

A Gentle Introduction to Secure Computation

Eleftheria Makri | High-Tech Women 2024, Darmstadt

25/09/2024



Universiteit
Leiden

Bij ons leer je de wereld kennen

A Gentle Introduction to Secure Computation

Eleftheria Makri | High-Tech Women 2024, Darmstadt

25/09/2024



Universiteit
Leiden

Bij ons leer je de wereld kennen

Eleftheria Makri

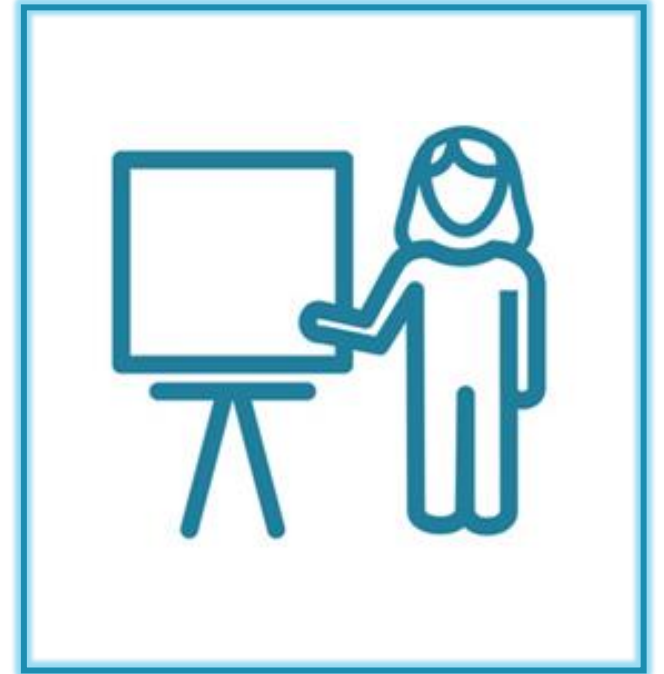
Mom



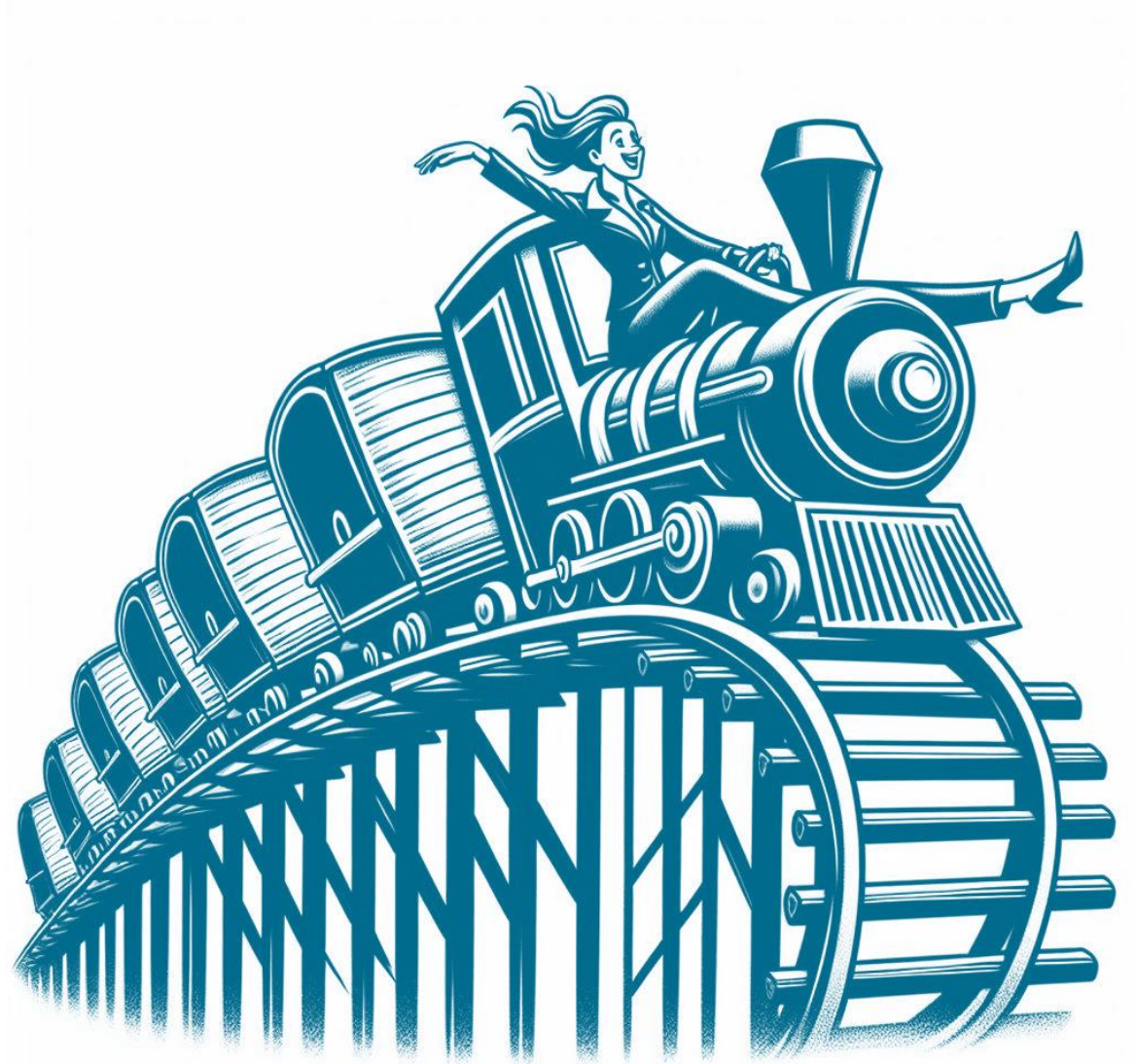
Balanced Human Being



Assistant Professor



Eleftheria Makri – A career roller coaster



High-Tech Women: A minority?

Bachelor 2005



Master 2009



Systems & Security staff,
LIACS, now

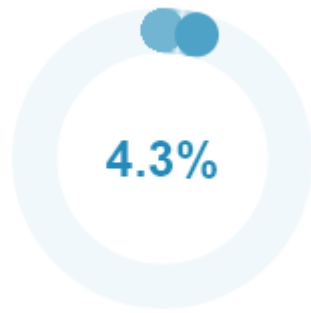


High-Tech Women: A minority?

Bachelor 2005



5 females out of 116 students



Master 2009



Systems & Security staff,
LIACS, now

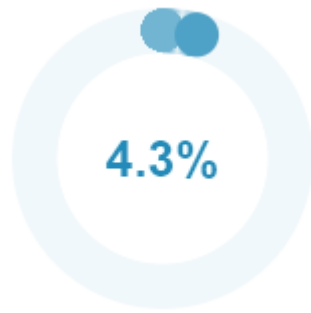


High-Tech Women: A minority?

Bachelor 2005



5 females out of 116 students



Master 2009



3 females out of 12 students



Systems & Security staff,
LIACS, now

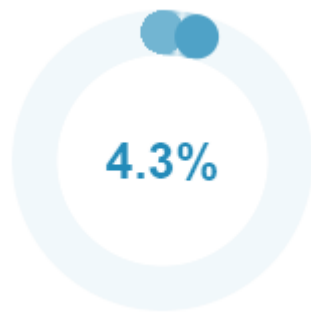


High-Tech Women: A minority?

