Advancing MPC: From Real-World Applications to LUT-Based Protocols

Dr-Ing. Hossein Yalame

Agenda

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO
CRYPTOGRAPHY AND PRIVACY ENGINEERING

(European) Vision for AI

Privacy-Preserving Computing Toolbox

Our Technical Contributions

Impact

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

(European) Vision for AI

Motivation: AI Advances Raise Privacy Issues

496 Million TB data generated per **day** in 2025.

$1.3 Trillion AI market size projected for 2030.

65% of **companies** use AI internally.

74% of **companies** are testing AI technologies.

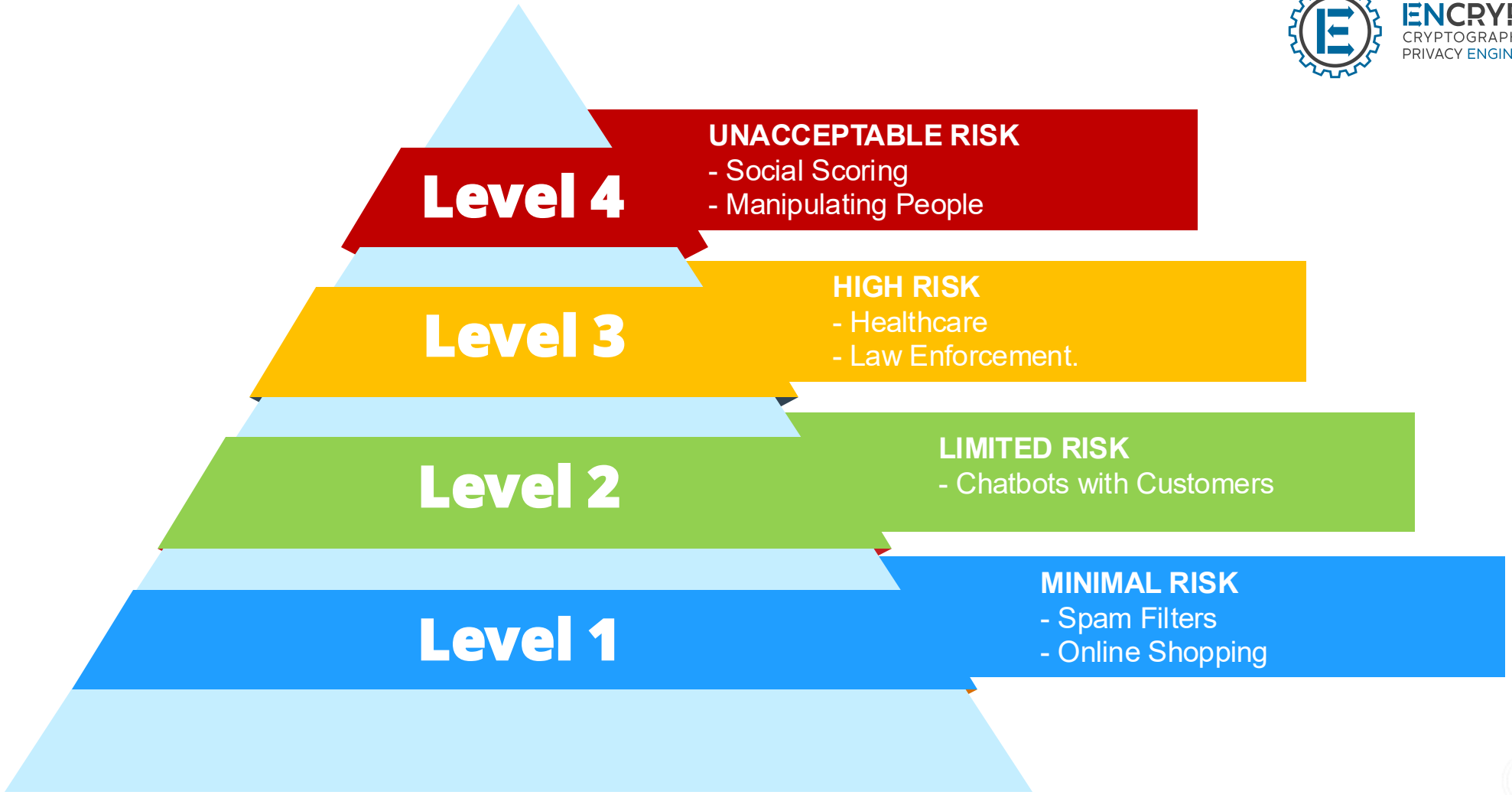
50% of overall investment in US startups went to AI companies in 2024.

More the data -> better the model

GDPR-like regulations became or will become effective in many important markets
(71% of the world's countries have enacted data protection and privacy laws + 9% with draft legislation[1])

[1] *Data Protection and Privacy Legislation Worldwide*. Source: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
Sources: Exploding Topics, Tech.co, https://www.hhs.gov/hipaa/index.html, https://gdpr-info.eu/, https://oag.ca.gov/privacy/ccpa

The AI Act Classifies AI According To Its Risk Into 4 Levels



Source: https://cacm.acm.org/research/the-eu-ai-act-and-the-wager-on-trustworthy-ai/

Countries adapting frameworks prioritizing public trust in AI systems

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

CANADA
PAN-CANADIAN AI STRATEGY
HUMAN RIGHTS
INNOVATION

CHINA
TRANSPARENCY LAWS
PUBLIC ORDER
ChatGPT RESTRICTIONS

UNITED STATES
BLUEPRINT FOR AN AI BILL OF RIGHTS
HEALTHCARE
EMPLOYMENT

JAPAN
SOCIETY 5.0 INITIATIVE
ALIGN ADVANCED TECHNOLOGY
WITH SOCIETAL VALUES

UNITED KINGDOM
GUIDELINES FOR FAIR AND ETHICAL AI
BOOST PUBLIC CONFIDENCE
CONSUMER RIGHTS

G7 COUNTRIES
THE HIROSHIMA AI PROCESS
ENCOURAGE ETHICAL AI DEVELOPMENT

Source: https://cacm.acm.org/research/the-eu-ai-act-and-the-wager-on-trustworthy-ai/

“Computational power requires immediate substantial financial capital, from both public and private sector. In this context, I welcome the European AI Champions Initiative that pledges EUR 150 billion EUR from providers, investors and industry. Today, I can announce with our InvestAI initiative that we can top up by EUR 50 billion. Thereby we aim to mobilise a total of EUR 200 billion for AI investments in Europe. We will have a focus on **industrial** and **mission-critical** applications. It will be the largest public-private partnership in the world for **the development of trustworthy AI**.”

Ursula von der Leyen, President of the European Commission — Speech, Paris, February 11, 2025

Source: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_25_471

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Privacy-Preserving Computing Toolbox

Privacy Preserving Computing Technologies

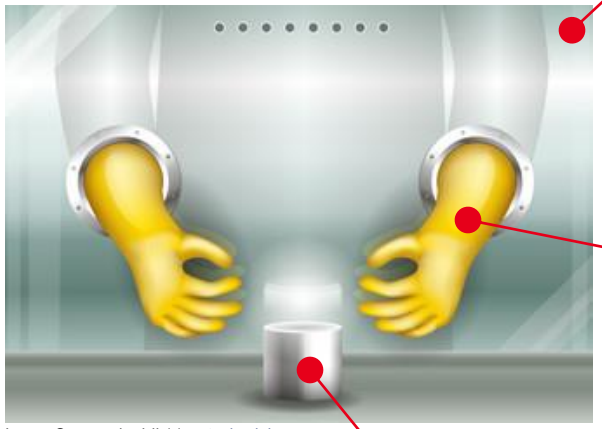
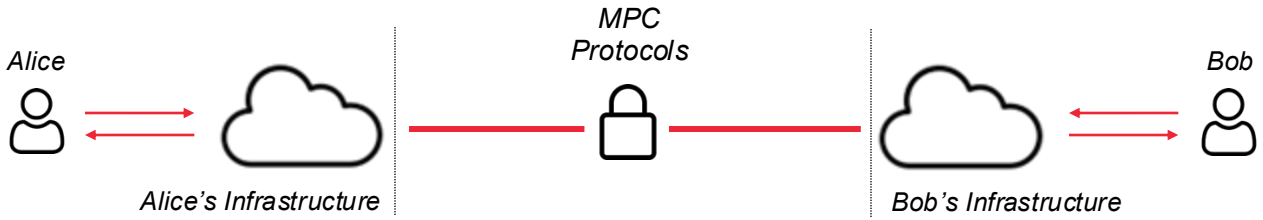


Image Source: denisik11 – stock.adobe.com

Privacy-Preserving Computing Technologies (PPCTs) **seal computing environments** to enforce

- Confidentiality
  (Data is **protected from unauthorized extraction**)
- Integrity
  (Data is **protected from unauthorized alteration**)
- Control
  (Data can be **processed via authorized algorithms only)**

Secure Multiparty Computation



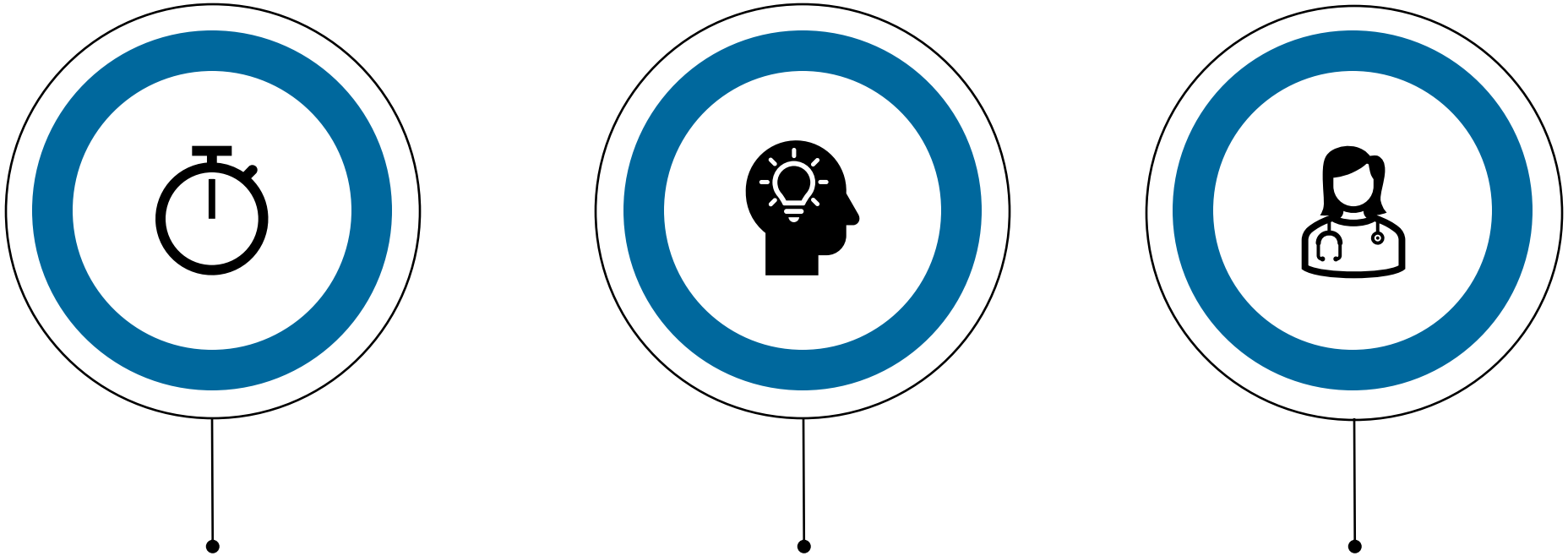
Secure Multiparty Computation *(MPC) uses* **cryptographic protocols** *to distribute a computation among* **multiple parties** *in such a way that* **none of the parties can see the data of the other parties** *or have to trust any system components other than their own.*

- MPC allows a set of parties with private inputs to compute some joint function of their inputs
- Properties of MPC:
  - **Correctness** – Parties should obtain the correct function output
    - Arithmetic/Boolean/Lookup Table Circuits
  - **Privacy** – Nothing more than the function output should be revealed
    - Semi-honest vs Malicious

Trustworthy AI faces three major technical challenges hindering practicality.

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

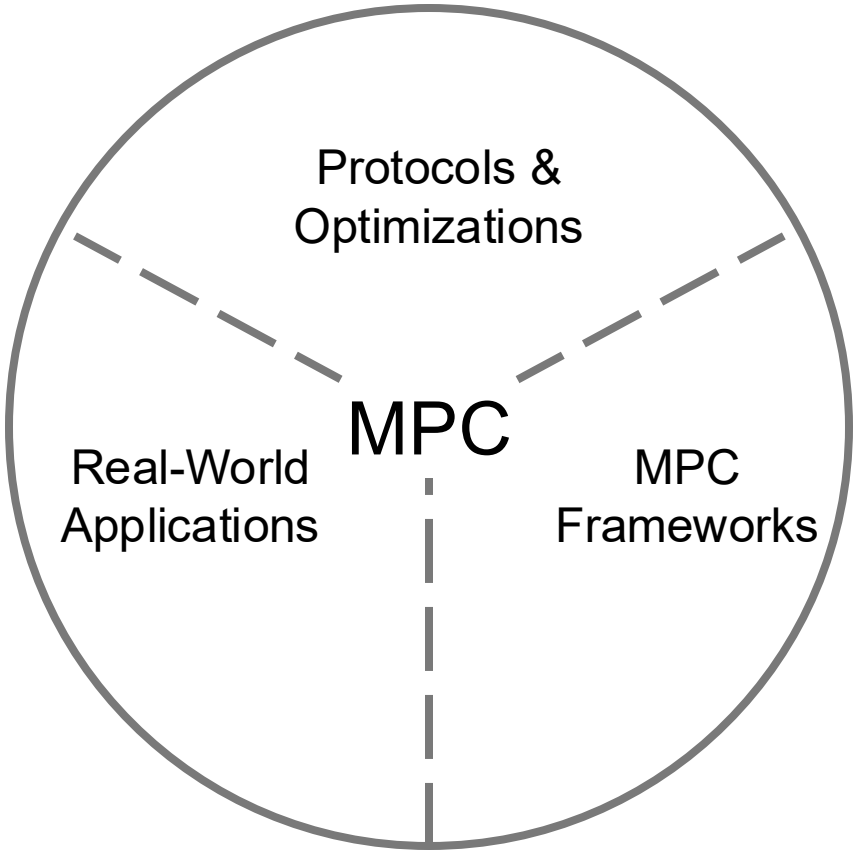


C1 - Efficiency

C2 - Usability

C3 - Interdisciplinarity

Trustworthy AI faces three major technical challenges hindering practicality.

