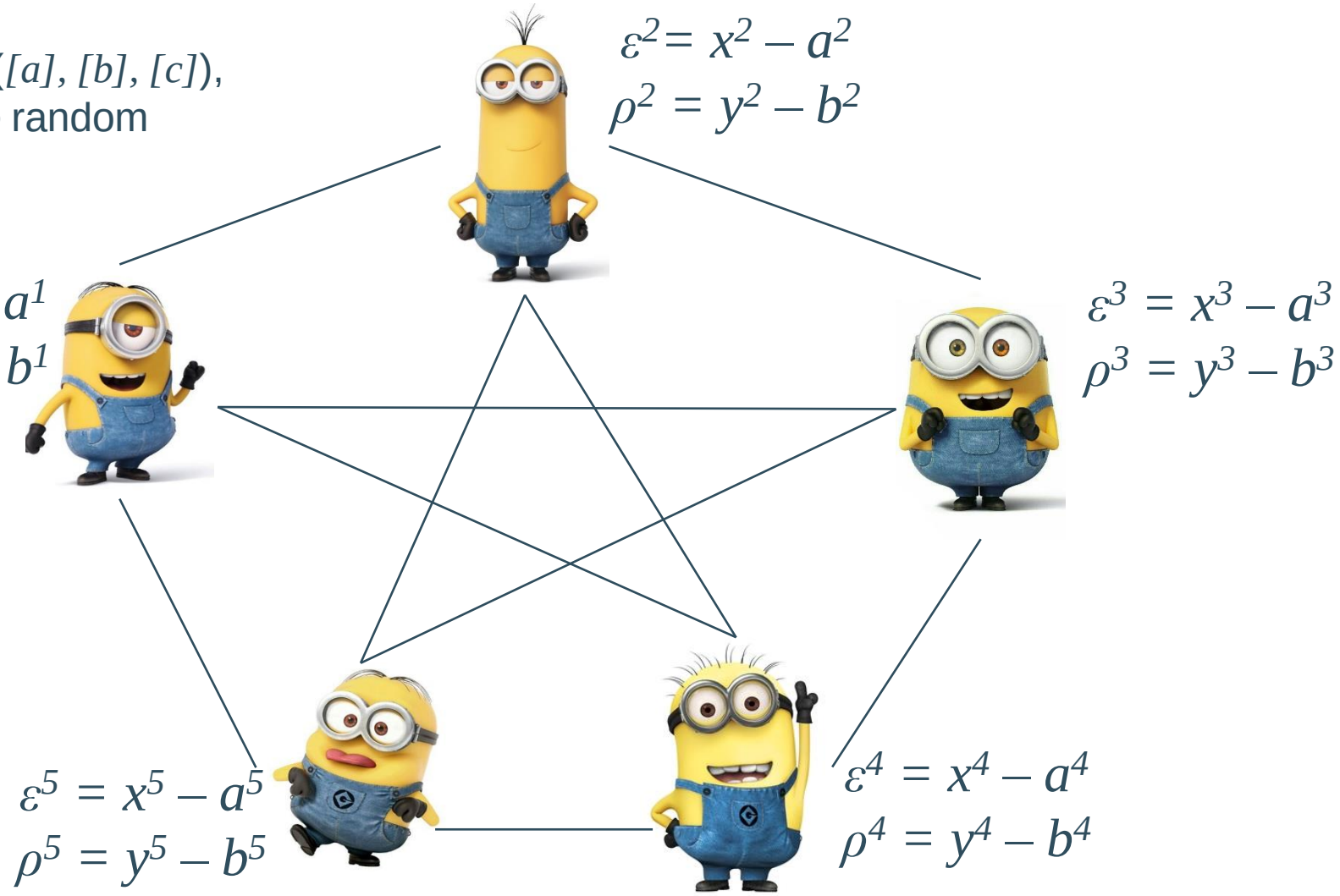
Share Input x (online phase)