Bachelor 2005



5 females out of 116 students



Master 2009



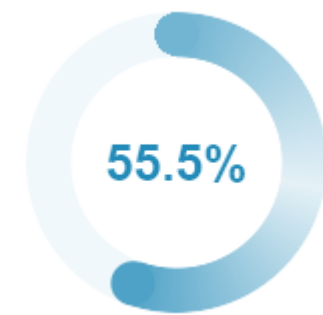
3 females out of 12 students



Systems & Security staff,
LIACS, now



5 females out of 9 scientific staff



A Gentle Introduction to Secure Computation

Eleftheria Makri | High-Tech Women 2024, Darmstadt

25/09/2024



Universiteit
Leiden

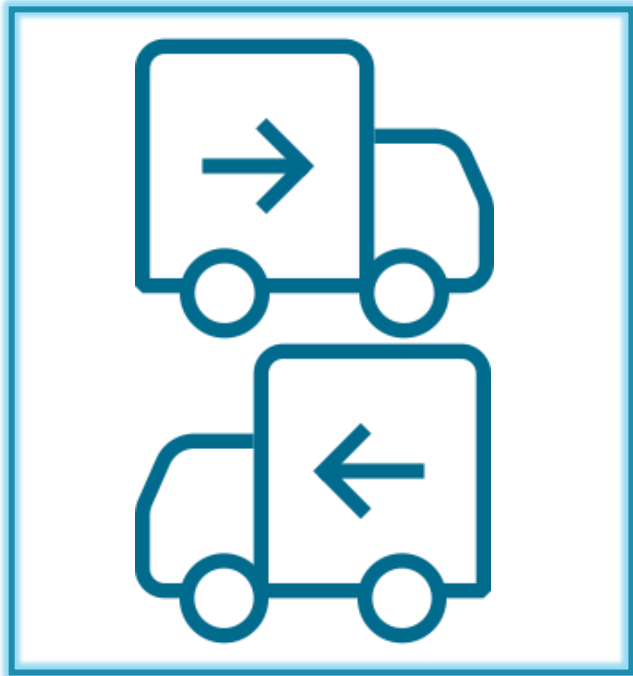
Bij ons leer je de wereld kennen

Privacy Enhancing Technologies



The Three States of Data

Data in Transit



Data at Rest

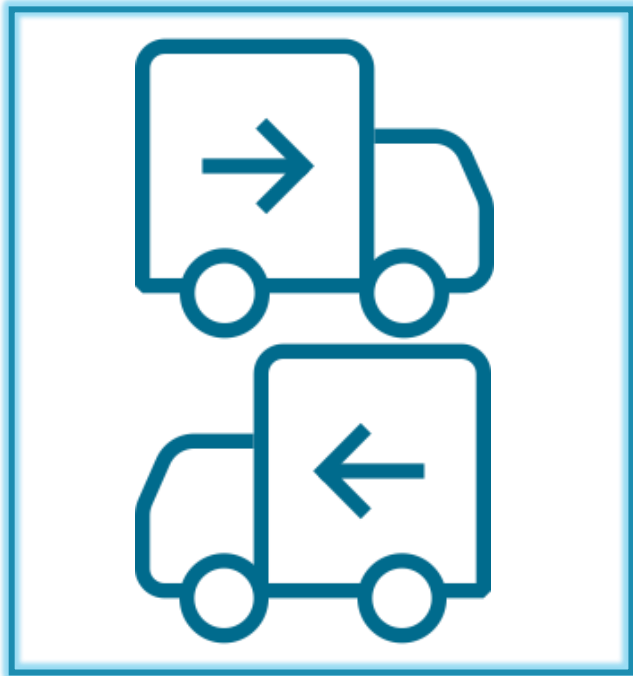


Data in Use



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



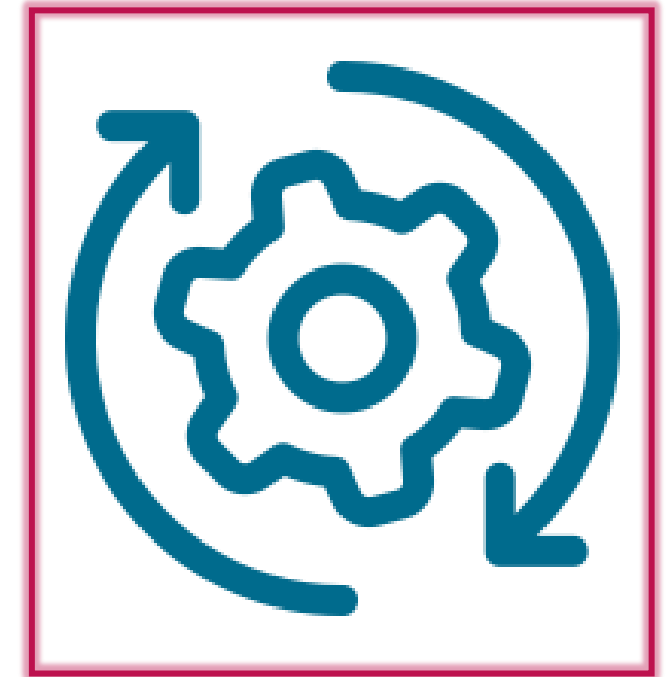
Traditional Cryptography

Secure Computation
Technologies

Data in Use



Data in Use

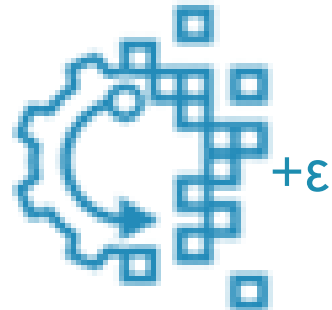


“How to allow the collection and purposeful processing of private data, without compromising individual privacy?”