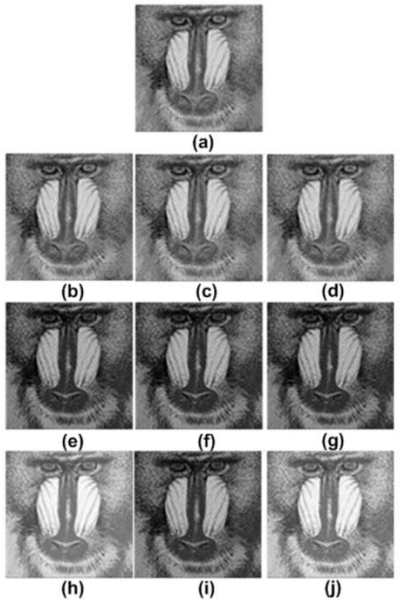


Research Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Approximation for Efficient ML Implementation

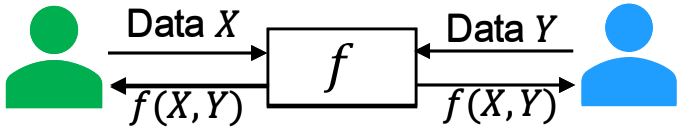


(IEEE TC'20)

Cryptographic Protocols

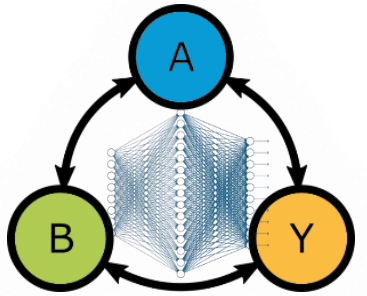
Secure Multi-Party Computation (MPC)

(**USENIX Security'21**,**ACSAC'21**,**IEEESP'23**,**ASIACRYPT'23**, **IEEESP'24**)



Privacy-Preserving Machine Learning (PPML)

(ARES'20,DLS@IEEES&P'21,SECRYPT'21,**PETS'21**,**USENIX Security'22**,**IEEETIFS'23**,DLS@IEEES&P'23,SATML'24,ESORICS'24)



Compilers for Cryptographic Protocols

(ACNS'21,HOST'21,SECYRPT'23,DAC'24,ACSAC'24)

2017 2019 2024

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

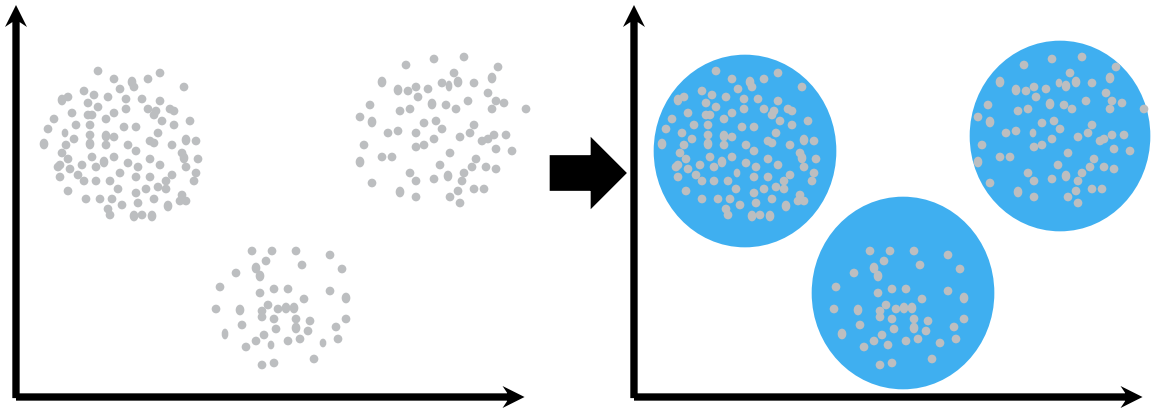
Our Technical Contributions

Clustering groups similar items

- **Input**: $x_1, x_2, \ldots, x_N \in X$
- **Distance**: $d(x_1, x_2)$

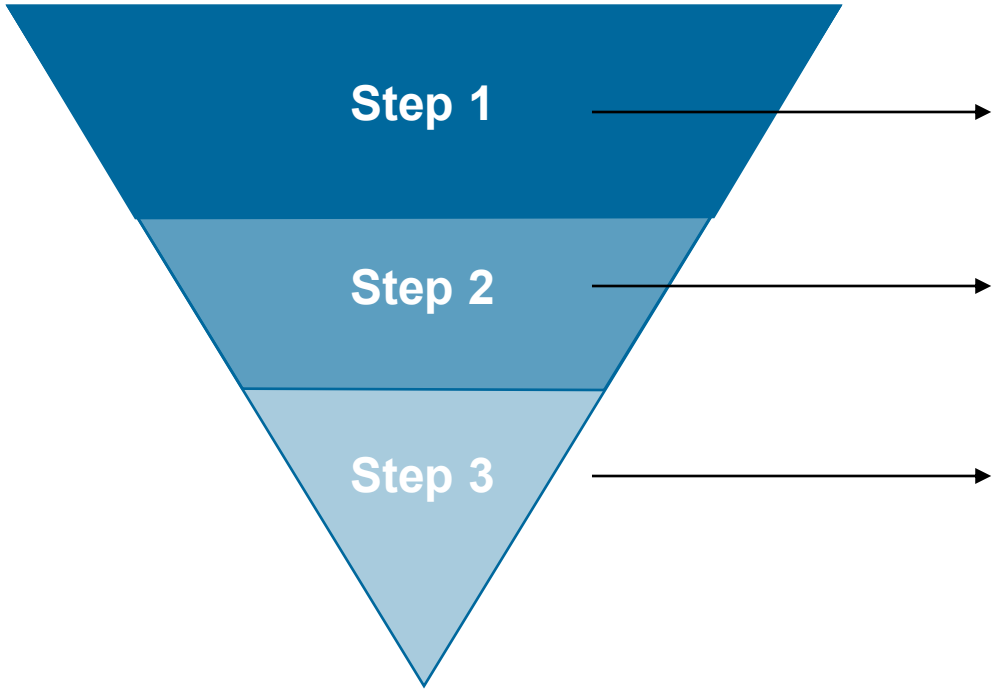
⇒ **Optimal clustering**:

  - Elements in same cluster should be close
  - Elements in different clusters should be far apart



[HMSY21] A. Hegde, H. Möllering, T. Schneider, and **H. Yalame**. SoK: Efficient Privacy-Preserving Clustering. In PETS, 2021. CORE rank A.

How to choose a suitable privacy-preserving clustering scheme?



Application Requirements Analysis

Identify and priorities the application's requirements w.r.t.

a) computational efficiency,
b) communication efficiency,
c) participant scenario including
d) number of involved parties,
e) privacy guarantees,
f) plaintext clustering.

Incompatibility Elimination

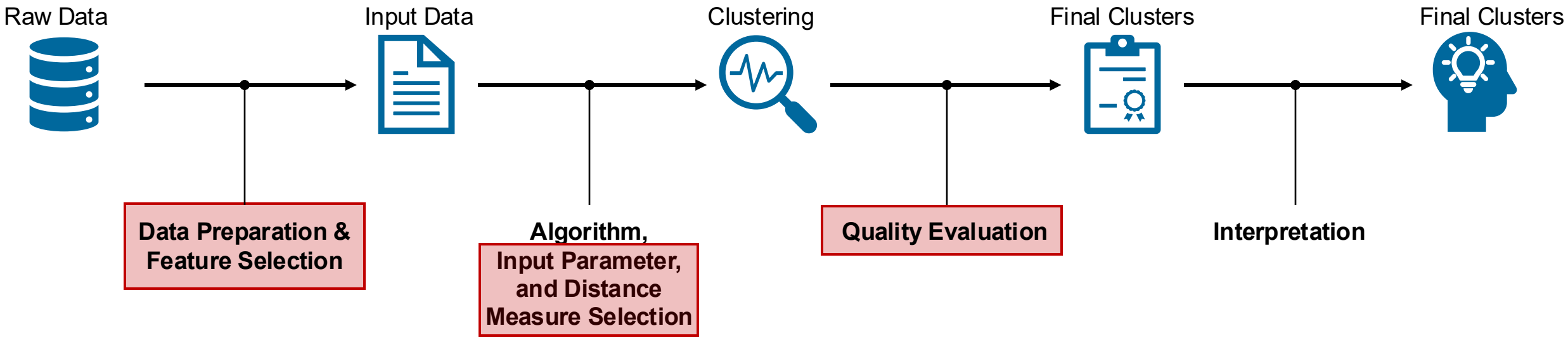
Eliminate not suitable protocols based on the outcome of Step 1.

Final Selection

Select the most appropriate scheme from the remaining options based on the relevant key factors of the application.

Open Research Direction

- E2E-Perspective:



Our Contributions (PETS'21)

✓ First **systemization** of privacy-preserving clustering schemes

✓ Identifcation of the most efficient fully privacy-preserving clustering protocols

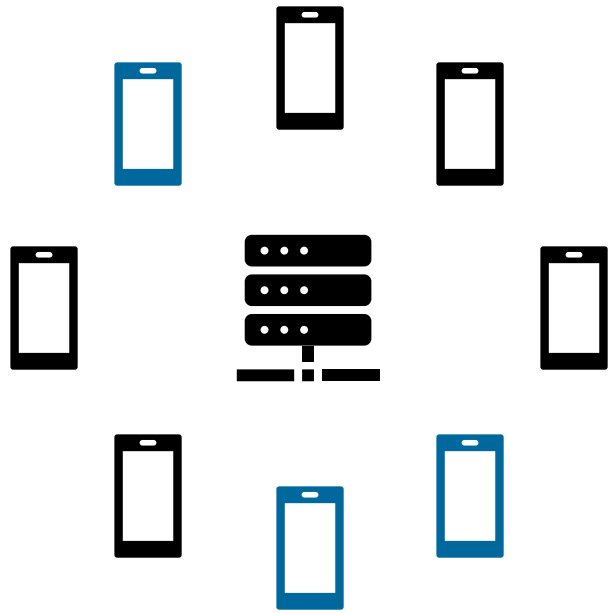
✓ In-depth theoretical and empirical comparisons

✓ Identification of practical deployment **limitations**

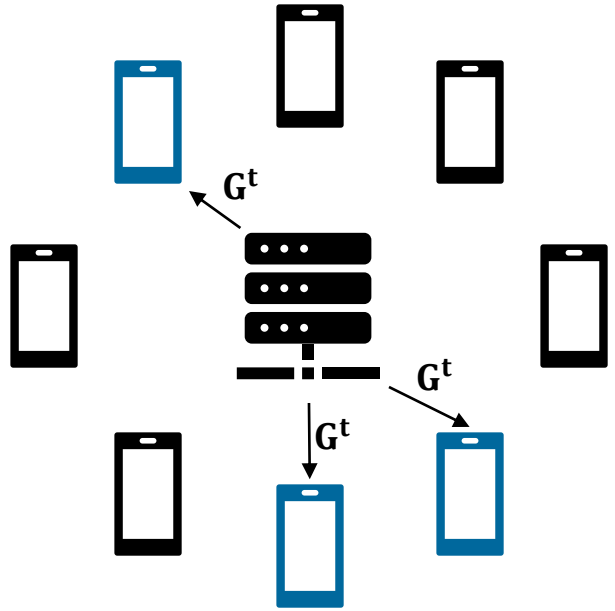
✓ **Open-source** implementation and benchmarks (MIT license)

[HMSY21] A. Hegde, H. Möllering, T. Schneider, and **H. Yalame**. SoK: Efficient Privacy-Preserving Clustering. In PETS, 2021. CORE rank A.

Federated Learning [MMR+17]

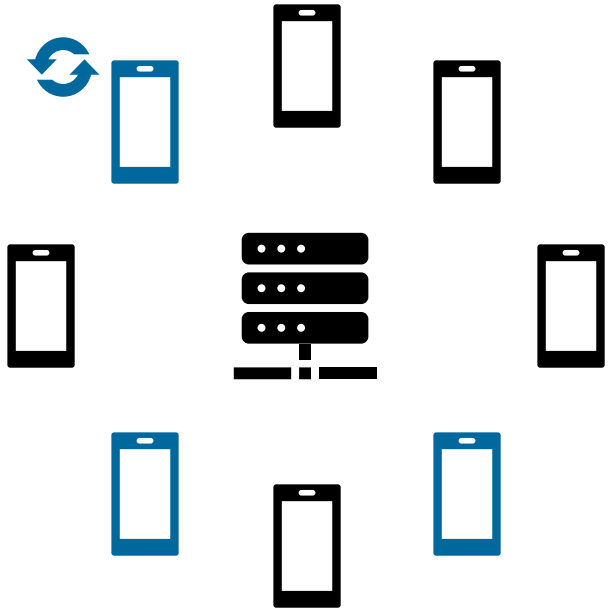


(a) Client Selection

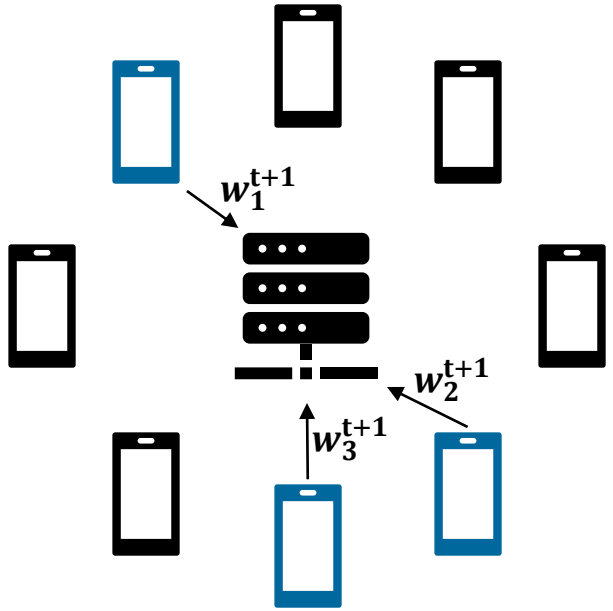


(b) Retrieval of Global Modal

Federated Learning [MMR+17]

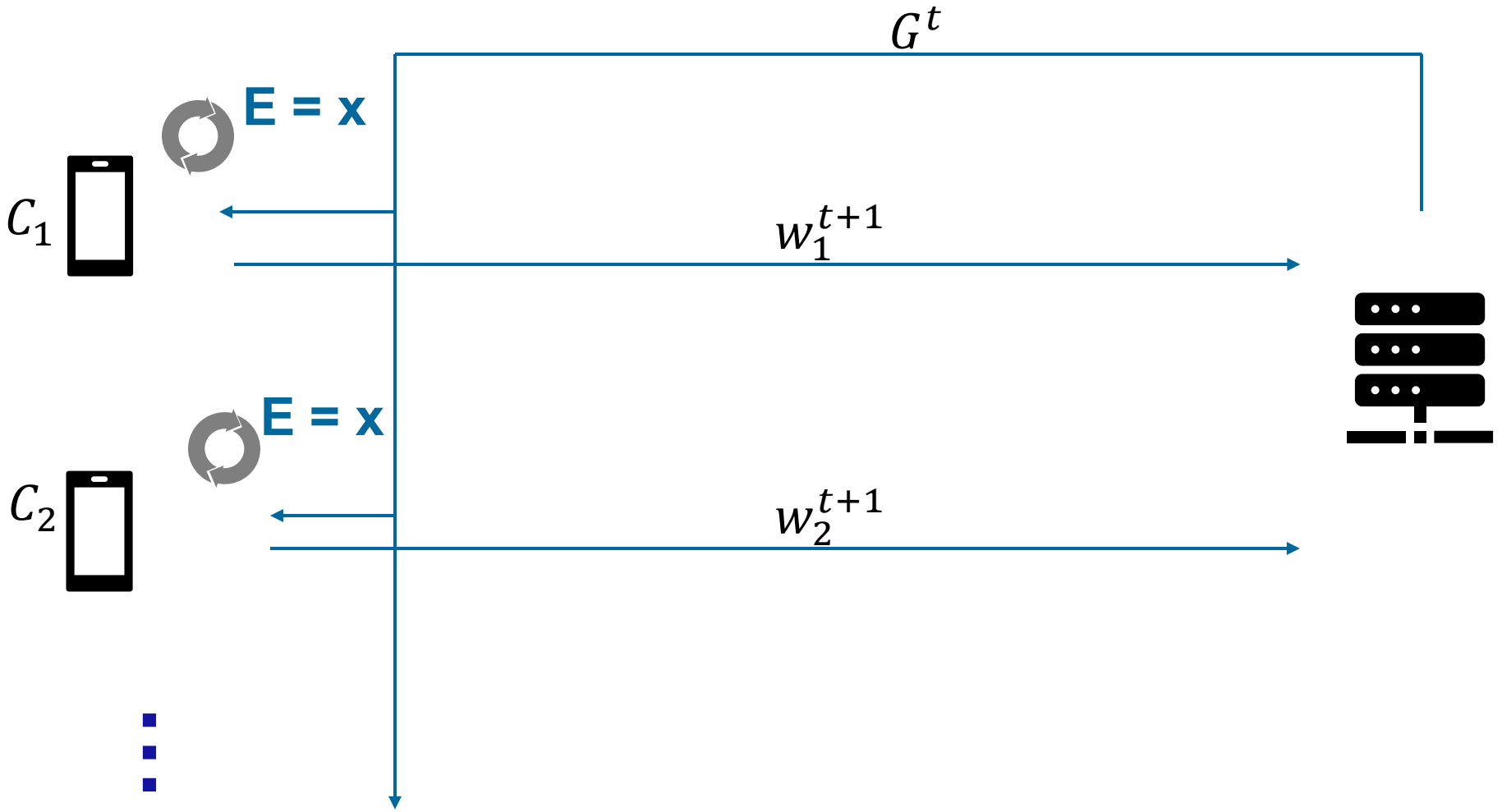


(c) Local Training



(d) Aggregation

Federated Learning [MMR+17]



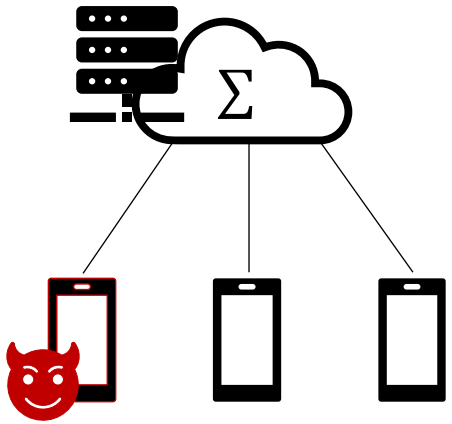
$$G^{t+1} = G^t + \eta \sum_{k=1}^{K} \frac{n_k}{n} w_k^{t+1}$$

FL has deficits in terms of security and data privacy.