Using preprocessed $(r, [r])$



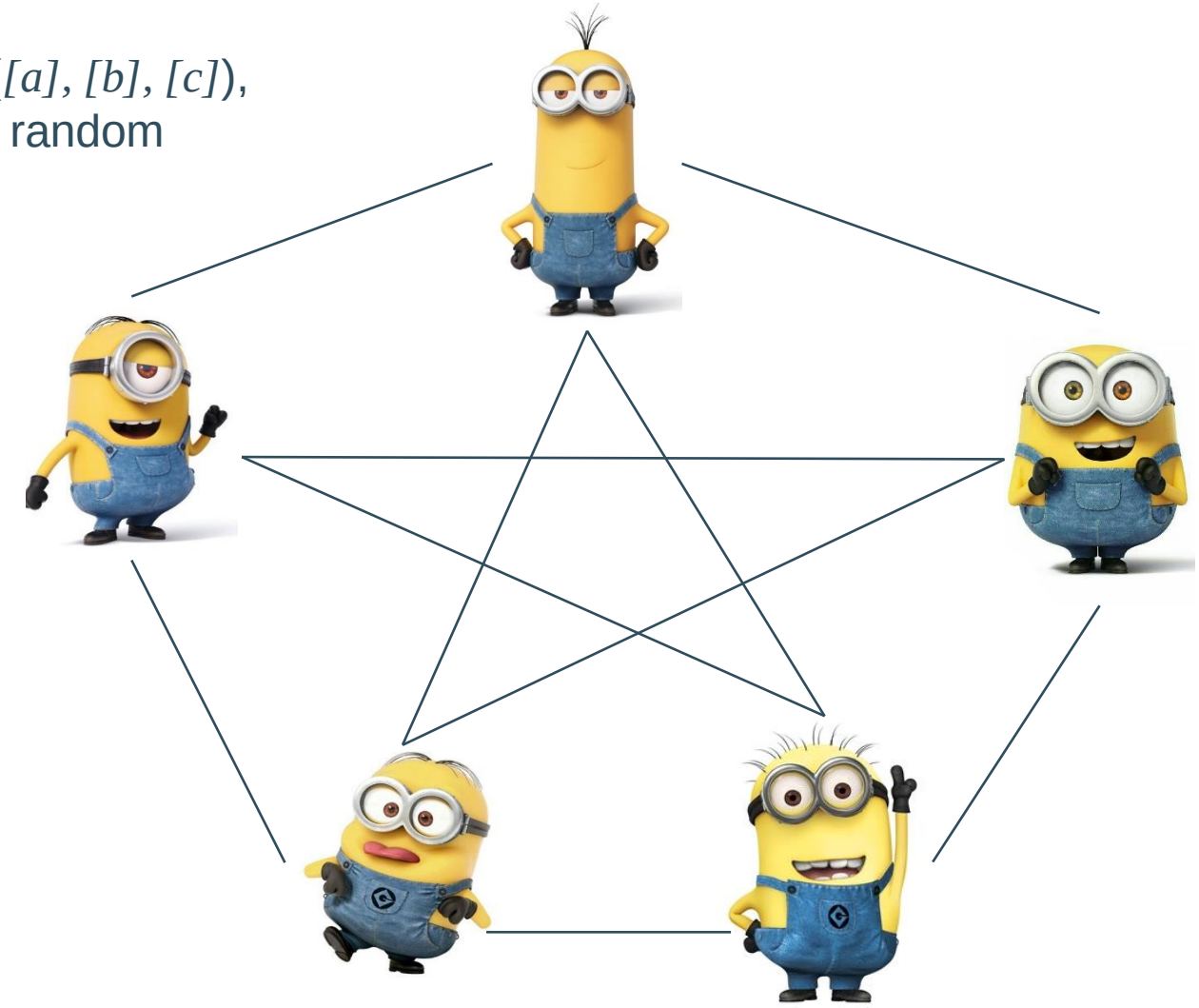
Compute Product $z = x \cdot y$ (online phase) 1/3