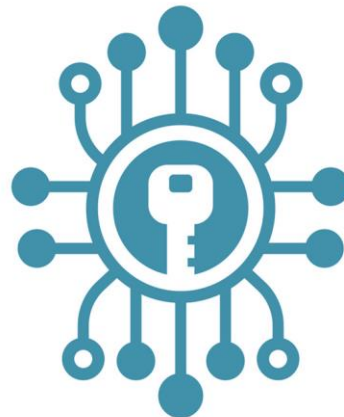
Securing Data in Use – PETs



Data Anonymization

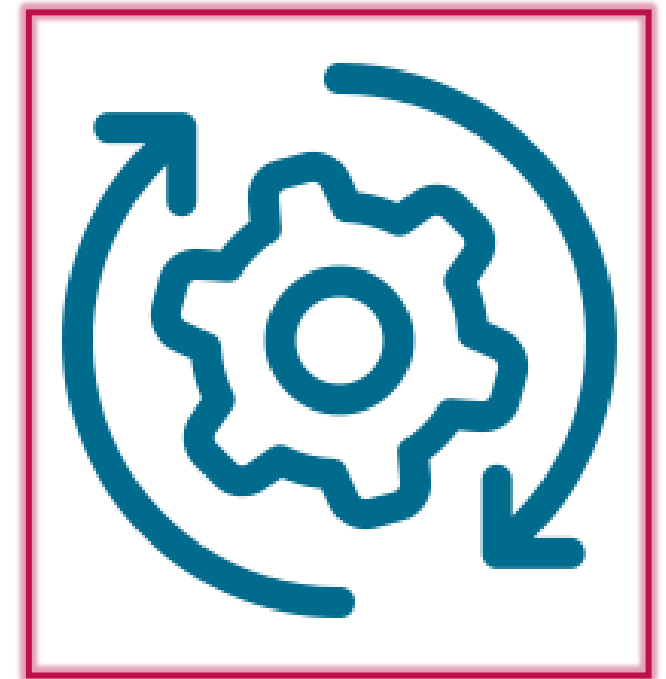


Differential Privacy

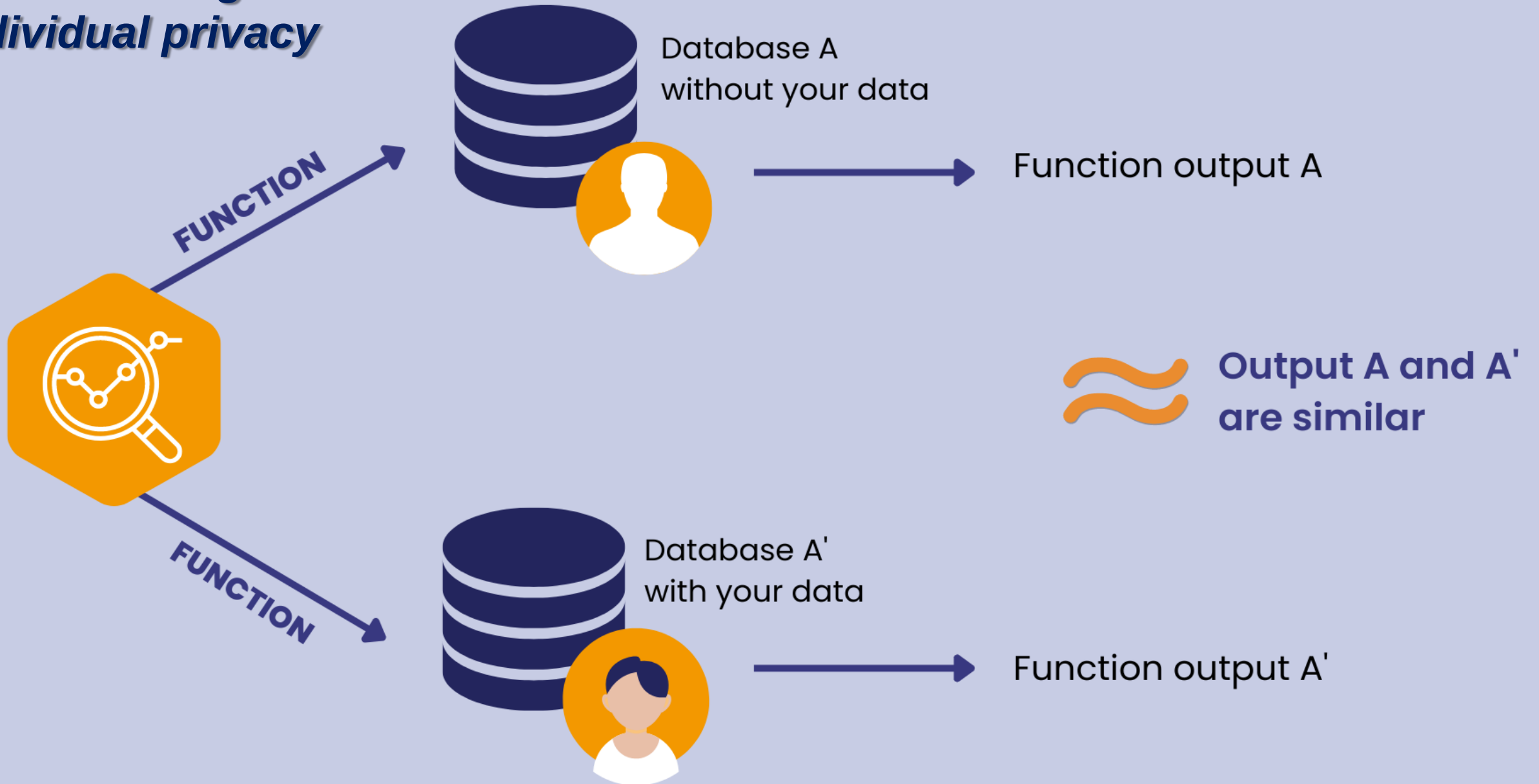


Cryptographic Techniques
for Secure Computation

Data in Use



DP – Ensuring individual privacy



DP – Ensuring individual privacy

FUNCTION



SENSITIVITY



Determine the
function sensitivity



Choose a noise
addition mechanism

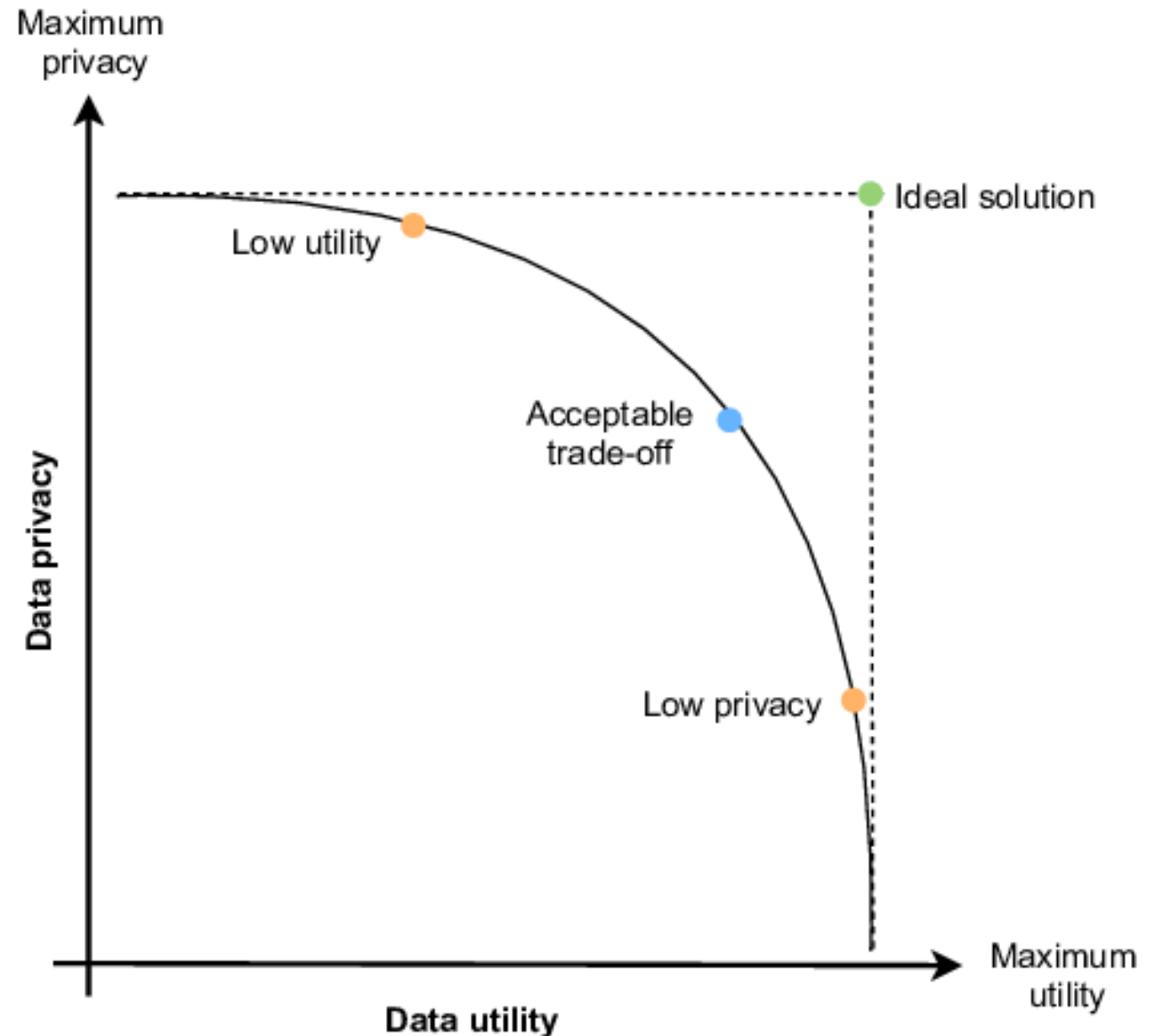


DATA WITH NOISE



DP - The Penalties

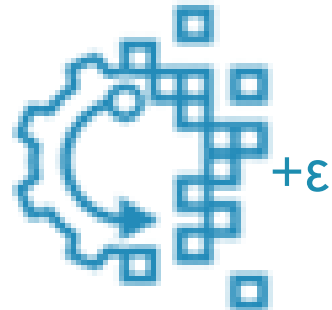
- Inherent information leakage, called privacy budget in DP terms.
- Inherent tradeoff between data privacy and data utility