TECHNISCHE UNIVERSITÄT DARMSTADT

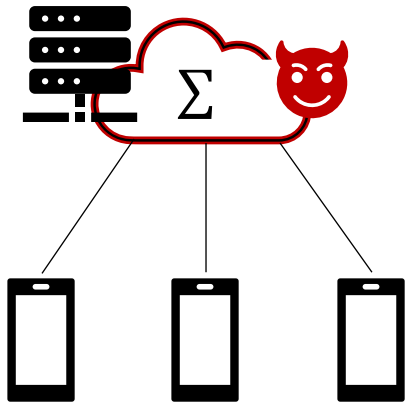
ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Poisoning



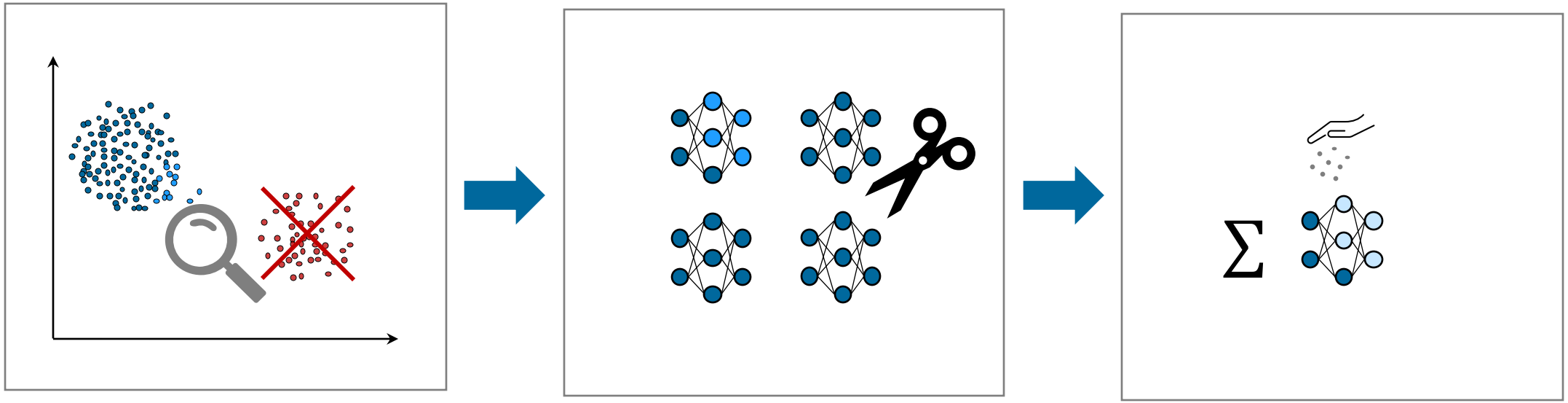
→ Affecting model performance or injecting a backdoor

Inference



→ Extracting information about local training data

We defend poisoning in three steps.



1. Dynamic Model Filtering via Clustering

2. Adaptive Model Clipping

3. Adaptive Noising

Major Manipulations

Minor Manipulations

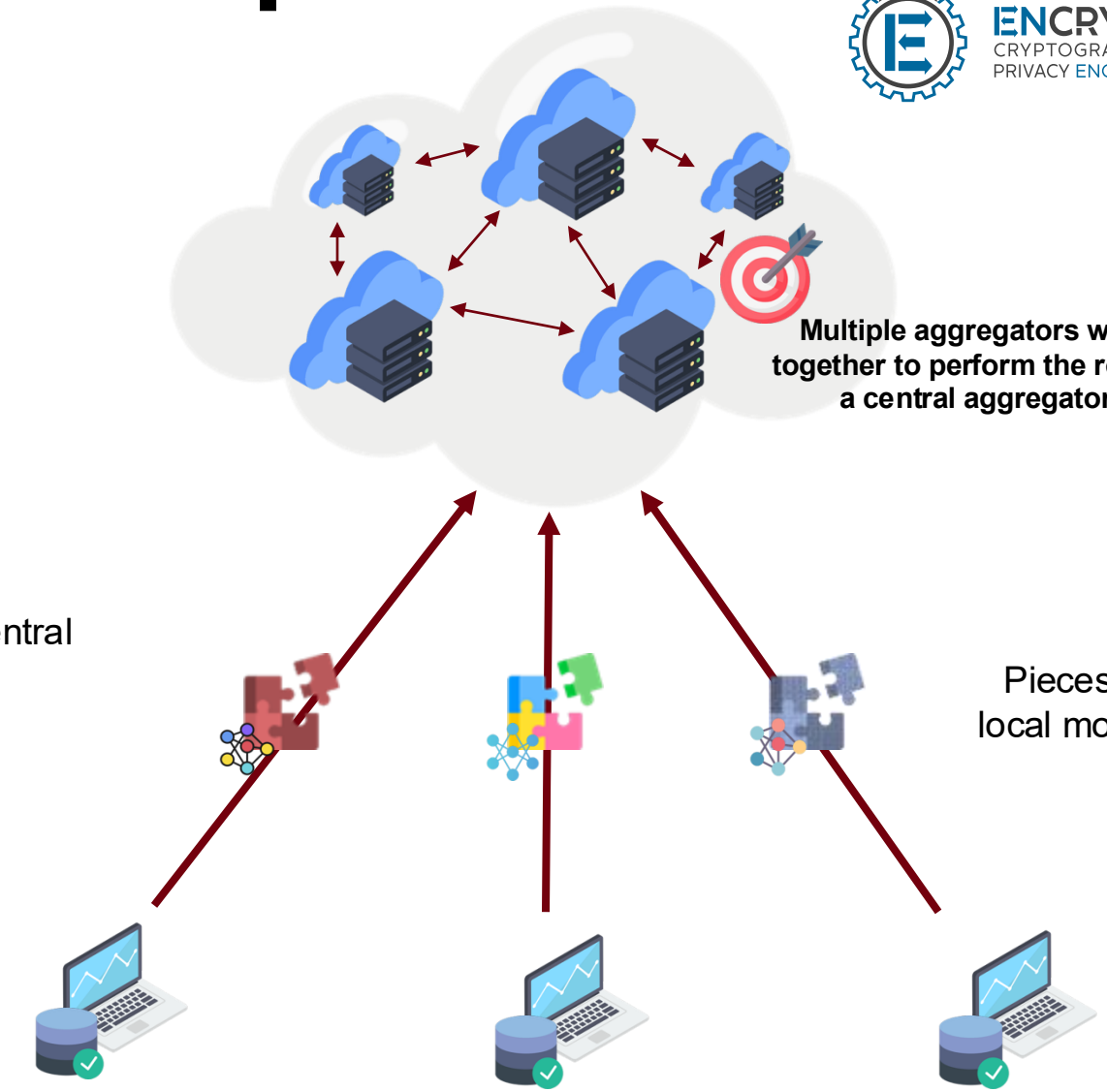
We realize FL “under encryption” to also defend inference attacks on local updates.

TECHNISCHE UNIVERSITÄT DARMSTADT

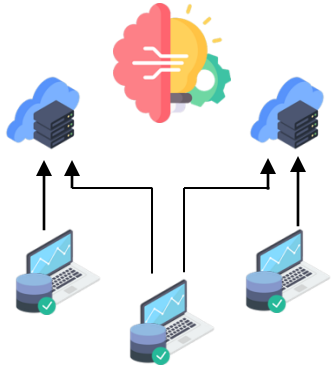
ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

MPC-based Distributed Secure Aggregation

- Utilizes MPC for secure aggregation.
- Ensures privacy through secret-sharing across multiple servers.
- Prevents any server from learning an individual client's update.
- Mitigates model inconsistency attacks from a malicious central aggregator.

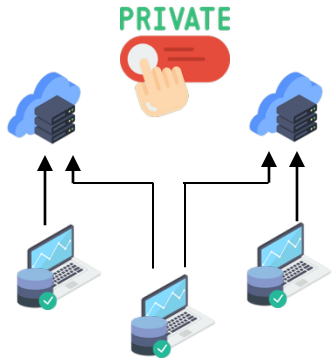


Our FL System



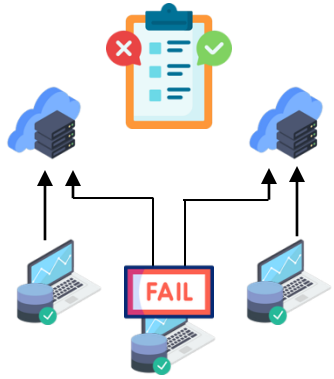
Distributed Aggregation

Multiple servers collectively aggregate as opposed to a central aggregator



Cryptographically-Guaranteed Privacy

Employs secure multi-party computation techniques for secure aggregation



Client Dropout Handling

Ensures correct aggregation in the event of dropouts

Our Contributions (USENIX Security'22/IEEE TIFS'23)

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

✓ **Identification** of privacy **vulnerabilities** in privacy-enhanced federated learning [LLX+21]

✓ **Robustness** and **privacy** for **FL**

✓ **Flexibility** for Various Attack Types

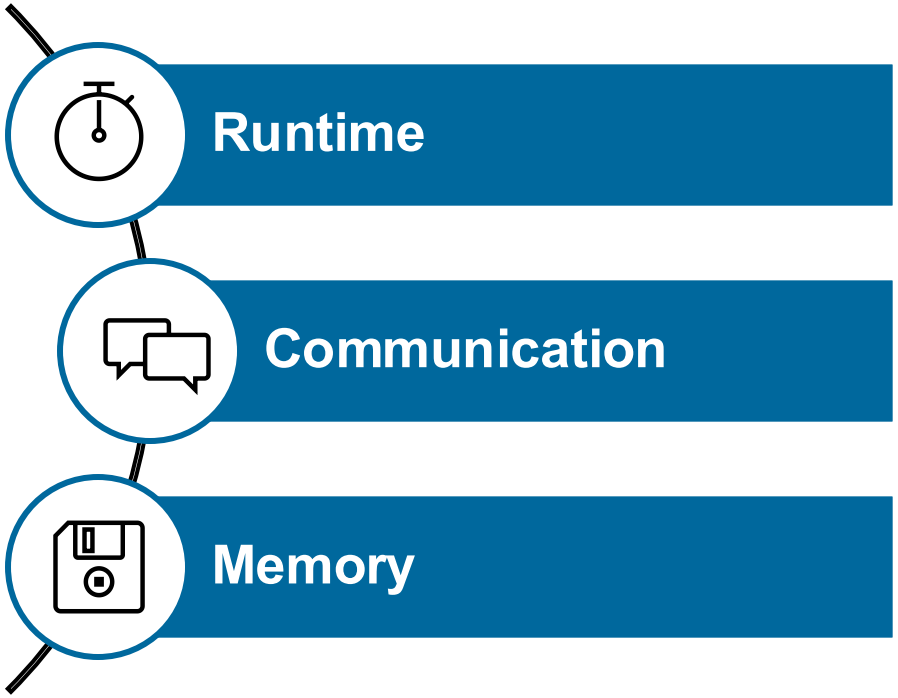
✓ **Comparable** defense **performance** to plaintext version

✓ **Verification** of **Practical** Efficiency in multiple benchmarks

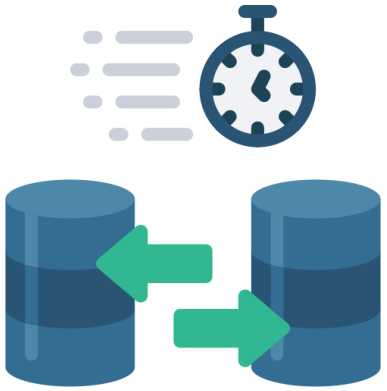
[NRC+22] T. D. Nguyen, P. Rieger, H. Chen, **H. Yalame**, H. Möllering, H. Fereidooni, S. Marchal, M. Miettinen, A. Mirhoseini, S. Zeitouni, F. Koushanfar, A.R. Sadeghi, T. Schneider. FLAME: Taming Backdoors in Federated Learning. In USENIX Security, 2022. CORE Rank A*.

[SSY23] T. Schneider, A. Suresh, **H. Yalame**. Comments on "Privacy-Enhanced Federated Learning Against Poisoning Adversaries". In IEEE TIFS, 2023. CORE Rank A.

Efficiency includes three aspects.



Trustworthy AI Bottlenecks in Practice



Throughput

Network Heterogeneity

Computational Complexity

Our Contributions (ACSAC'21)

- Garbled Circuit (Yao86)

✓ **Automatic batch identification** and computation techniques for efficient use of AES

  - XOR gates free [KS08]
  - AND gate communication:

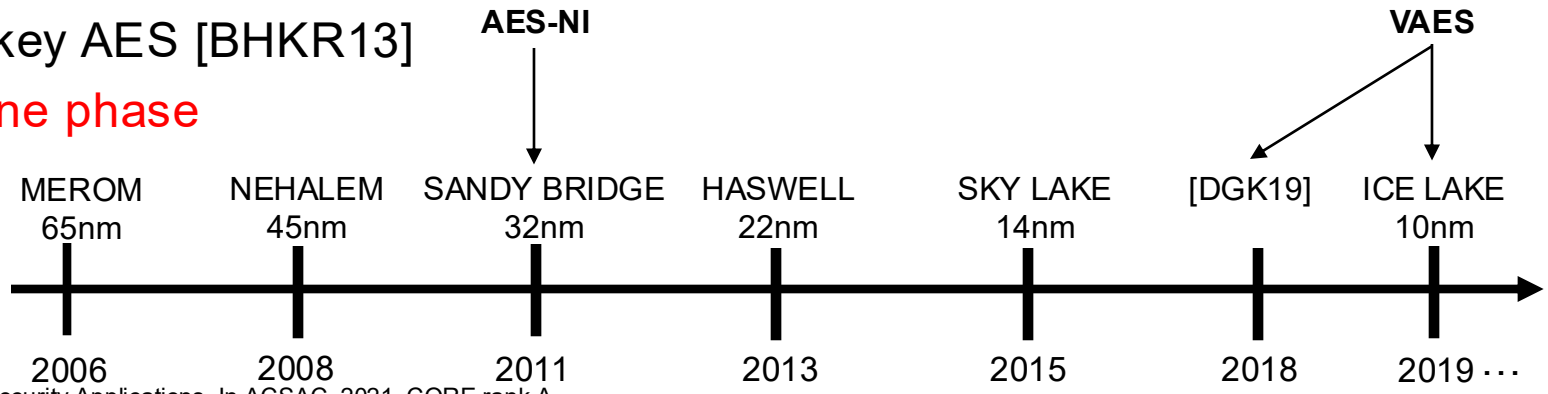
Classical [Yao86]	$4(\kappa+\sigma) = 672$ bit
Point & Permute [BMR90]	$4\kappa = 512$ bit
3-Row Reduction [NPS99]	$3\kappa = 384$ bit
HalfGates [ZRE15]	$2\kappa = 256$ bit
ThreeHalves [RR21]	$1.5\kappa = 192$ bit

$\kappa = 128$: computational security parameter
$\sigma = 40$: statistical security parameter