Using preprocessed ($[a]$, $[b]$, $[c]$),
with $c = a \cdot b$, and a, b random



Compute Product $z = x \cdot y$ (online phase) 2/3

Using preprocessed $([a], [b], [c])$,
with $c = a \cdot b$, and a, b random



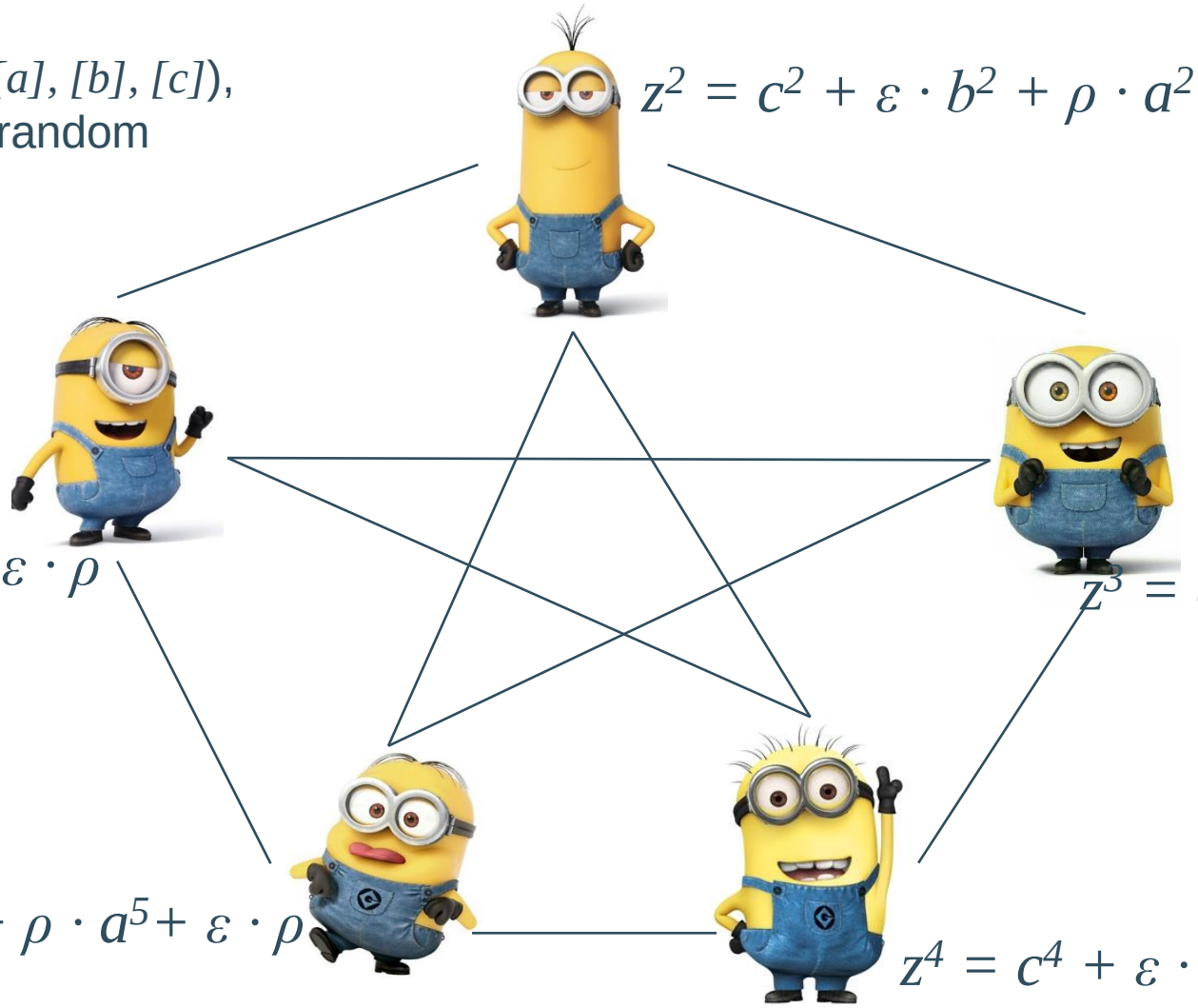
Open

$\varepsilon = x - a$

$\rho = y - b$

Compute Product $z = x \cdot y$ (online phase) 3/3

Using preprocessed ($[a]$, $[b]$, $[c]$),
with $c = a \cdot b$, and a, b random



$z^2 = c^2 + \varepsilon \cdot b^2 + \rho \cdot a^2 + \varepsilon \cdot \rho$

$z^1 = c^1 + \varepsilon \cdot b^1 + \rho \cdot a^1 + \varepsilon \cdot \rho$

$z^3 = c^3 + \varepsilon \cdot b^3 + \rho \cdot a^3 + \varepsilon \cdot \rho$

$z^5 = c^5 + \varepsilon \cdot b^5 + \rho \cdot a^5 + \varepsilon \cdot \rho$

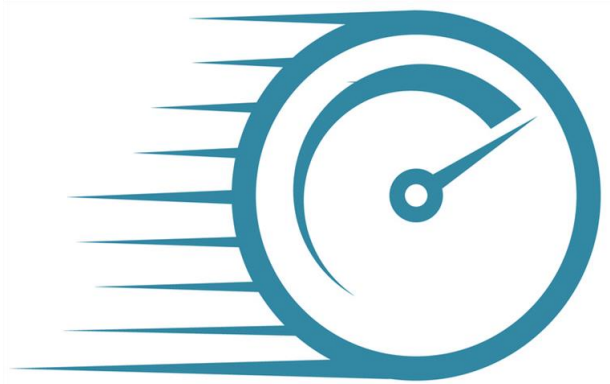
$z^4 = c^4 + \varepsilon \cdot b^4 + \rho \cdot a^4 + \varepsilon \cdot \rho$

Set $[z] = [c] + \varepsilon \cdot [b] + \rho \cdot [a] + \varepsilon \cdot \rho$

The tradeoffs

Functionality

Security

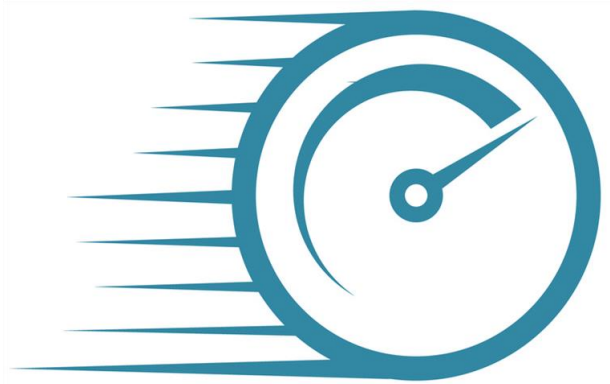


Efficiency

The tradeoffs

Security

Functionality



Efficiency

MPC Applications

- Auctions
- e-Voting
- Statistical Analysis and Collaborative Analytics
- Fraud Detection
- e-Health and general medical research applications
- Key Management
- Machine Learning

According to Gartner, by 2025, 50% of large organizations will implement privacy-enhancing computation to process data in untrusted environments and multiparty data analytics use cases.

Questions and Discussion