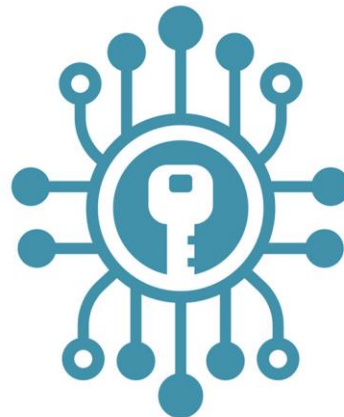
Securing Data in Use – PETs



Data Anonymization

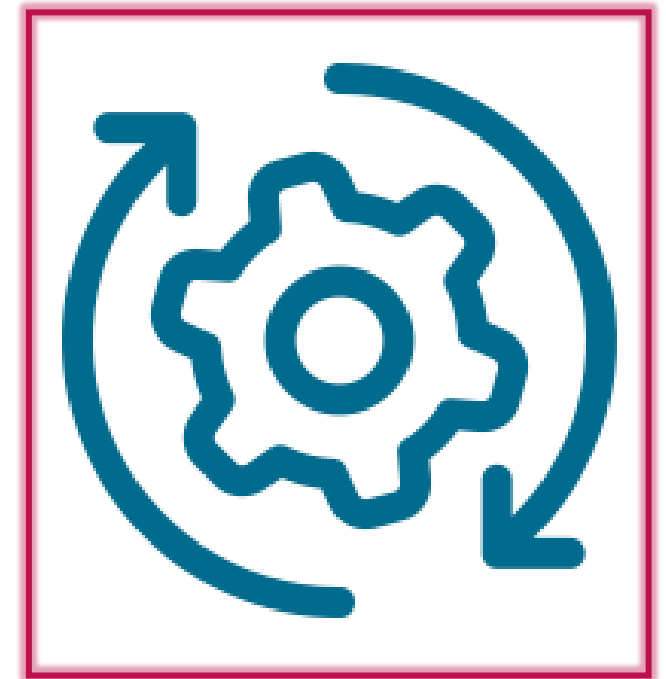


Differential Privacy



Cryptographic Techniques
for Secure Computation

Data in Use



Data Anonymization



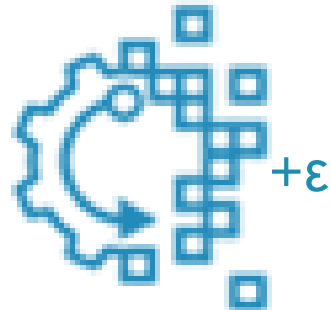
~~Data Anonymization~~



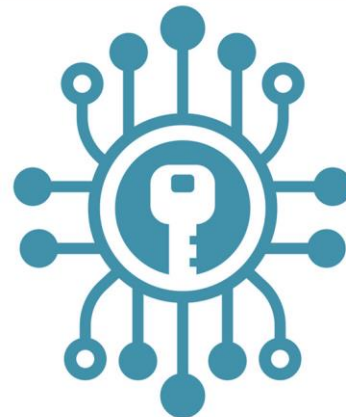
Securing Data in Use – PETs



Data Anonymization



Differential Privacy



Cryptographic Techniques
for Secure Computation

Data in Use



Homomorphic Encryption



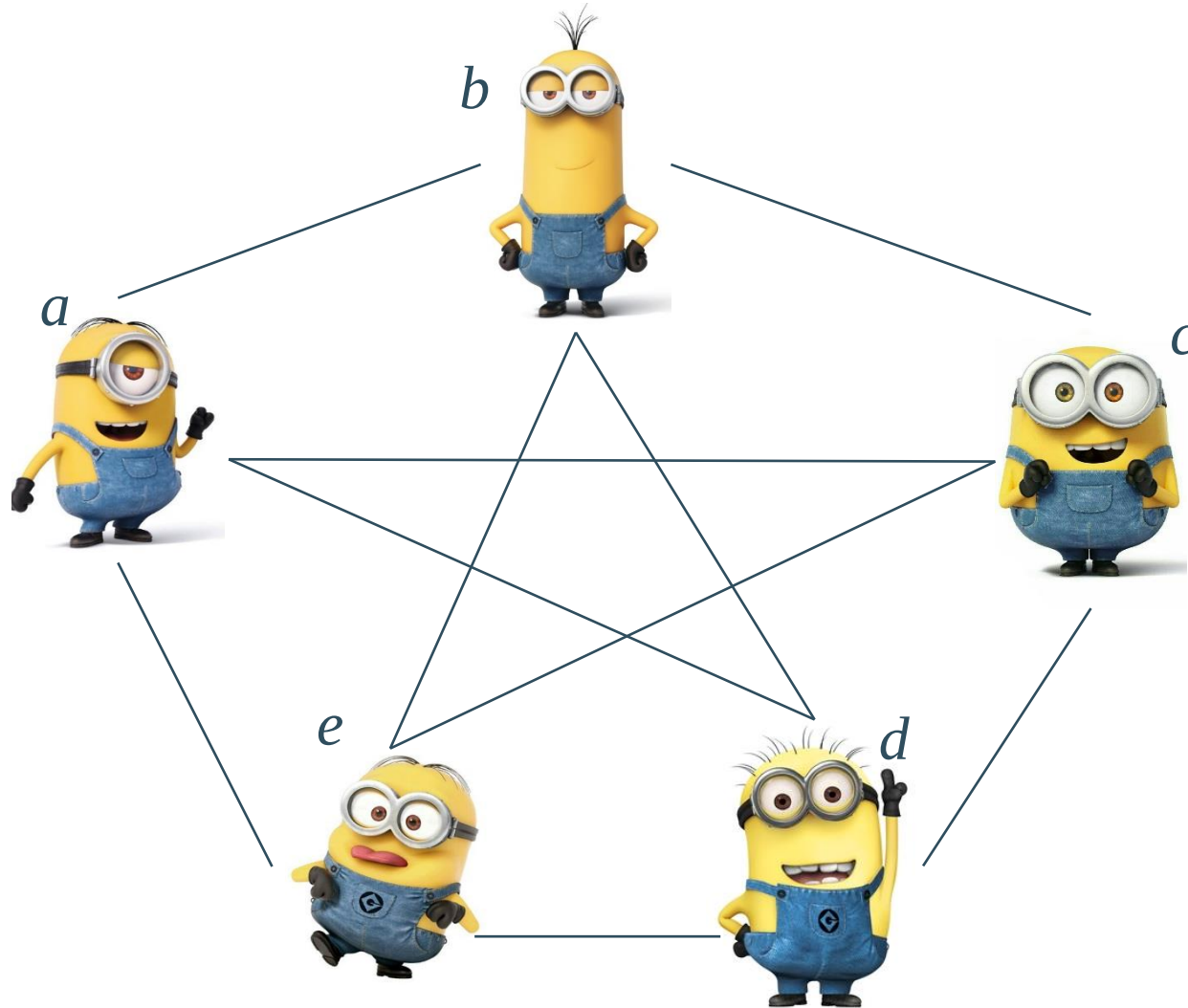
Types of Homomorphic Encryption

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

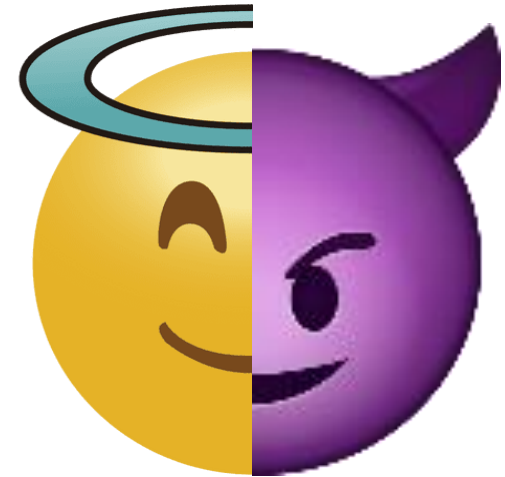
- A ***minimum of two parties*** (servers) is required to perform computation
- ***Trust*** is distributed and there are various security models one can consider
- ***Multiple rounds*** of communication required in an interactive protocol
- ***Communication and computational cost*** is considerably larger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

Security Models

- Active Security

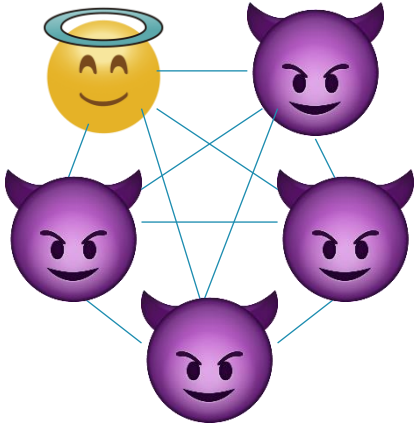
vs.

- Passive Security



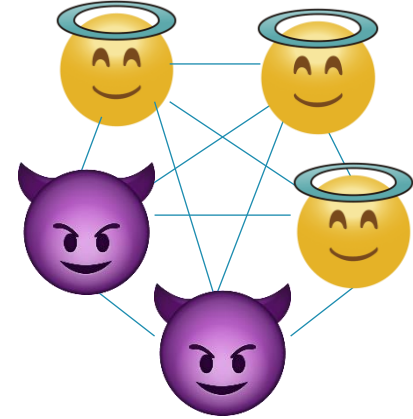
Corruption Thresholds

- Dishonest Majority



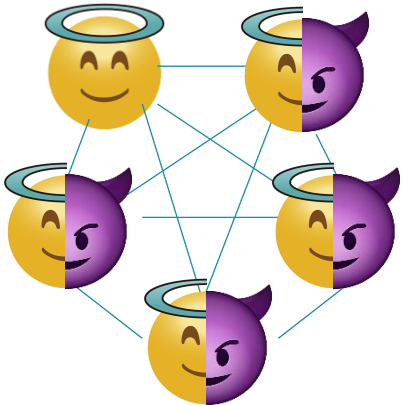
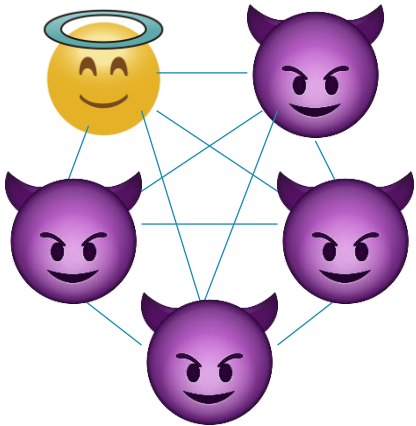
vs.