✓ **First** performance measurements for VAES in the area of MPC

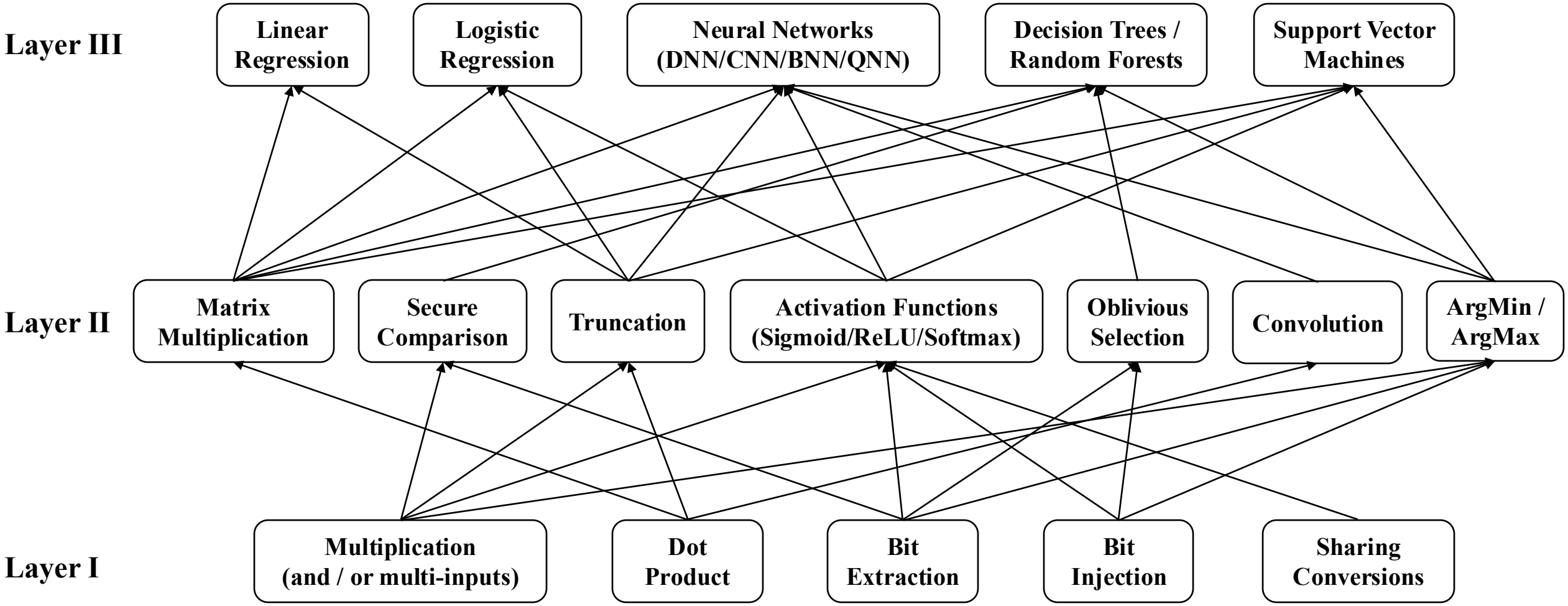
✓ **Open-source** implementation

  - AND gate computation: Fixed-key AES [BHKR13]
    - AES operations in the online phase

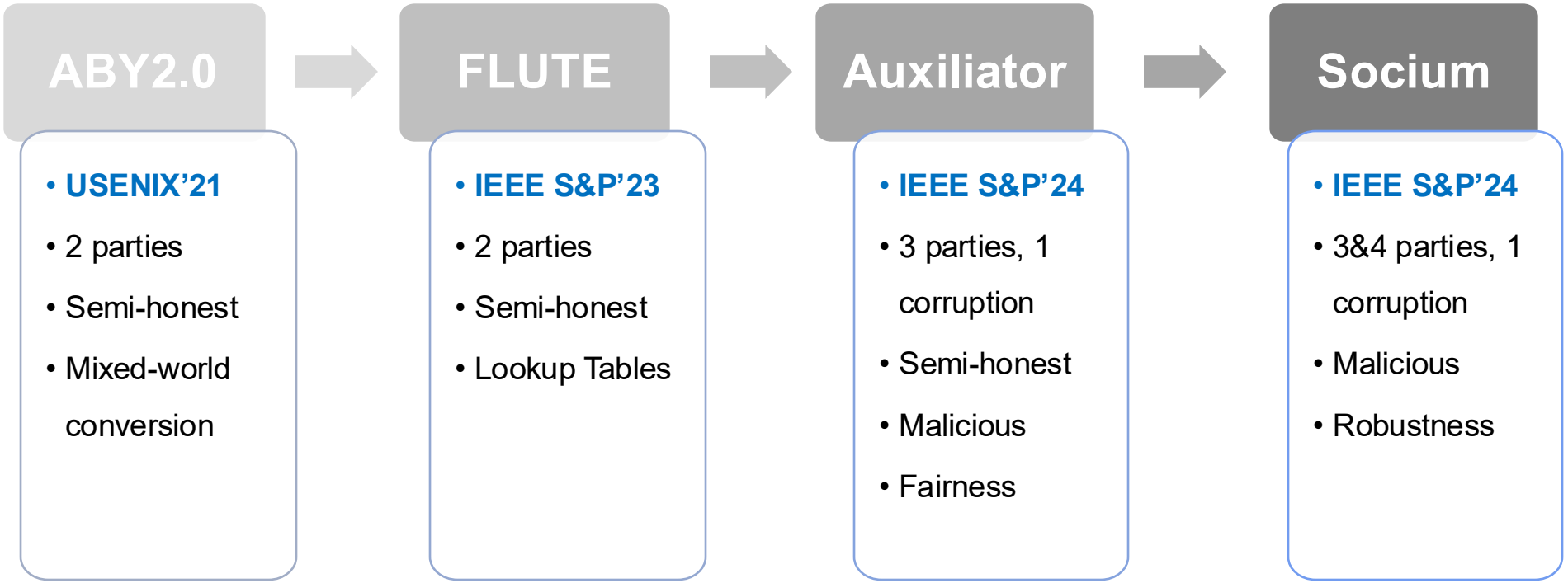


[MSY] J.P. Münch, T. Schneider, and **H. Yalame**. VASA: Vector AES Instructions for Security Applications. In ACSAC, 2021. CORE rank A.

Our three-layer framework



Progress so far ...



Setting	Work	Security	Dot Product		#Active players
			Preprocessing	Online	
3 parties, 1 corruption (semi-honest)	Prior-Work	Semi-honest	0	3	3
	Auxiliator	Semi-honest	1	2	2

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Summary of our results

Dot Product
(d-length vectors)

$$\vec{x} \odot \vec{y} = \sum_{i=1}^{d} x_i y_i$$

Setting	Work	Security	Dot Product		#Active players
			Preprocessing	Online	
3 parties, 1 corruption (semi-honest)	Prior Work	Semi-honest	0	3	3
	Auxiliator	Semi-honest	1	2	2
3 parties, 1 corruption (malicious)	Prior Work	Abort	12d	9d	3
	Auxiliator	Fair	3	3	2

Summary of our results

Dot Product
(d-length vectors)

$$\vec{x} \odot \vec{y} = \sum_{i=1}^{d} x_i y_i$$

Setting	Work	Security	Dot Product		#Active players
			Preprocessing	Online	
3 parties, 1 corruption (semi-honest)	Prior Work	Semi-honest	0	3	3
	Auxiliator	Semi-honest	1	2	2
3 parties, 1 corruption (malicious)	Prior Work	Abort	12d	9d	3
	Auxiliator	Fair	3	3	2

1st time in 3PC malicious:
Dot product with size independent communication

Summary of our results

Dot Product
(d-length vectors)

$$\vec{x} \odot \vec{y} = \sum_{i=1}^{d} x_i y_i$$

Setting	Work	Security	Dot Product		#Active players
			Preprocessing	Online	
3 parties, 1 corruption (semi-honest)	Prior Work	Semi-honest	0	3	3
	Auxiliator	Semi-honest	1	2	2
3 parties, 1 corruption (malicious)	Prior Work	Abort	12d	9d	3
	Auxiliator	Fair	3	3	2
4 parties, 1 corruption (malicious)	Prior Work	Robust	6	6	2
	Socium	Fair & Robust	2	3	2

Summary of our results

Dot Product
(d-length vectors)

$$\vec{x} \odot \vec{y} = \sum_{i=1}^{d} x_i y_i$$

Setting	Work	Security	Dot Product		#Active players
			Preprocessing	Online	
3 parties, 1 corruption (semi-honest)	Prior Work	Semi-honest	0	3	3
	Auxiliator	Semi-honest	1	2	2
3 parties, 1 corruption (malicious)	Prior Work	Abort	12d	9d	3
	Auxiliator	Fair	3	3	2
4 parties, 1 corruption (malicious)	Prior Work	Robust	6	6	2
	Socium	Fair & Robust	2	3	2
2 parties, 1 corruption	Prior Work	Semi-honest	d.|Triples|	4d	2
	ABY2.0	Semi-honest	d.|Triples|	2	2

Summary of our results

Dot Product
(d-length vectors)

$$\vec{x} \odot \vec{y} = \sum_{i=1}^{d} x_i y_i$$

Setting	Work	Security	Dot Product		#Active players
			Preprocessing	Online	
3 parties, 1 corruption (semi-honest)	Prior Work	Semi-honest	0	3	3
	Auxiliator	Semi-honest	1	2	2
3 parties, 1 corruption (malicious)	Prior Work			9d	3
	Au			3	2
4 parties, 1 corruption (malicious)	P			6	2
	Socia	Re	2	3	2
2 parties, 1 corruption	Prior Work	Semi-honest	d.|Triples|	4d	2
	ABY2.0	Semi-honest	d.|Triples|	2	2

1st time in 2PC:
Dot product with size independent online communication

Summary of our results

Dot Product
(d-length vectors)

$$\vec{x} \odot \vec{y} = \sum_{i=1}^{d} x_i y_i$$

NN Inference

	Runtime (ms)	
	LAN	WAN
SOTA [MZ17]	8.77	1760
ABY2.0	**2.66**	**744**
Improvement	**3.3x**	**2.4x**

	Throughput (queries/min)	
	LAN	WAN
SOTA [MZ17]	40.89	0.12
ABY2.0	**30,795.17**	**91.57**
Improvement	**753x**	**763x**

Dot Product in ABY2.0

Two hidden layers with 128 neurons each, and output of a vector with 10 elements on the MNIST dataset

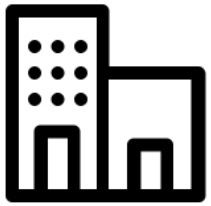
Impact

Science

All code open source & top publications

Society & Citizens

Promotes fundamental rights, including the right to privacy and data protection — core to the EU's vision of human-centric and trustworthy AI.



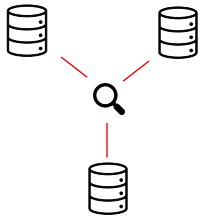
Companies & Developers

Enables a **competitive edge** by embedding privacy-by-design, fostering trust and accountability as outlined in the **EU AI Act** and **Ethics Guidelines for Trustworthy AI**.

Enabling Trustworthy Data Collaboration in AI and Analytics

TECHNISCHE UNIVERSITÄT DARMSTADT

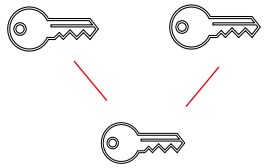
ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING



Virtual Data Pooling

Perform arbitrary computations on top of distributed *virtually* pooled data without transferring any of your data outside your sphere of control

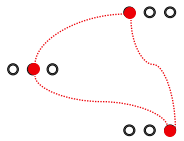
e.g., cross-silo analytics for improved decision making , synthetic data generation



Secrets Management

Distribute cryptographically decomposed sensitive data over multiple locations for maximum security and process it in arbitrary ways without materializing the data in a single location

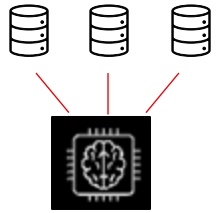
e.g., Virtual HSM with the flexibility of a software-defined solution combined with the security of a hardware-based HSM



Private Correlation

Compute correlations across sensitive datasets and perform arbitrary operations on it

e.g., distributed supply chain risk analysis or cross-organization cyber threat intelligence



Collaborative Learning

Protect training data and machine learning models end-to-end in federated and machine learning settings

e.g., improve data driven services using sensitive customer data, synthetic data generation

Thank you

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

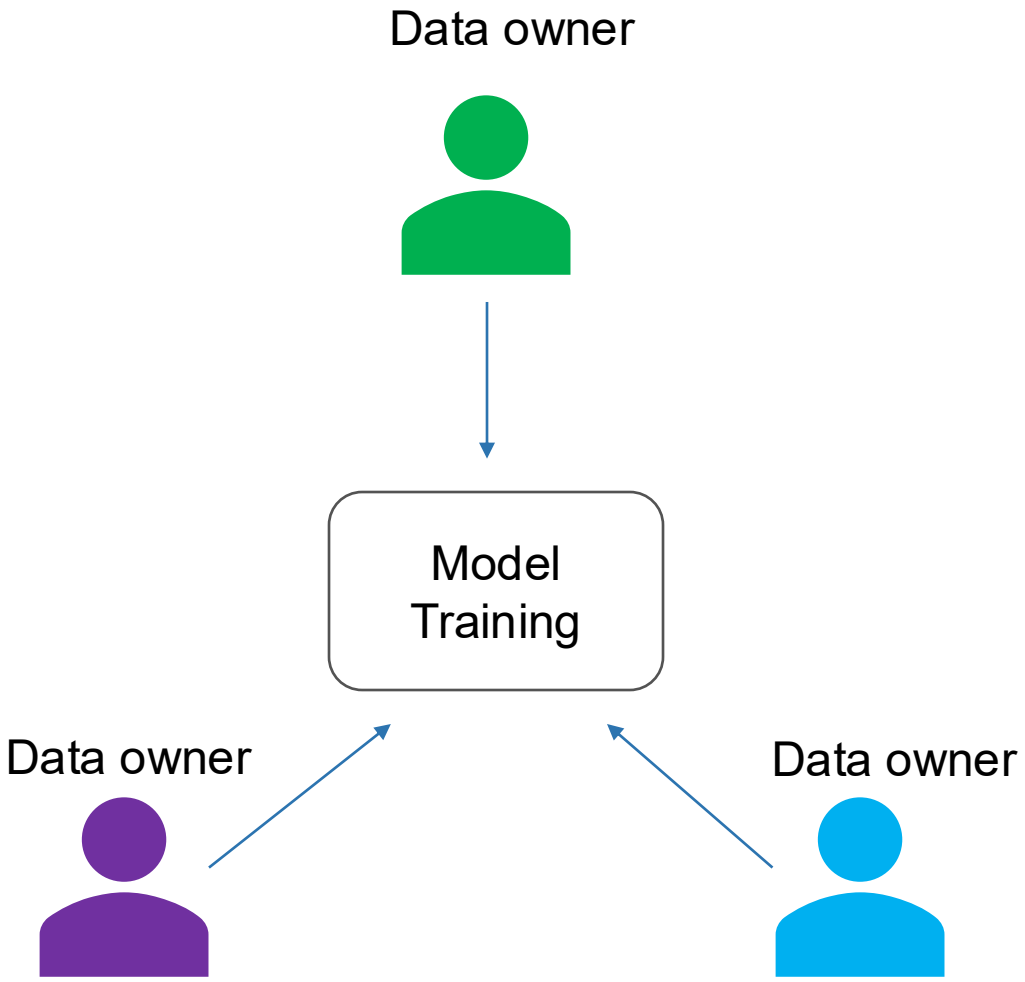
1. *SoK: Efficient Privacy-Preserving Clustering.* PETS'21 [CORE - A]
   Authors: Aditya Hegde, Helen Möllering, Thomas Schneider, and Hossein Yalame.
2. *VASA: Vector AES Instructions for Security Applications.* ACSAC'21 [CORE - A]
   Authors: Jean-Pierre Münch, Thomas Schneider, and Hossein Yalame.
3. *ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation.* USENIX Security'21 [CORE - A*]
   Authors: Arpita Patra, Thomas Schneider, Ajith Suresh, and Hossein Yalame.
4. *FLAME: Taming Backdoors in Federated Learning.* USENIX Security'22 [CORE - A*]
   Authors: Thien Duc Nguyen, Phillip Rieger, Huili Chen, Hossein Yalame, Helen Möllering, Hossein Fereidooni, Samuel Marchal, Markus Miettinen, Azalia Mirhoseini, Shaza Zeitouni, Farinaz Koushanfar, Ahmad Reza Sadeghi, and Thomas Schneider.
5. *Comments on "Privacy-Enhanced Federated Learning against Poisoning Adversaries".* IEEE TIFS'23 [CORE - A]
   Authors: Thomas Schneider, Ajith Suresh, and Hossein Yalame.
6. *Breaking the Size Barrier: Universal Circuits Meet Lookup Tables.* ASIACRYPT'23 [CORE - A]
   Authors: Yann Disser, Daniel Günther, Thomas Schneider, Maximilian Stillger, Arthur Wigandt, and Hossein Yalame.
7. *FLUTE: Fast and Secure Lookup Table Evaluations.* IEEE S&P'23 [CORE - A*]
   Authors: Andreas Brüggemann, Robin Hundt, Thomas Schneider, Ajith Suresh, and Hossein Yalame.
8. *Don't Eject the Impostor: Fast Three-Party Computation with A Known Cheater.* IEEE S&P'24 [CORE - A*]
   Authors: Andreas Brüggemann, Oliver Schick, Thomas Schneider, Ajith Suresh, and Hossein Yalame.