- Honest Majority



Corruption Thresholds

- Dishonest Majority



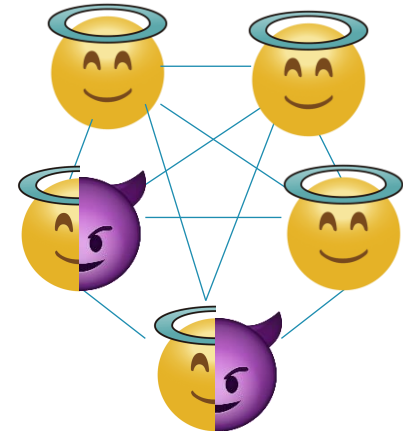
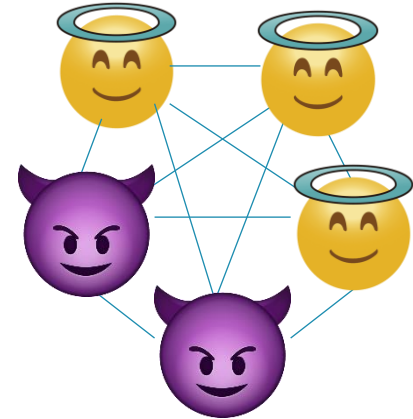
vs.

in the active model

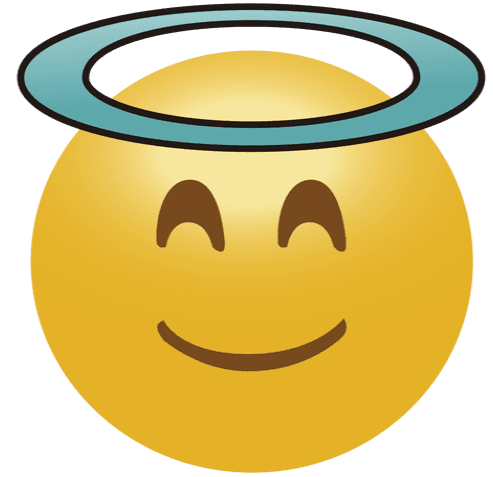
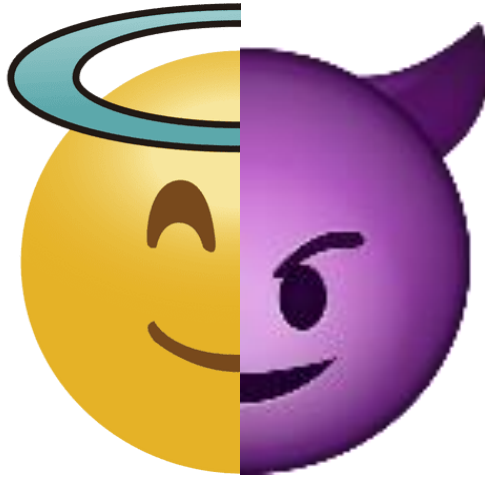
OR

in the passive model

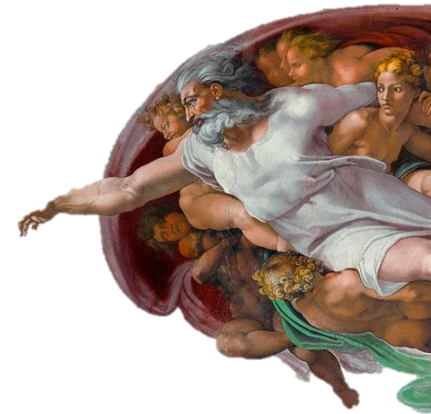
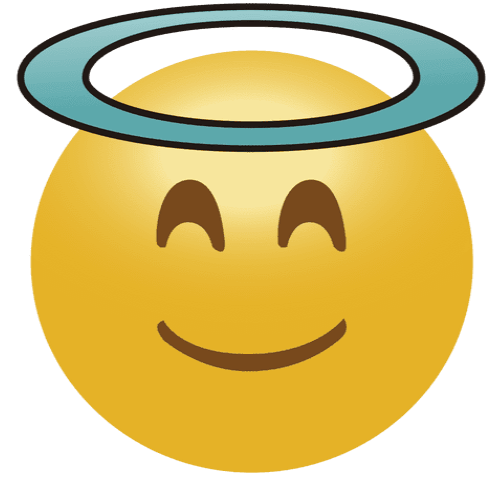
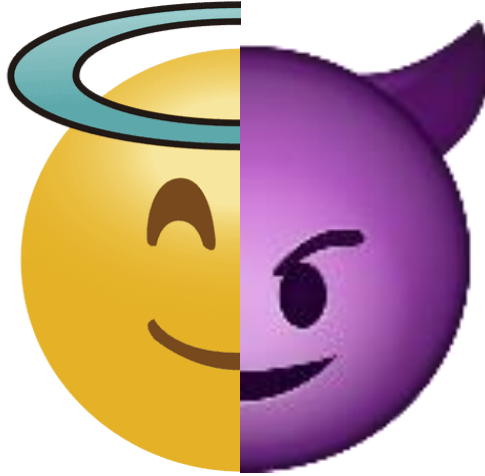
- Honest Majority