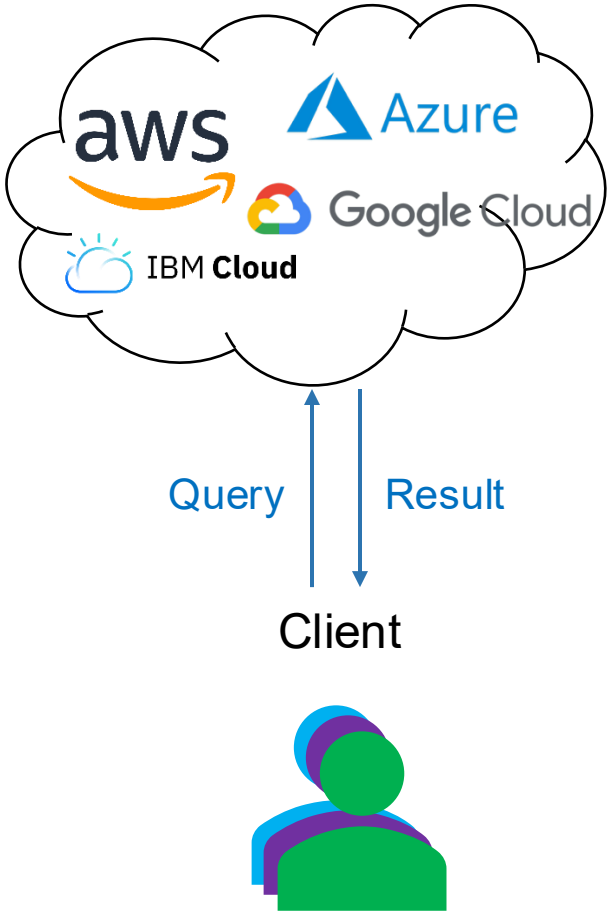
TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

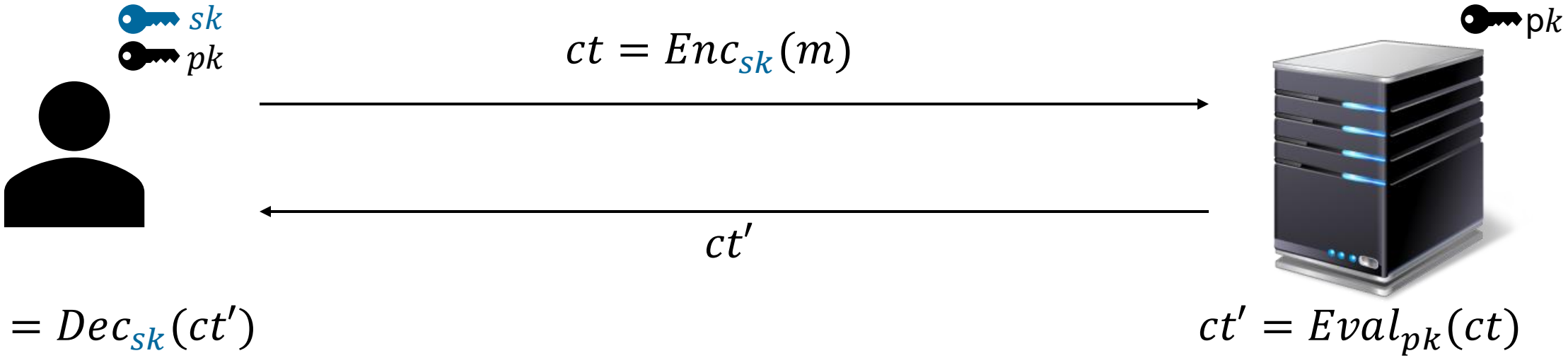
Backup - MISC

Privacy in AI

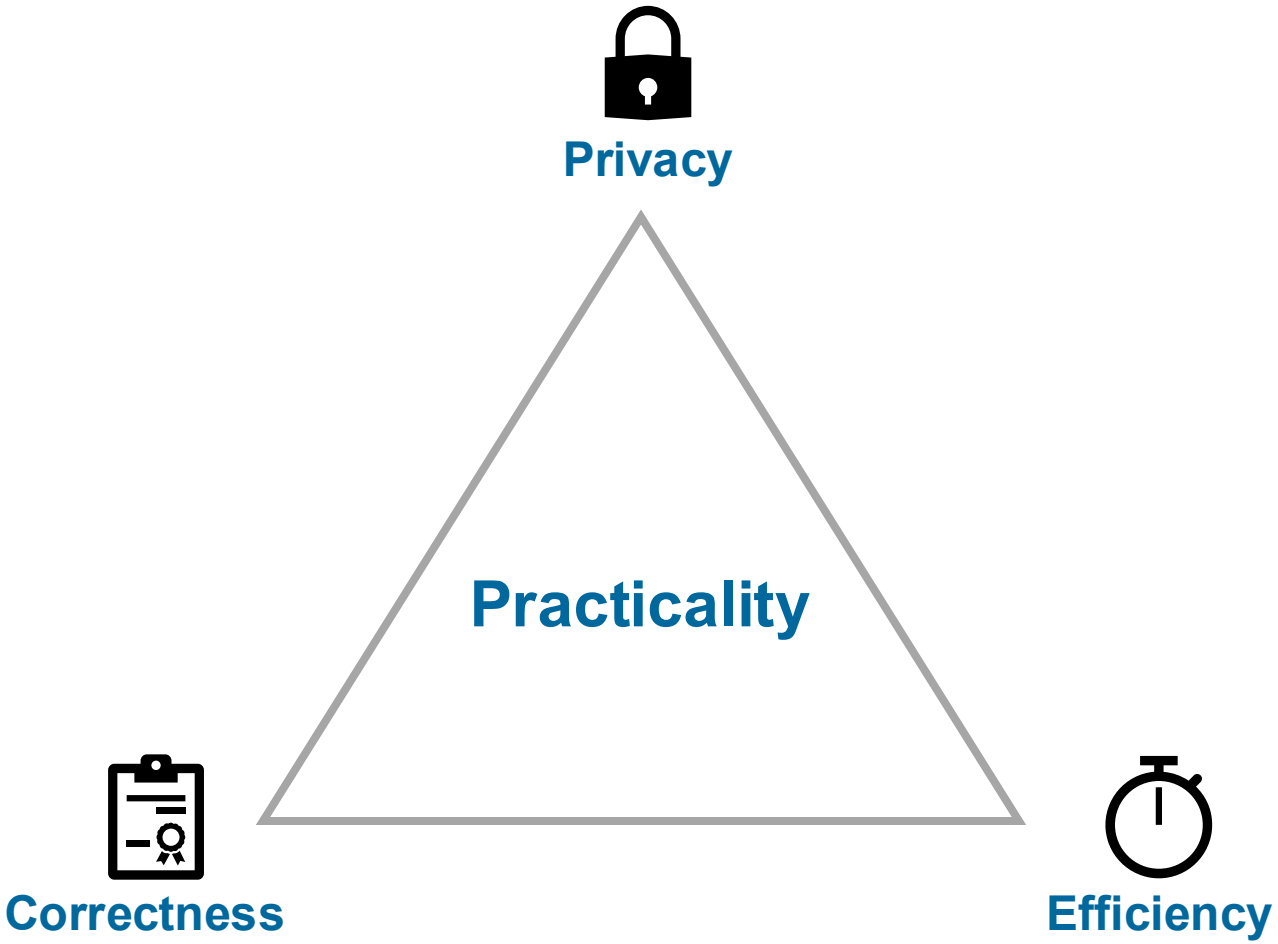




Homomorphic Encryption



Practical Private Solutions

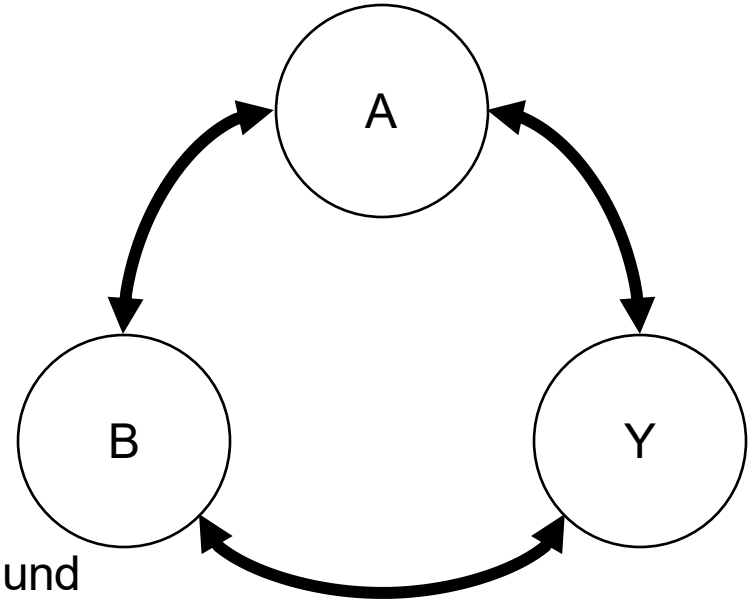


Why Semi-Honest Security

- Semi-honest/passive security: All parties honestly follow the protocol (honest-but-curious)
- Weaker than malicious/active security: Any cheating is detected and no information leakage
- But:
  - Often parties are semi-honest already:
    must comply with regulations, potential loss of reputation, …
  - Baseline performance/lower Bounds:
    What is the minimal overhead of secure computation over plaintext computation?
  - Can be extended to stronger security models via standard techniques
    e.g., cut-and-choose, zero-knowledge proofs, …

Mixed Protocols

Arithmetic Sharing [GMW87:STOC]
- Computations over ring $\mathbb{Z}_{2^\ell}$
- ADD: free
- MUL: **4 elements communication**, 1 round
- N−MUL: **4 (N-1) elements communication**, $\boldsymbol{log N_2}$ **round**



Boolean Sharing [GMW87:STOC]
- Computations over bits $\{0,1\}$
- XOR: free
- AND: **4 bits communication**, 1 round
- N−AND: **4 (N-1) bits communication**, $\boldsymbol{log N_2}$ **round**

Yao Sharing = Garbling [Yao86:FOCS]
- Computations over bits $\{0,1\}$
- XOR: free
- AND: communication, no rounds

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Backup - Clustering

Clustering Applications

Open Research Directions (1/2)

TECHNISCHE UNIVERSITÄT DARMSTADT

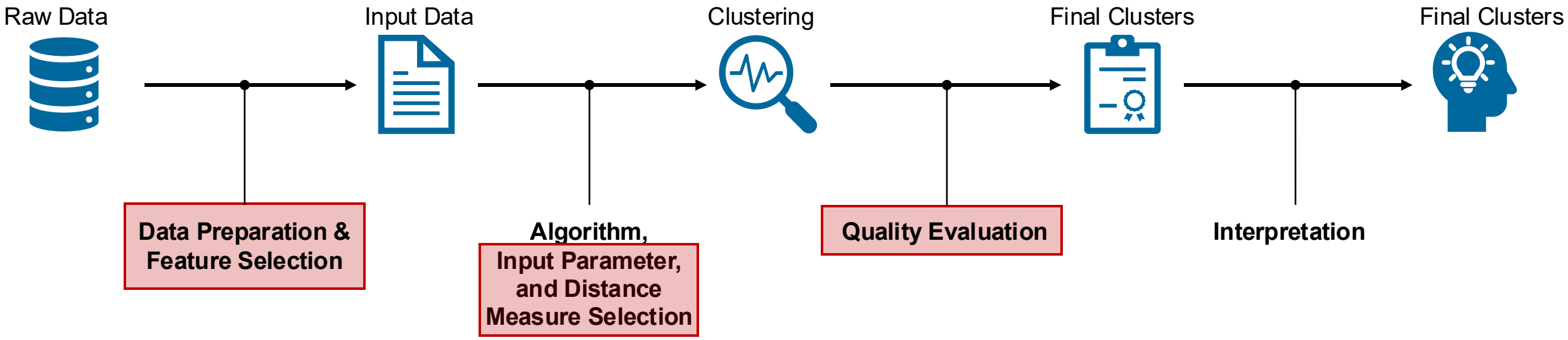
ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

- More Clustering Algorithms:

	K-means	K-medoids	GMM	Mean-shift	DBSCAN	HC	BIRCH	Aff. Prop.
Cluster Shapes	-	-	-	+	+	○	-	-
Large Datasets	○	-	○	-	-	-	+	-
Update Input Data	+	+	+	○	+	-	+	-
Nominal Variables	-	+	-	-	+	+	-	+
Outliers	-	○	○	-	+	○	+	+
Input Order	+	+	+	+	○	+	-	+
Storage	+	-	+	+	+	-	+	-
# Parameters	-	-	-	○	○	-	○	○
Fully Private	✓	✗	✗	✓	✓	✓	✗	✓

Open Research Directions (2/2)

- E2E-Perspective:

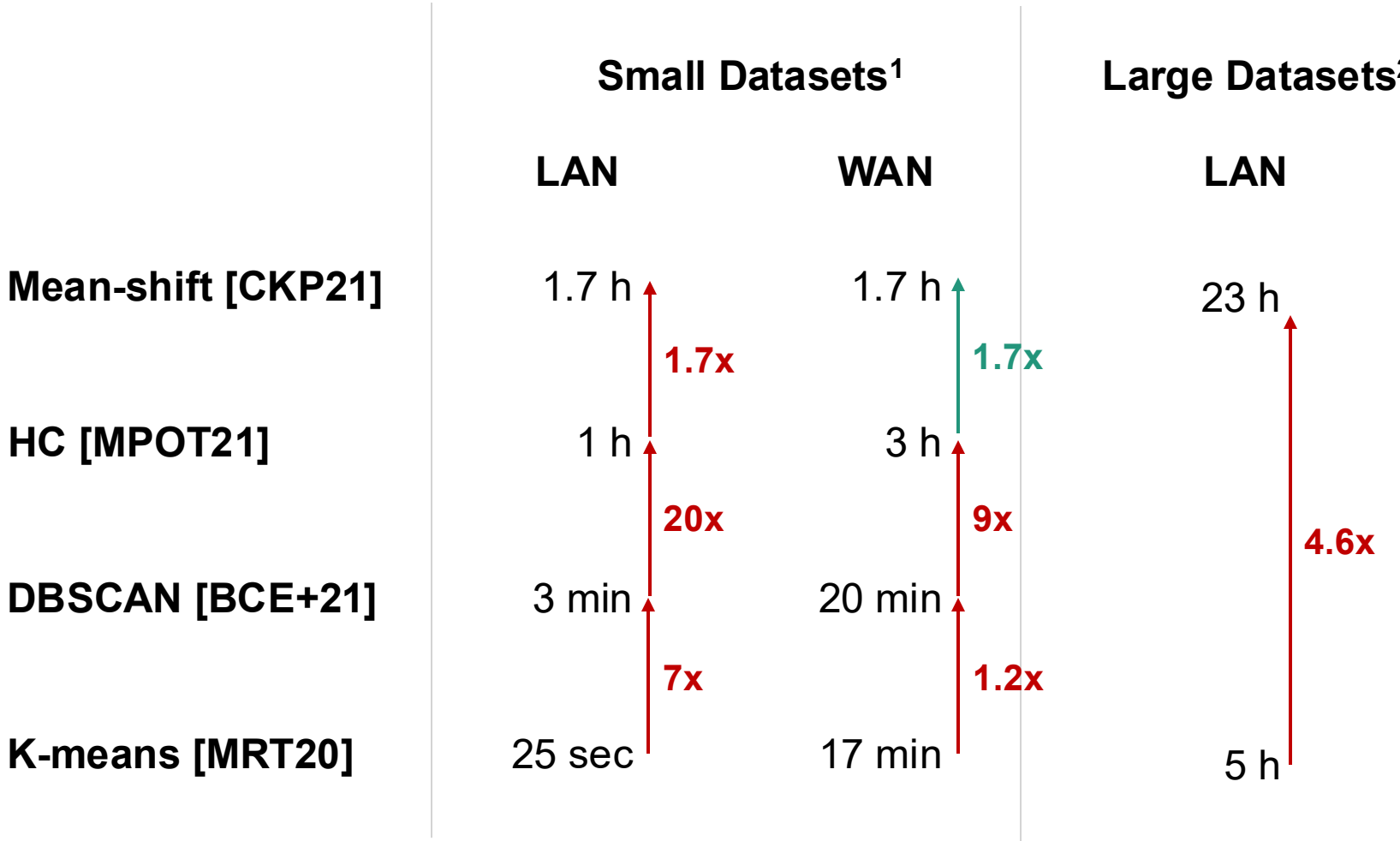


59 Works for Privacy-Preserving Clustering

Algorithm	Scheme	Privacy	Security	PETs	L1	L2	L3	L4	O1	O2	O3	Interactivity (Scenario)	Data	Other issues
K-means	[82, KDD'03]	✗	◐	HE+blinding	(✗)[1]	✗	✗	✗	✗	✓	✗	all data owners (≥ 3)	v	
	[83, KDD'05]	✗	◐	HE+ASS+GC	✓	✓	✗	✗	✓	✓	✗	2PC	a	wrong division
	[84, ESORICS'05]	✗	◐	HE *or* OPE	✗	✓	✓	✗	✗	✓	✗	2PC	h	
	[12, CCS'07]	✓	◐	HE+ASS	✓	✓	✓	✗	✗	✓	✗	2PC	a	
	[85, SECRYPT'07]	✗	◐	blinding	✗	✓	✗	✗	✓	✓	✗	all data owners	v/h	
	[86, AINAW'07]	✗	◐	HE+ASS+OPE	✓	✗	✗	✗	✓	✓	✗	2PC	h	
	[87, PAIS'08]	✗	◐	ASS	✓	✓	✗	✗	✓	✓	✗	all data owners (≥ 4)	v	
	[88, WIFS'09]	✗	◐	HE	✗	✓	✗	✓	✓	✗	✗	data owners + 1 server	h	
	[89, KAIS'10]	✗	◐	HE+ASS	✓	✓	✗	✗	✓	✗	✗	all data owners	h	
	[90, PAISI'10]	✗	◐	SS	✓	✗	✗	✗	✓	✓	✗	Outsourcing ≥ 3 servers	a	
	[91, ISPA'10]	✗	◐	HE	✓	✓	✗	✗	✗	✓	✗	all data owners	v/h	
	[92, WIFS'11]	✗	◐	HE+GC	✓	✗	✓	✓	✓	✗	✗	Outsourcing, 3 servers	h	
	[93, ISI'11]	✗	◐	HE+ASS	(✗)[1]	✗	✗	✗	✓	✗	✗	2PC	v	
	[94, TM'12]	✗	◐	SSS	✗	✗	✓	✗	✗	✓	✗	all data owners	h	distance calculation unclear
	[95, JIS'13]	✗	◐	HE	✗	✓	✓	✗	✓	✗	✗	data owners + 2 servers	h	
	[96, ICDCIT'13]	✗	●	SSS+ZKP	✗	✗	✓	✗	✗	✓	✗	all data owners	h	
	[97, ASIACCS'14]	✗	◐	HE	✗	✗	✗	✗	✓	✓	✗	outsourcing, 1 data owner + 1 server	–	insecure HE [107]
	[98, MSN'15]	✗	◐	HE	✗	✗	✗	✓	✗	✗	✗	outsourcing, data owners + 1 server	h	insecure HE [107]
	[99, IJNS'15]	✗	◐	HE	✗	✗	✗	✗	✗	✓	✗	all data owners	h	
	[13, CIC'15]	✓	◐	HE	✓	✓	✓	✗	✗	✓	✗	Outsourcing, 2 servers	h	
	[100, ICACCI'16]	✗	N/A	SS	✗	✗	✗	✗	✓	✗	✗	arbitrary number of servers	a	
	[101, ISPA'16]	✗	◐	blinding	✗	✗	✗	✓	✗	✓	✗	all data owners (≥ 3)	h	
	[102, SecComm'17]	✗	◐	HE	✓	✗	✗	✓	✗	✓	✗	outsourcing, ≥ 4 servers	h	
	[103, TII'17]	✗	◐	HE	✗	✗	✗	✗	✗	✗	✗	data owners + 1 server	h	
	[14, SAC'18]	✓	◐	HE	✓	✓	✓	✓	✗	✓	✗	Outsourcing, 1 server	–	
	[15, CLOUD'18]	✓	◐	HE	✓	✓	✓	✗	✗	✓	✗	Outsourcing, 2 servers	–	distance calculation unclear
	[108, CCPE'19]	✗	N/A	HE	✗	✗	✗	✗	✗	✓	✗	Outsourcing, 2 data owners + 1 server	h	insecure HE [107]
	[104, TCC'19]	✗	◐	HE	✓	✗	✗	✓	✓	✗	✗	Outsourcing, 1 data owner + $\geq$ 1server(s)	–	
	[105, Inf. Sci.'20]	✗	◐ (●)[2]	HE+GC	✗	✗	✗	✗	✗	✓	✗	Outsourcing, 2 data owners + 1 server	h	
	[106, SCN'20]	✗	◐	HE+SKC	✓	✗	✗	✓	✗	✓	✗	Outsourcing, 3 servers	h	
	[11, PETS'20]	✓	◐	GC	✓	✓	✓	✗	✗	✓	✗	2PC/Outsourcing	h	
	[8, TKDE'20]	✗	◐	HE	✓	✗[3]	✓	✗	✗	✓	✗	Outsourcing, 2 servers	a	
Kernel K-means	[58, KAIS'16]	✗	N/A	PKC	✓	✗	✗	✗	✓	✗	✗	Outsourcing, 1 server	–	security model
Possibilistic C-means	[43, TBD'17]	✗	N/A	HE	✗	✗	✗	✗	✓	✓	✗	Outsourcing, 1 data owner + 1 server	–	
K-medoids	[57, SMC'07]	✗	N/A	HE+blinding	✓	✗	✗	✓	✗	✗	✗	all data owners	v	exhaustive search
	[71, CCSEIT'12]	✗	N/A	HE+blinding	✓	✗	✗	✓	✗	✗	✗	all data owners	v	exhaustive search
GMM	[45, KAIS'05]	✗	◐	blinding	✓	✓	✗	✗	✓	✗	✗	all data owners	h	
	[44, DCAI'19]	✗	◐	ASS	✓	✓	✗	✗	✓	✗	✗	all data owners (> 2)	v/h	
Affinity Propagation	[81, INCoS'12]	✗	◐	HE + blinding	✓	✓	✗	✓	✓	✗	✗	all data owners	v	
	[16, SECRYPT'21]	✓	◐/●	ASS+GC	✓	✓	✓	✓	✓	✗	✗	all data owners/Outsourcing	a	
Mean-shift	**[9, SAC'19]**	✓	◐	HE	✓	✓	✓	✓	✓	✗	✗	Outsourcing, 1 server	–	
DBSCAN	[72, ISI'06]	✗	◐	blinding	✓	✓	✗	✓	✗	✗	✗	all data owners	v	lack of complete protocol
	[73, ADMA'07]	✗	◐	HE+blinding	✓	✗	✗	✓	✓	✗	✗	2PC	v/h	
	[74, IJSIA'07]	✗	◐	PKC+blinding	✓	✓	✗	✓	✓	✗	✗	all data owners	v	
	[75, ITME'08]	✗	◐	HE+blinding	✓	✗	✗	✓	✓	✗	✗	data owners + 1 server	h	
	[22, TDP'13]	✗	◐	HE+blinding	✓	✗	✗	✓	✓	✗	✗	2PC	a	
	[17, S&P'12]	✓	◐/●[5]	GC	✓	✓	✓	✓	✓	✓	✗	2PC	h	
	[46, SIBCON'17]	✗	◐	HE+PKC	✓	✓	✗	✓	✓	✗	✗	all data owners	v	cluster expansion missing
	[47, PRDC'17]	✗	◐	HE	✓	✗	✗	✓	✗	✗	✗	outsourcing, all data owners + 1 server	h	
	[76, AI'18]	✗	◐	HE	✓	✗	✗	✓	✓	✗	✗	data owners + 1 server	a	uses absolute distance
	[18, ASIACCS'21]	✓	◐	ASS+GC	✓	✓	✓	✓	✓	(✓)[4]	✗	2PC/Outsourcing	a	
HC	[77, SDM'06]	✗	◐	HE+ASS+GC	✓	✓	✗	✓	✗	✓	✗	2PC	h	
	[50, TKDE'07]	✗	◐	blinding *or* SKC	✓	✓	✗	✓	✓	✗	✗	data owners + 1 server	h	SKC not semantically secure
	[49, TDP'10]	✗	◐	HE+GC	✓	✓	✗	✓	✓	✓	✗	2PC	h	
	[48, ISI'14]	✗	N/A	HE	✓	✗	✗	✓	✓	✓	✗	2PC	v	
	[78, ISCC'17]	✗	◐	HE	✓	✓	✗	✓	✗	✗	✓	2PC	v/h	
	[19, ArXiv'19]	✓	◐	HE & GC	✓	✓	✓	✓	✗	✓	✓	2PC	h	
BIRCH	[79, SDM'06]	✗	◐	HE+ASS	✓	✓	✗	✓	✗	✗	✗	2PC	v	
	[80, ADMA'07]	✗	◐	HE+ASS	✓	✓	✗	✓	✗	✗	✗	2PC	a	

[1] Of the parameters hold by the respective data owner.
[2] Assuming max. 1 party deviates from the protocol.
[3] Leaks partial information about cluster sizes.
[4] Not implemented, but possible.
[5] Can be used with any security model of GCs.

Only 4 Practical Fully Private Clustering Schemes



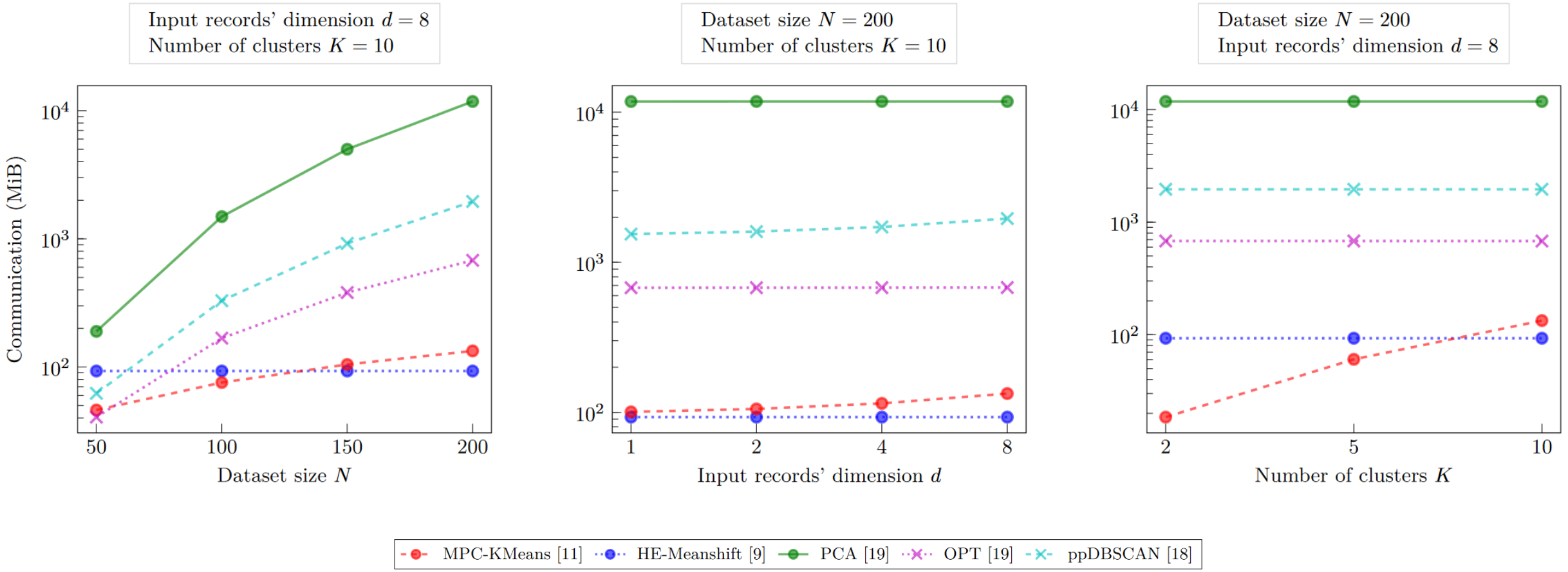
Key Takeaways:

- Most efficient solution: [MRT20]
- High latency scenarios: [CKP19]
- The best clustering quality: [BCE+21]

[1]Data records: $50 \leq N \leq 200$, dimension: $1 \leq d \leq 8$, number of clusters: $2 \leq K \leq 10$
[2]Data records: $2^{13} \leq N \leq 2^{16}$, dimension: $1 \leq d \leq 16$, number of clusters: $2 \leq K \leq 20$

Setup: 2 servers equipped with Intel Core i9-7960X, 128 GB RAM
LAN: 1 Gb/s, 1 ms RTT; WAN: 100 Mb/s, 100 ms RTT

Communication Efficiency



TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Backup – FL

PEFL Protocols

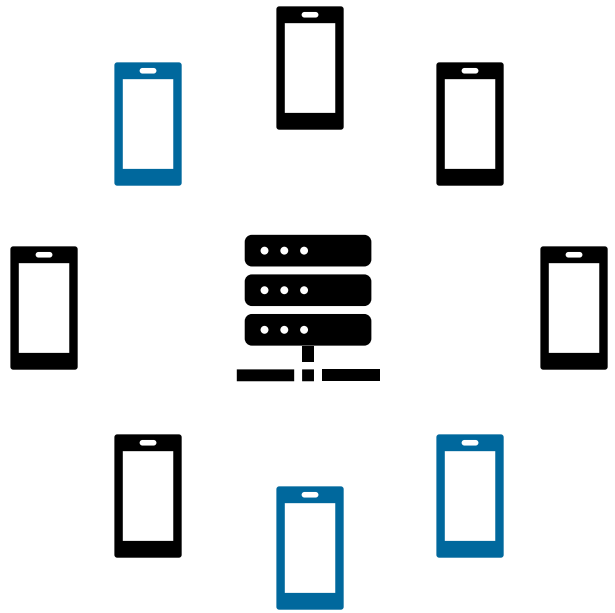
$$\vec{\mathbf{G}}_{\mathsf{m}\times\mathsf{n}} = \begin{array}{c} \\ U_1 \\ U_2 \\ \vdots \\ U_{\mathsf{m}} \end{array} \begin{array}{c} \begin{array}{ccccccc} c_1 & c_2 & \cdots & c_i & \cdots & c_{\mathsf{n}-1} & c_{\mathsf{n}} \end{array} \\ \begin{pmatrix} g_1^1 & g_1^2 & \cdots & g_1^i & \cdots & g_1^{\mathsf{n}-1} & g_1^{\mathsf{n}} \\ g_2^1 & g_2^2 & \cdots & g_2^i & \cdots & g_2^{\mathsf{n}-1} & g_2^{\mathsf{n}} \\ \vdots & \vdots & \ddots & \vdots & \iddots & \vdots & \vdots \\ g_{\mathsf{m}}^1 & g_{\mathsf{m}}^2 & \cdots & g_{\mathsf{m}}^i & \cdots & g_{\mathsf{m}}^{\mathsf{n}-1} & g_{\mathsf{m}}^{\mathsf{n}} \end{pmatrix} \end{array}$$

$$\vec{\mathbf{V}}_{\mathsf{SecMed}} = \begin{array}{c} \\ U_1 \\ \vdots \\ U_{\mathsf{m}} \end{array} \begin{array}{c} \begin{array}{ccccc} c_1 & \cdots & c_i & \cdots & c_{\mathsf{n}} \end{array} \\ \begin{pmatrix} g_1^1 + r_1 & \cdots & g_1^i + r_i & \cdots & g_1^{\mathsf{n}} + r_{\mathsf{n}} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ g_{\mathsf{m}}^1 + r_1 & \cdots & g_{\mathsf{m}}^i + r_i & \cdots & g_{\mathsf{m}}^{\mathsf{n}} + r_{\mathsf{n}} \end{pmatrix} \end{array}$$