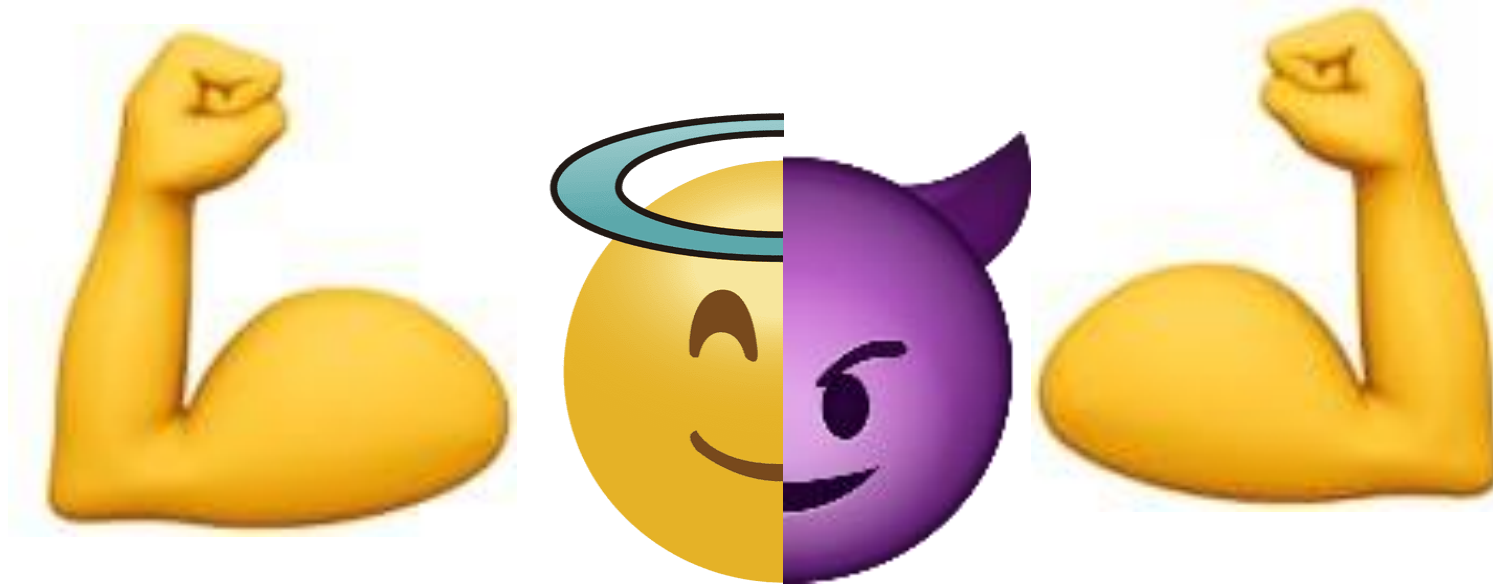
Types of Parties



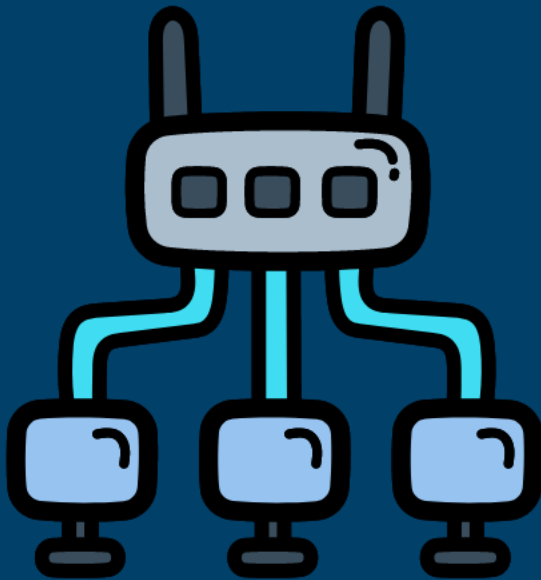
Types of Parties



Computational Power of Parties



Available Network Setting/Resources

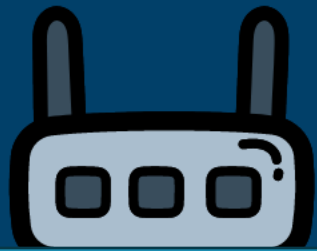


LAN



WAN

Available Network Setting/Resources



Minimum Data Transfer

LAN



Minimum Number of Rounds

WAN

The tradeoffs



The tradeoffs



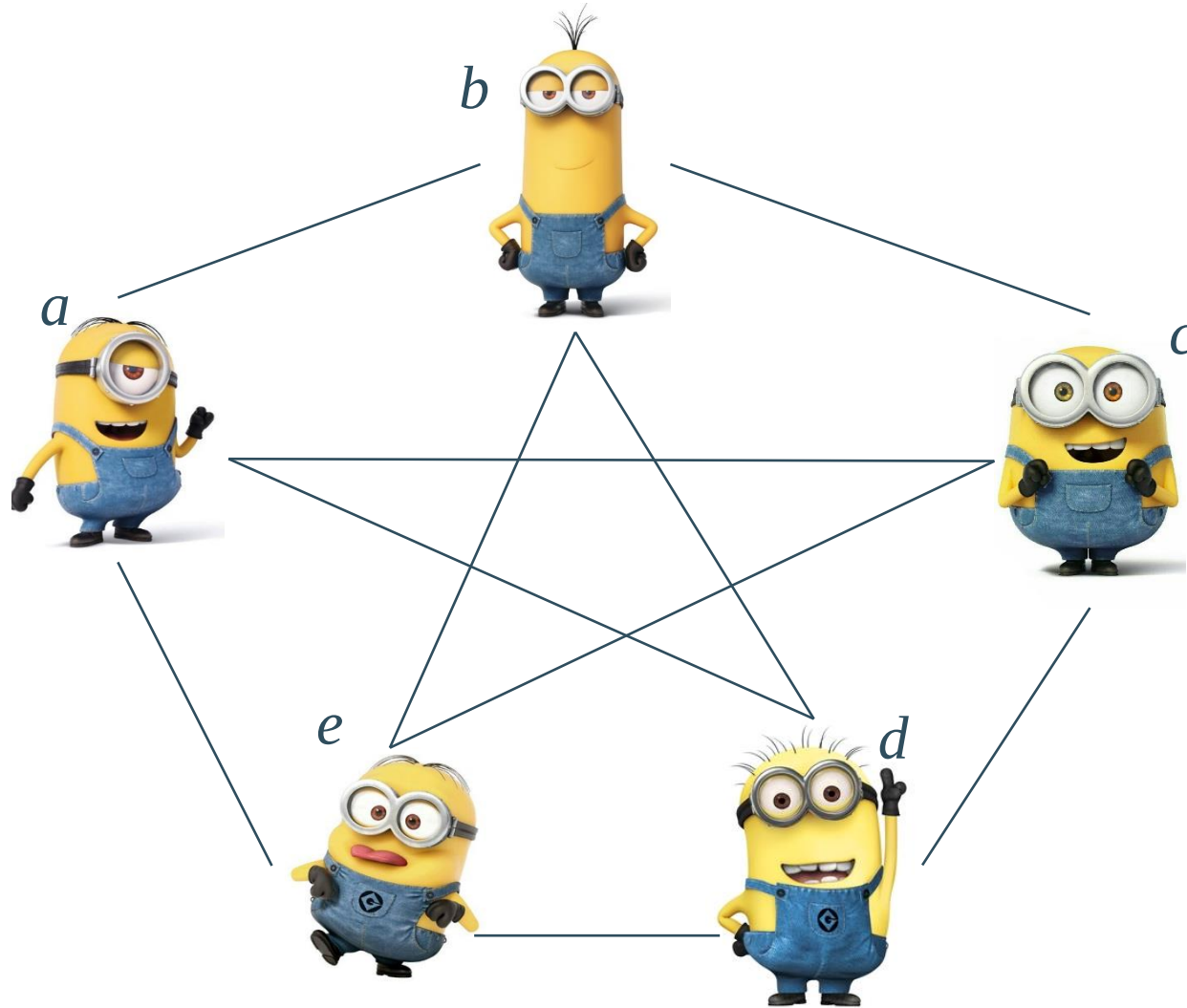
MPC Applications

- 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

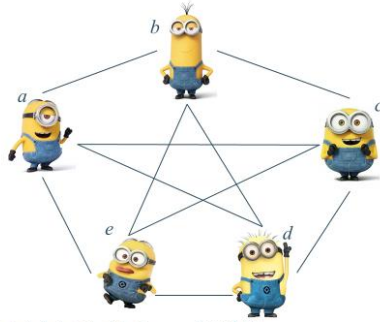
Secret Sharing Based MPC (e.g., additive)



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

Available Network Setting/Resources

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



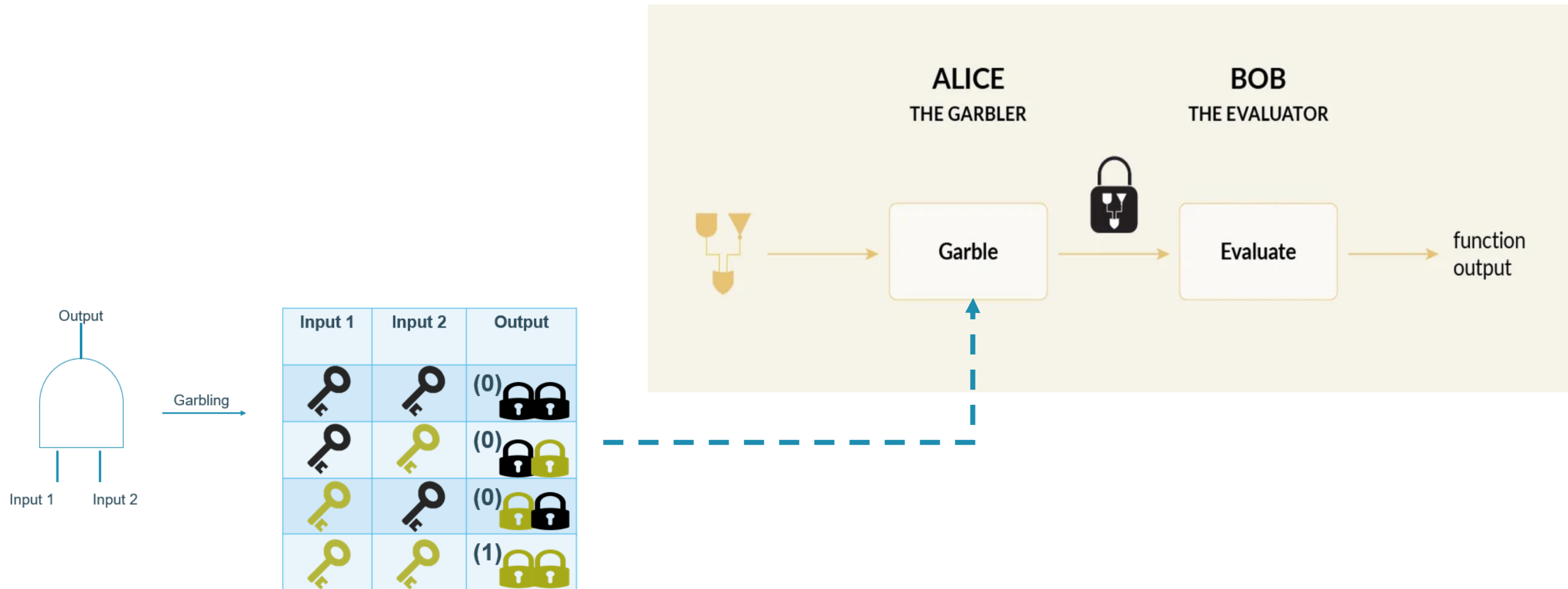
Secret $x = a + b + c + d + e \pmod{p}$

LAN

Minimum Number of Rounds

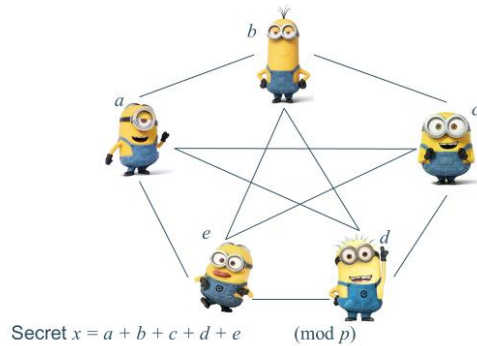
WAN

Garbling Based (MPC)