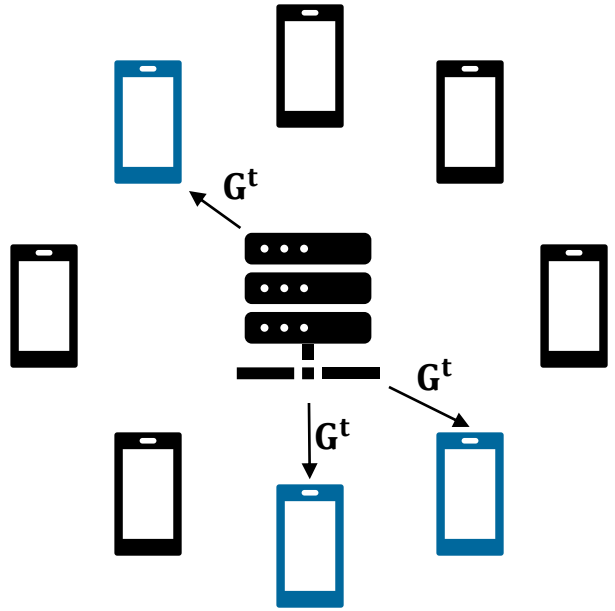
$$\vec{\mathbf{V}}_{\mathsf{SecPear}} = \begin{array}{c} \\ U_1 \\ \vdots \\ U_{\mathsf{m}} \end{array} \begin{array}{c} \begin{array}{ccccc} c_1 & \cdots & c_i & \cdots & c_{\mathsf{n}} \end{array} \\ \begin{pmatrix} g_1^1 \cdot p_1 & \cdots & g_1^i \cdot p_1 & \cdots & g_1^{\mathsf{n}} \cdot p_1 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ g_{\mathsf{m}}^1 \cdot p_{\mathsf{m}} & \cdots & g_{\mathsf{m}}^i \cdot p_{\mathsf{m}} & \cdots & g_{\mathsf{m}}^{\mathsf{n}} \cdot p_{\mathsf{m}} \end{pmatrix} \end{array}$$

$$\vec{\mathbf{V}}_{\mathsf{SecAgg}} = \begin{array}{c} \\ U_1 \\ \vdots \\ U_{\mathsf{m}} \end{array} \begin{array}{c} \begin{array}{ccccc} c_1 & \cdots & c_i & \cdots & c_{\mathsf{n}} \end{array} \\ \begin{pmatrix} g_1^1 + s_1 & \cdots & g_1^i + s_1 & \cdots & g_1^{\mathsf{n}} + s_1 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ g_{\mathsf{m}}^1 + s_{\mathsf{m}} & \cdots & g_{\mathsf{m}}^i + s_{\mathsf{m}} & \cdots & g_{\mathsf{m}}^{\mathsf{n}} + s_{\mathsf{m}} \end{pmatrix} \end{array}$$

Federated Learning [MMR+17]

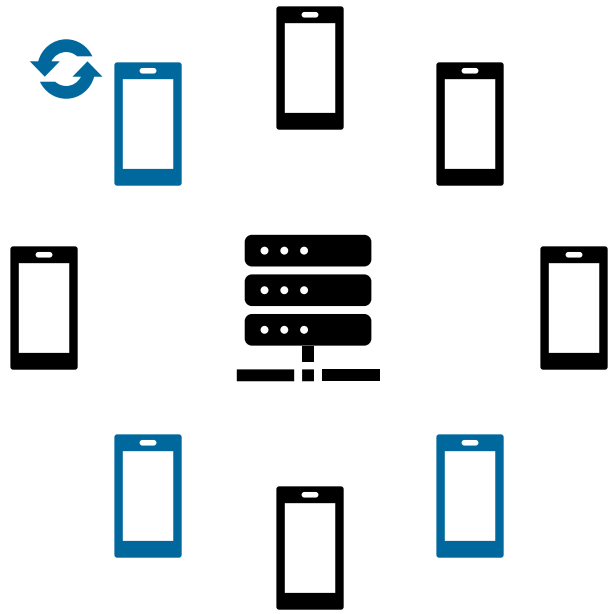


(a) Client Selection

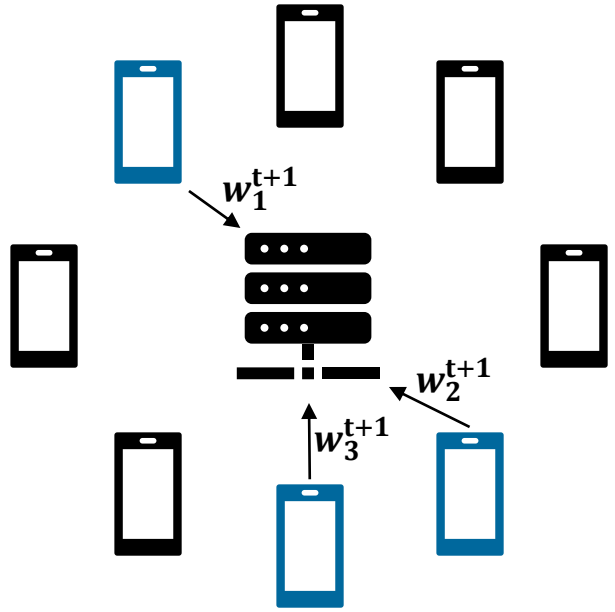


(b) Retrieval of Global Modal

Federated Learning [MMR+17]

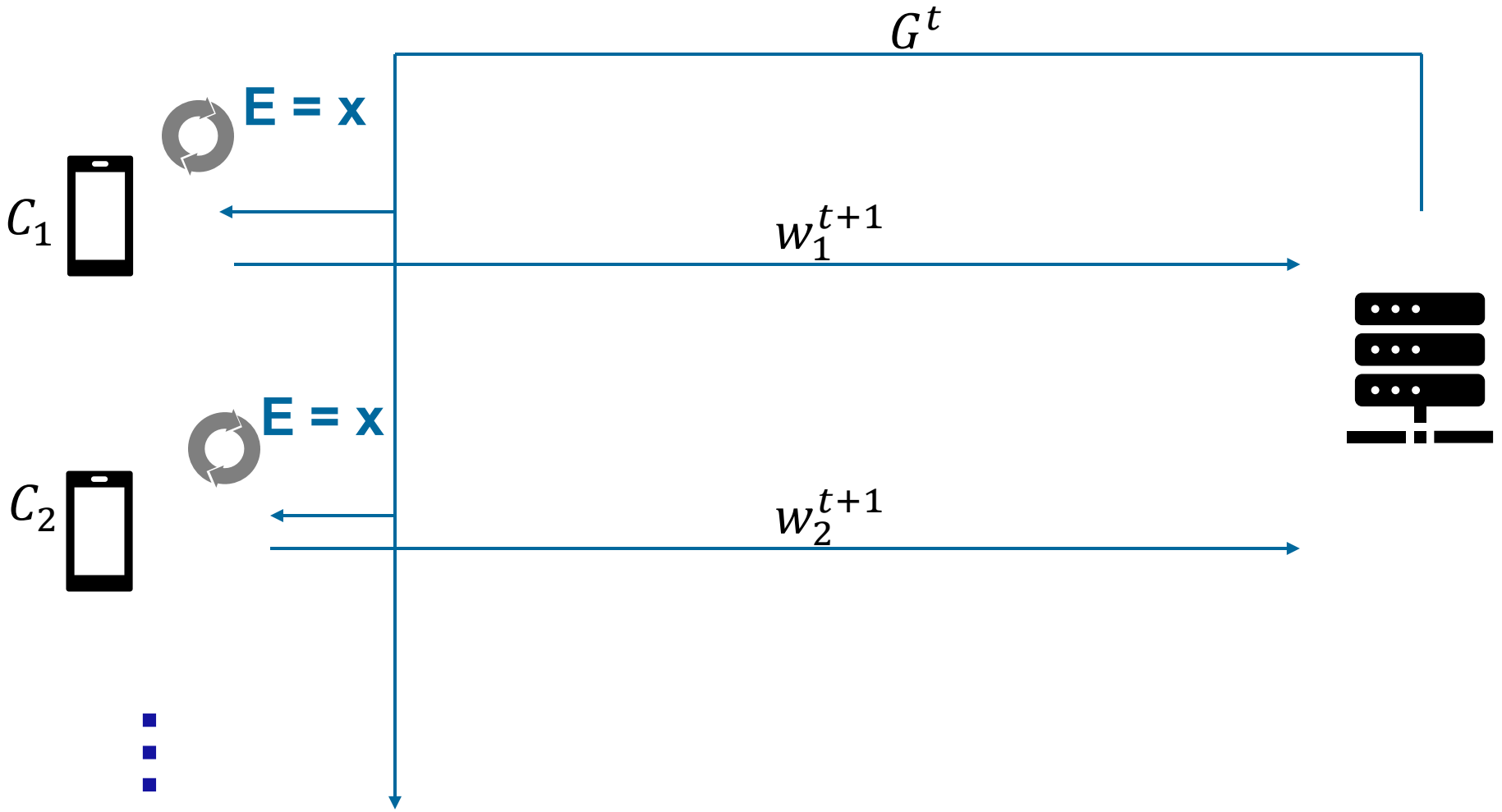


(c) Local Training



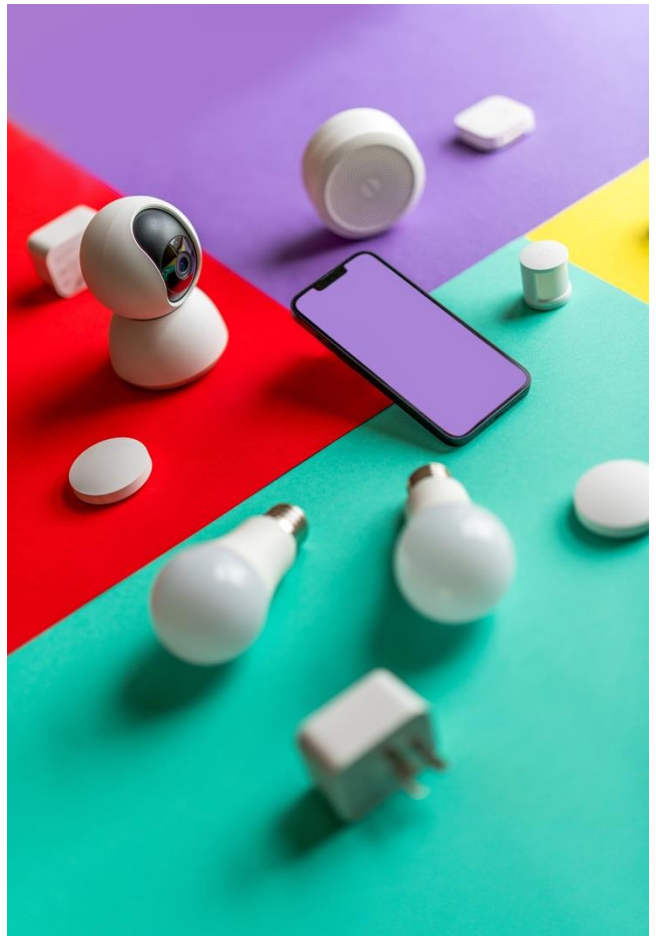
(d) Aggregation

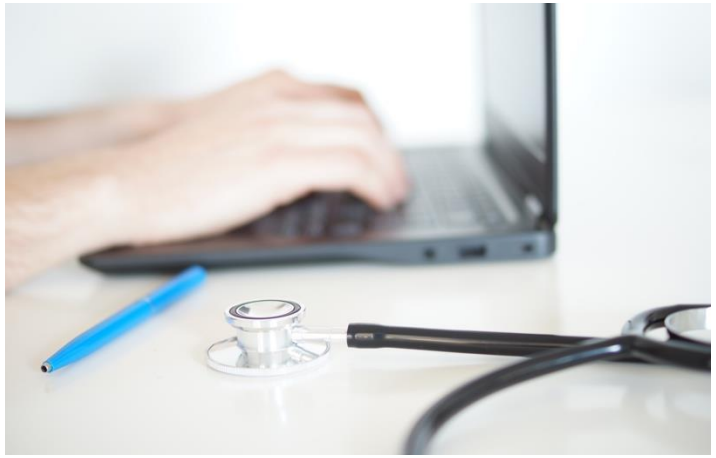
Federated Learning [MMR+17]



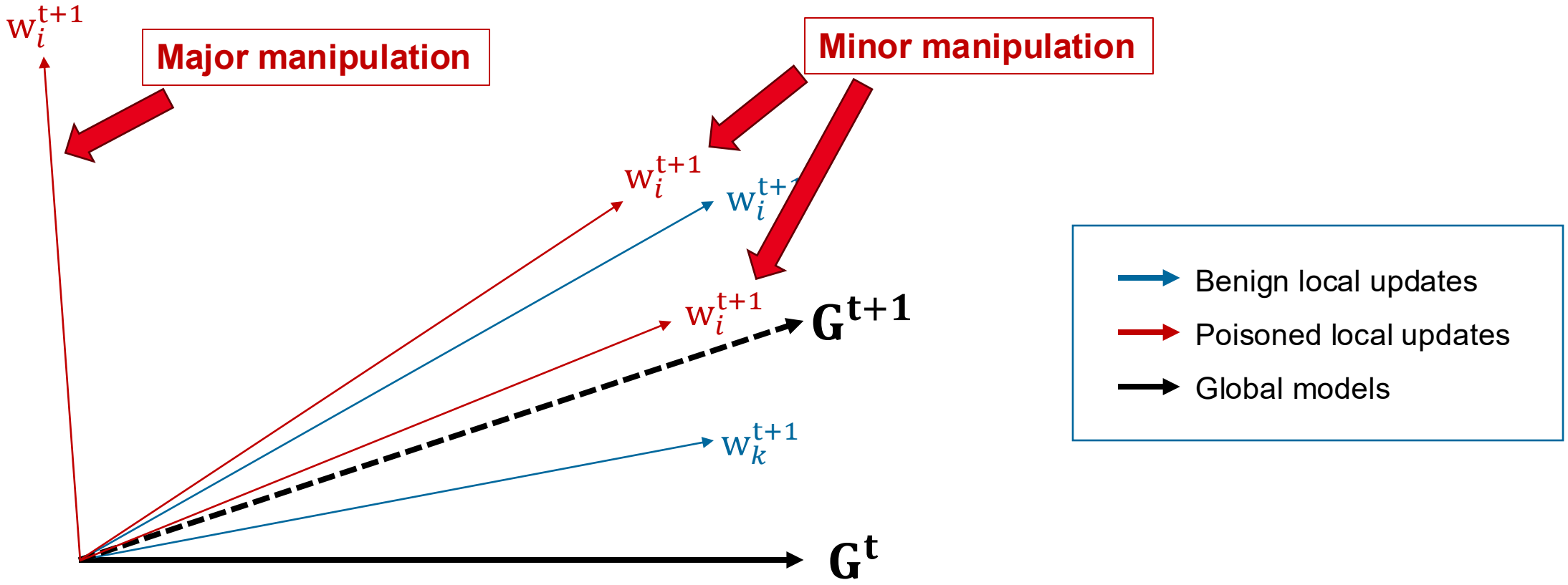
$$G^{t+1} = G^t + \eta \sum_{k=1}^{K} \frac{n_k}{n} w_k^{t+1}$$

FL Applications

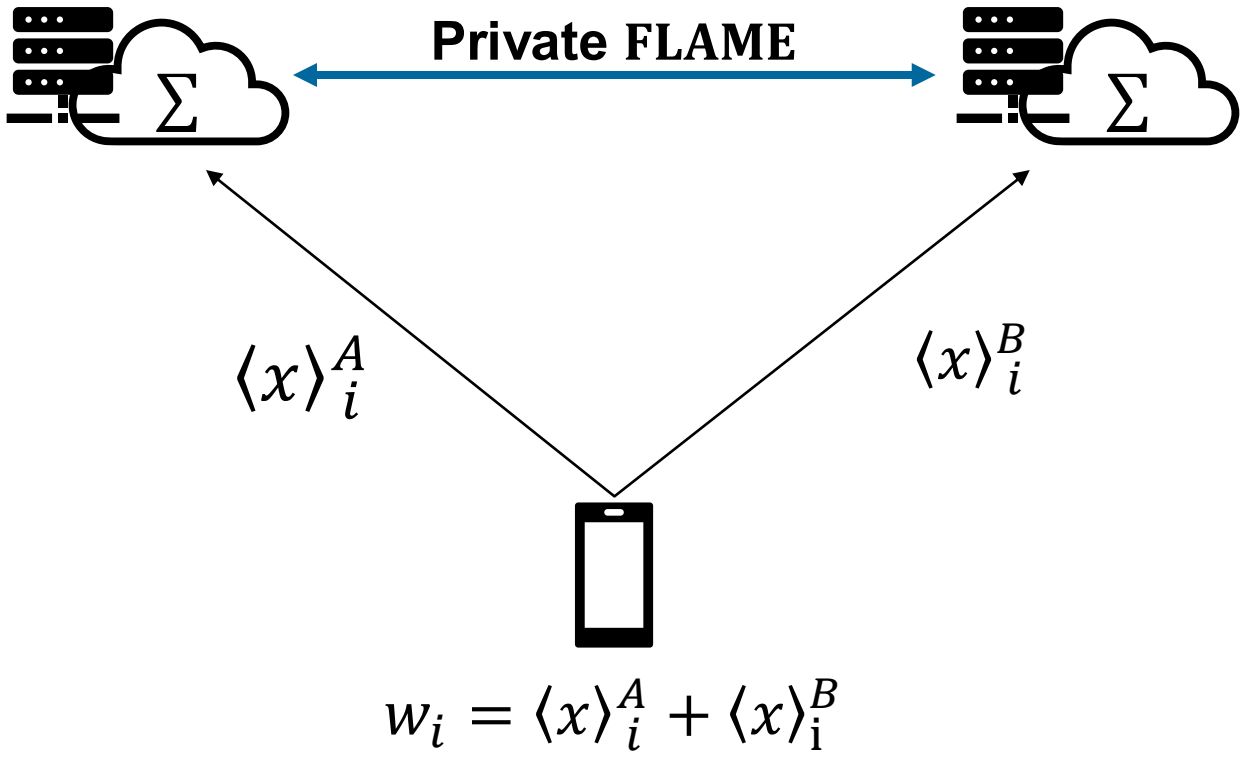




Poisoned updates disorientate the updates into an (un)targeted direction.