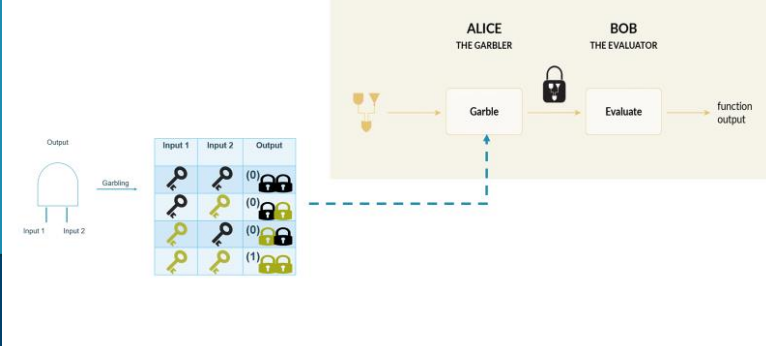
Available Network Setting/Resources

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



LAN

Garbling Based (MPC)



WAN

The Preprocessing Model

Offline Phase

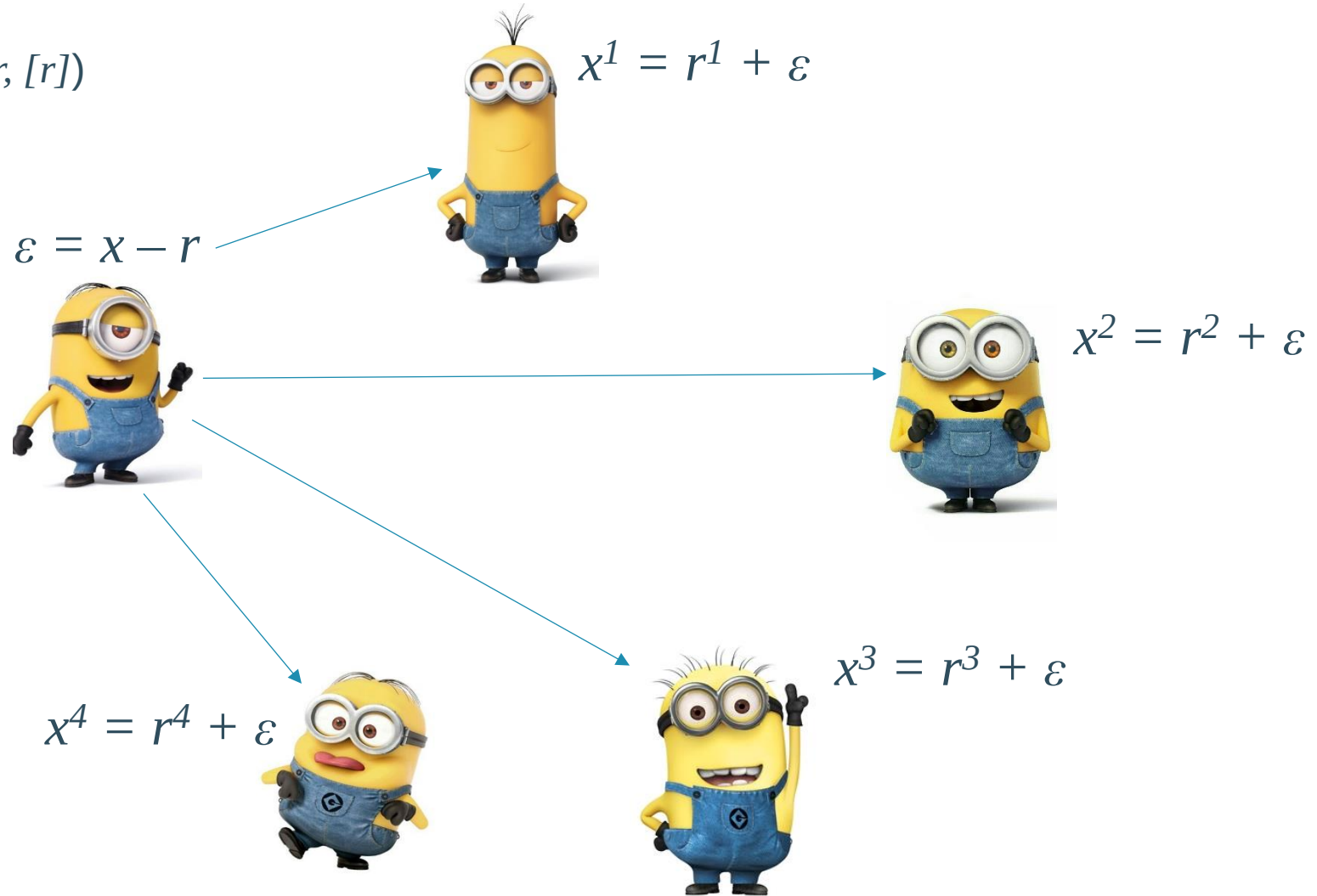
- Data independent
- Any time prior to protocol execution
- Prepare (random) material for input sharing and multiplication computations

Online Phase

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

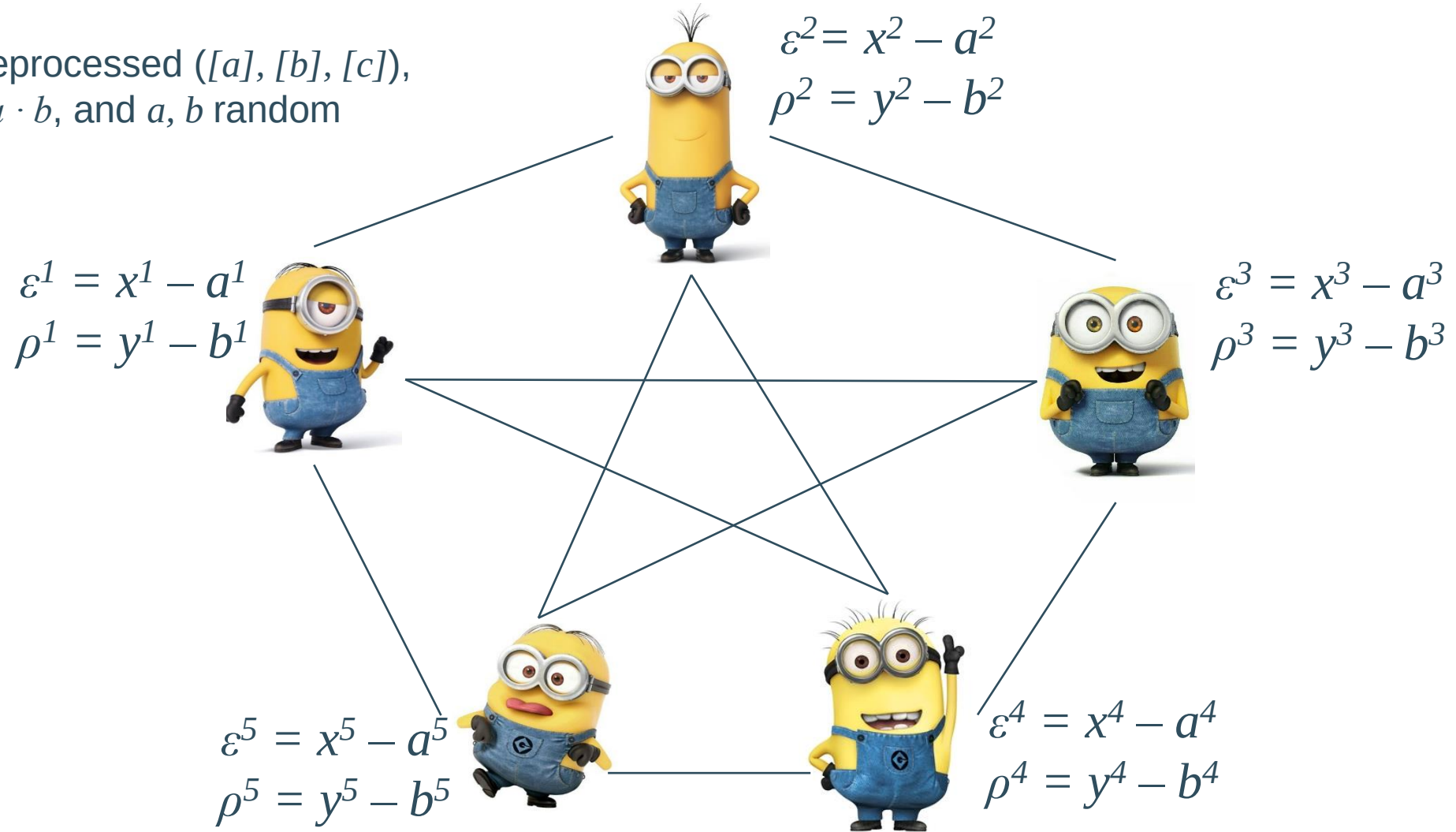
Share Input x (online phase)

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



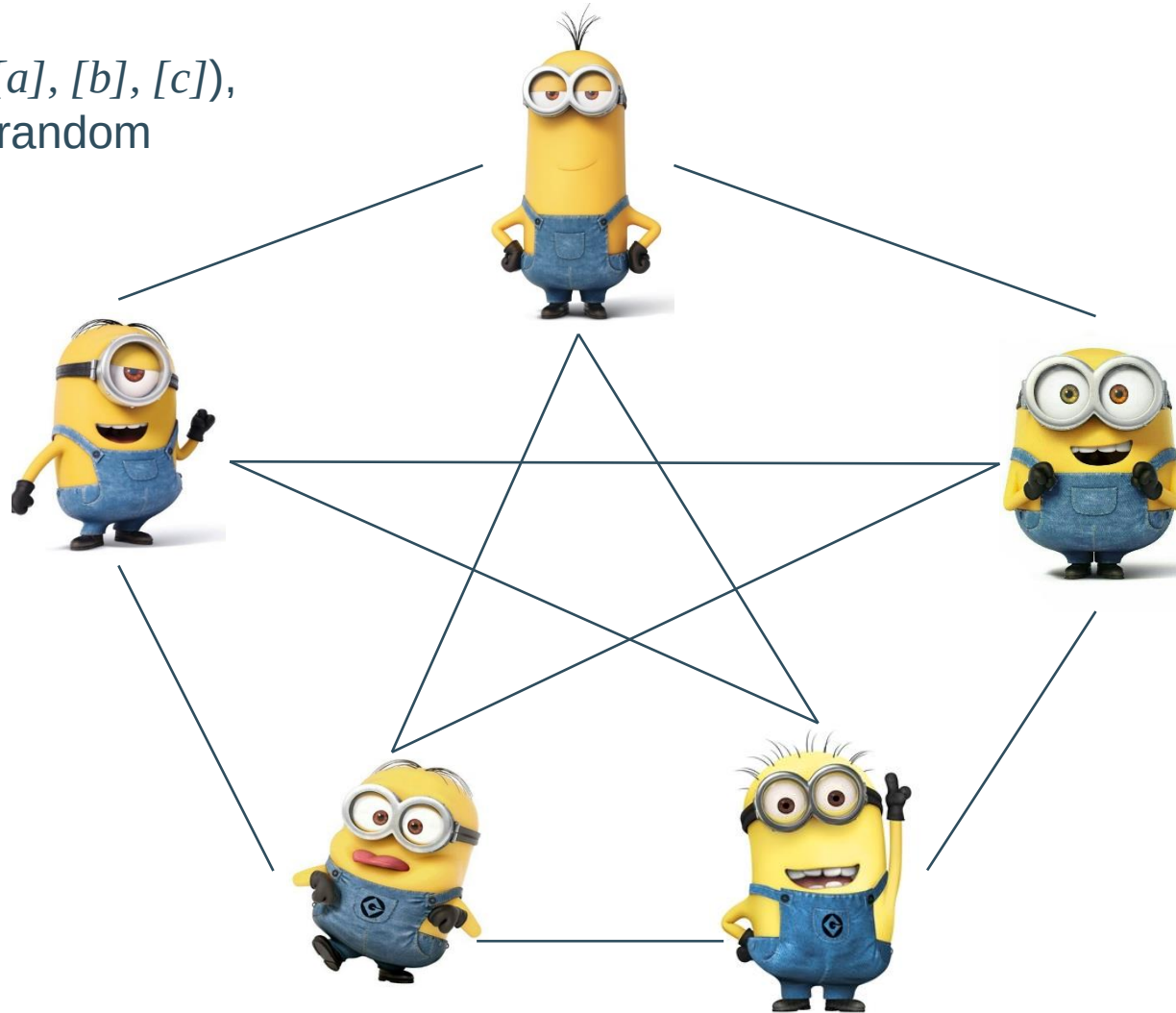
Compute Product $z = x \cdot y$ (online phase) 2/3

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

Open

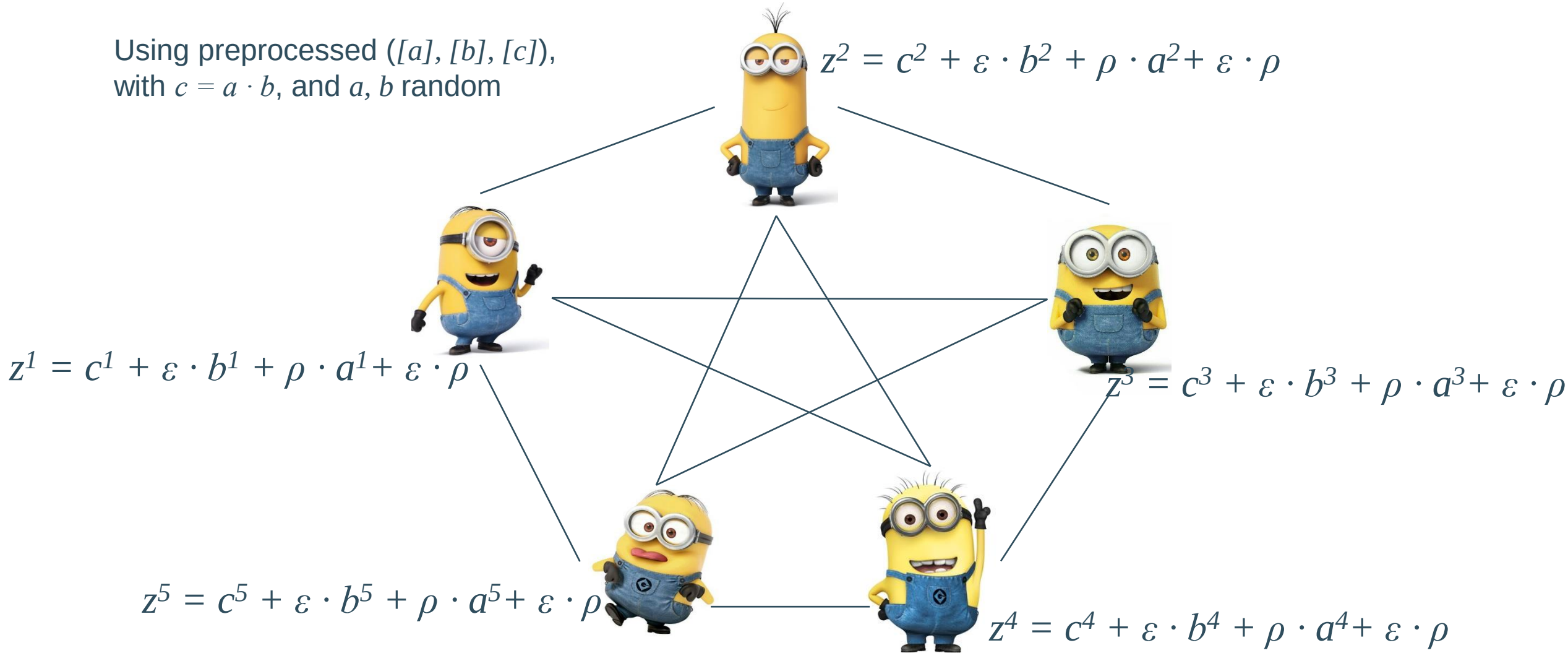
$$\varepsilon = x - a$$

$$\rho = y - b$$



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

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



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