We realize FLAME “under encryption” to also defend inference attacks on local updates.



Adversary Model

- Semi-honest aggregators
- Full control over compromised clients
- No control over benign clients
- Majority of clients is benign

Accuracy Benchmarks

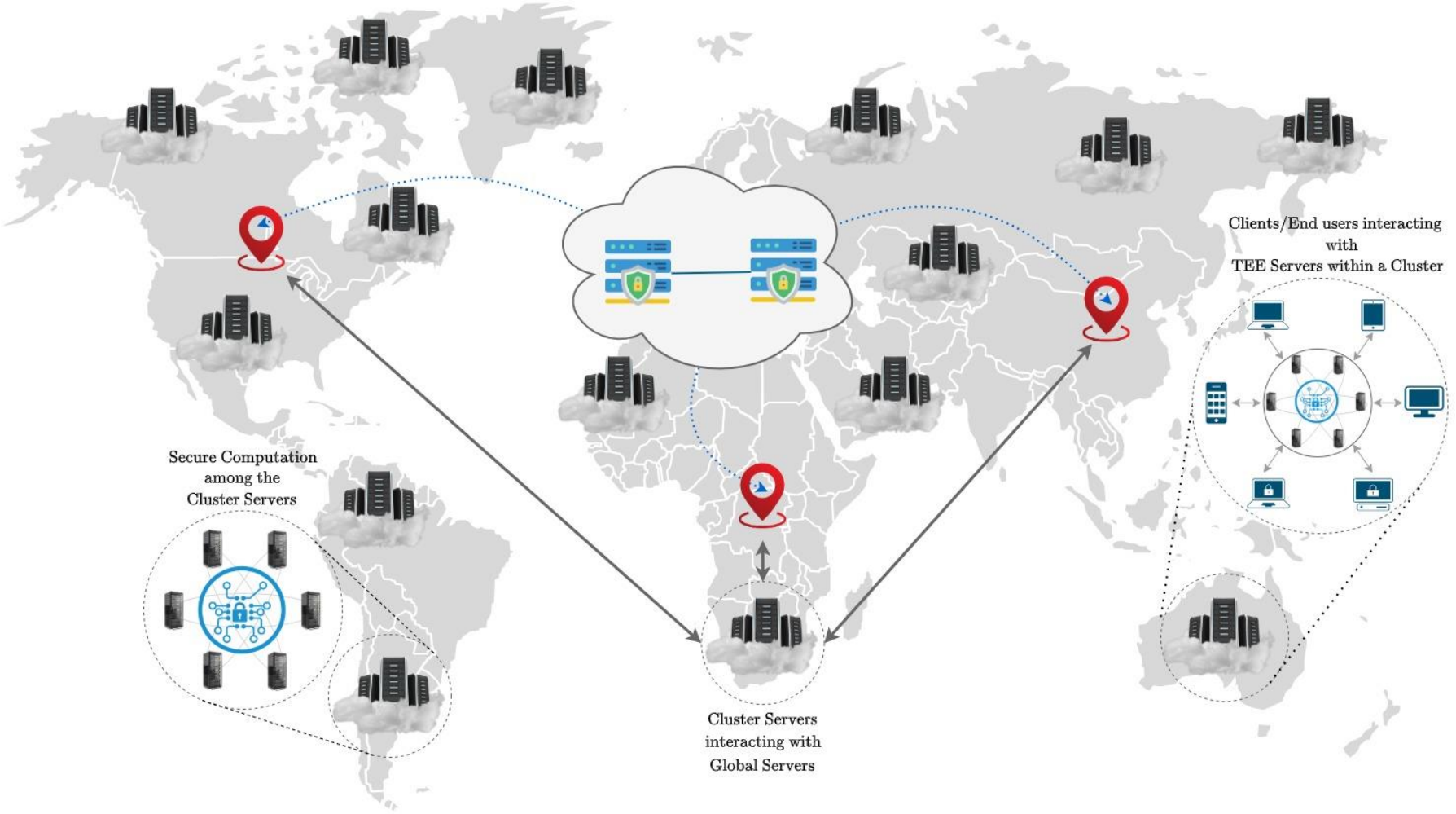
TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

	Reddit		CIFAR-10		IoT-Traffic	
	Plain	Private	Plain	Private	Plain	Private
Backdoor Accuracy	0.0	0.0	0.0	0.0	0.0	0.0
Main Task Accuracy	22.3	22.2	91.9	91.7	99.8	99.7
True Positive Rate	22.2	20.4	23.8	40.8	59.5	51.0
True Negative Rate	100.0	100.0	86.2	100.0	100.0	100.0

→ **Similar accuracy results in comparison to standard FLAME**

Our Worldwide Solution



TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Backup – PFE

Universal Circuit design VS Circuit Synthesis

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

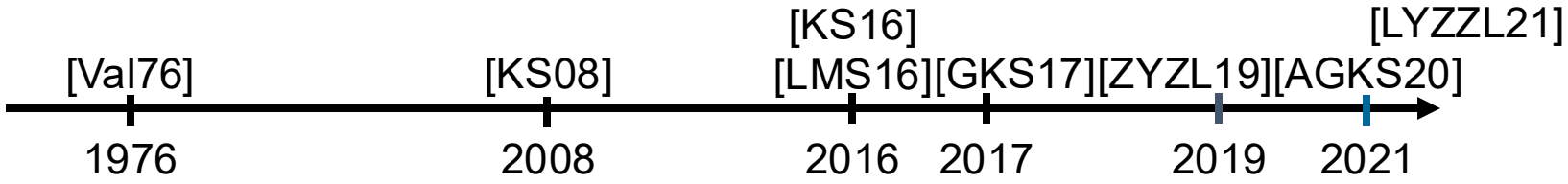
Universal Circuit Design

- Reduce prefactors of UC size
  $5.0n \log n$ [Val76]
  ↓
  $3.0n \log n$ [LYZ+21] ($2.95n \log n$ lower bound)
- Evaluate ρ-input LUTs [Val76, SS08]

Circuit Synthesis

- Evaluated circuit consists of 2-input, 1-output gates
- MPC-optimized circuits
  - Consisting of only AND and XOR gates [KS16, GKS17, AGKS20]
  - UCs can evaluate all $16 = 2^{2^2}$ possible gate types

Existing UC Constructions



	[Val76] 2-way	[Val76] 4-way	[KS08]	[GKS17] Hybrid(2, 4)	[LYZZL21] 2-way
Size	$5n \log n$	~~$4.75n \log n$~~ $4.5n \log n$	$0.75n \log^2 n + 2.25n \log n$	~~$4.75n \log n$~~ $4.5n \log n$	$3n \log n$
Code	✔	✔	✔	✔	✖

Lower bound:
$2.95n \log n$

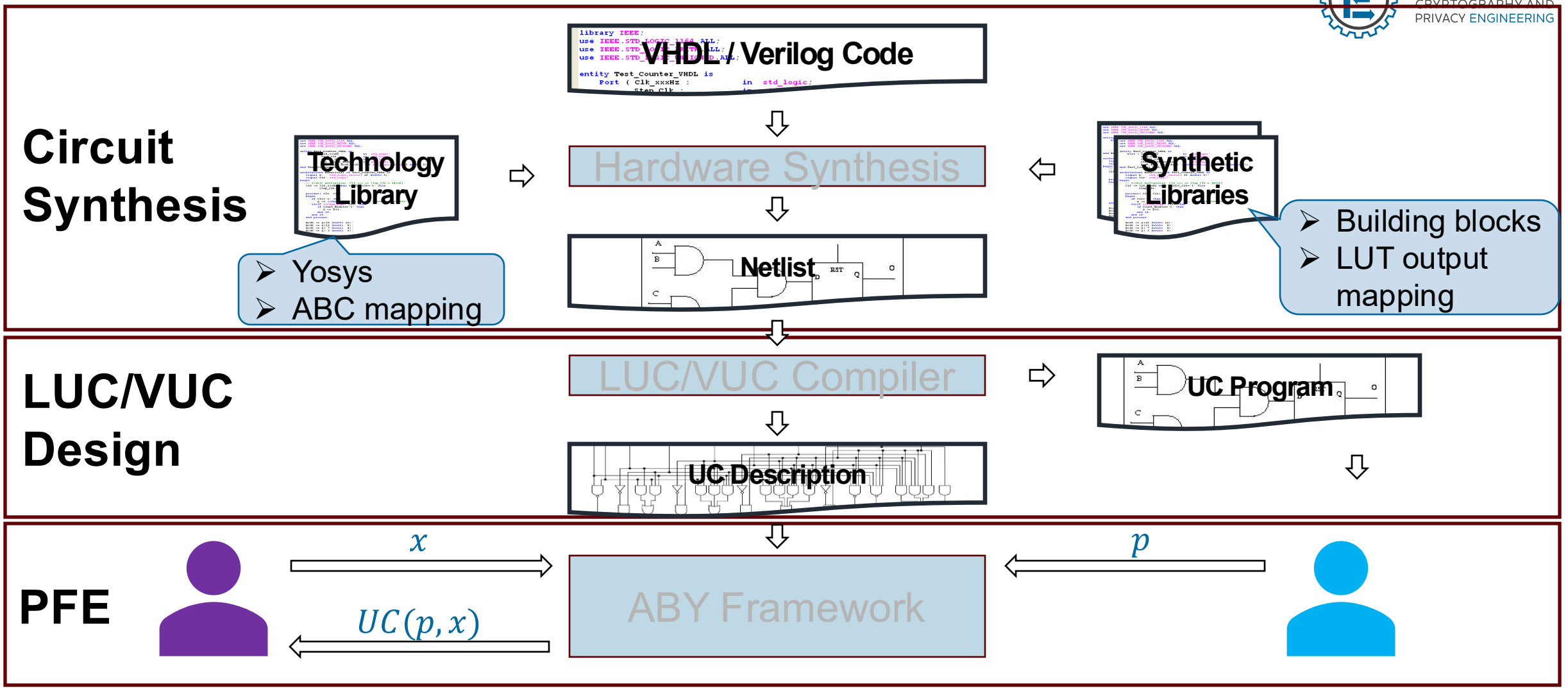
Building Block: LUC and UC Sizes

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Building Block	Boolean Circuit		LUT-Based Circuit		Improvement
	# Gates	UC Size	LUT Dimension	LUC Size	
Full Adder	4 XOR / 1 AND	$15b \log 5b$	$(3 \rightarrow 2)$-LUT	$9b \log b$	**1.67**×
Comperator	3 XOR / 1 AND	$12b \log 4b$	$(3 \rightarrow 1)$-LUT	$4.5b \log b$	**2.67**×
Multiplexer	2 XOR / 1 AND	$9b \log 3b$	$(3 \rightarrow 1)$-LUT	$4.5b \log b$	**2.00**×

Synthesis Toolchain



LUC and VUC Sizes

TECHNISCHE UNIVERSITÄT DARMSTADT

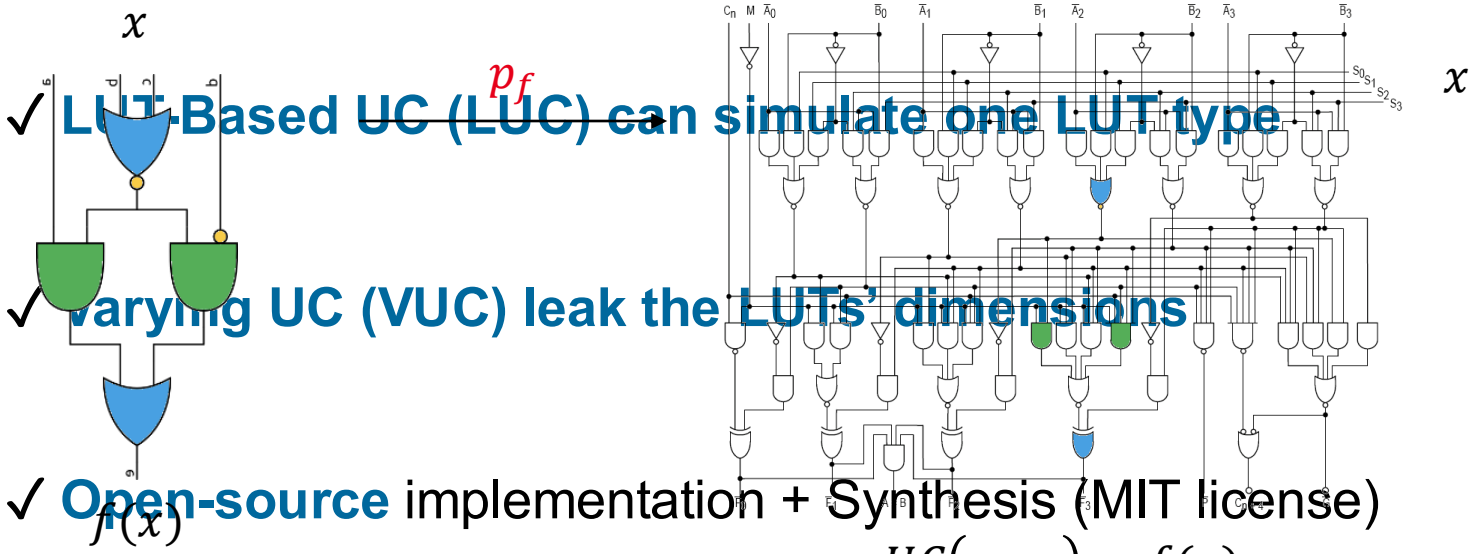
ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Circuit	UC Size	LUC Size	VUC Size	Improvement LUC / UC	Improvement VUC / LUC	LUT Dimension
AES	1,779,105	1,779,105	1,584,047	1.00×	1.13×	$(2 \to 1)$-LUT
DES	1,269,537	1,130,037	960,584	1.12×	1.17×	$(3 \to 1)$-LUT
SHA-256	10,652,234	5,351,972	4,591,982	1.99×	1.17×	$(3 \to 1)$-LUT
ADD-64	17,006	8,963	8,963	1.90×	1.00×	$(3 \to 2)$-LUT
Karatsuba	286,933	156,888	112,829	1.83×	**1.40**×	$(3 \to 3)$-LUT
Manhattan	327,203	150,046	112,829	**2.18**×	1.33×	$(3 \to 2)$-LUT
FP-ADD	113,620	90,964	90,964	1.25×	1.00×	$(3 \to 1)$-LUT
FP-MUL	293,125	247,859	185,968	1.18×	1.33×	$(3 \to 1)$-LUT
FP-DIV	372,101	236,300	181,904	1.57×	1.30×	$(3 \to 1)$-LUT
FP-SQRT	176,176	118,873	89,311	1.48×	1.33×	$(3 \to 1)$-LUT

Our Contributions (ASIACRYPT'23)

✗ Combing Circuit Synthesis and UC Design to **minimize the UC size** by evaluating **ρ-input, ω-output LUTs**!

A **Universal Circuit** (UC) is a Boolean circuit of asymptotic size $\Theta(n \log n)$ that can compute any Boolean function f of size n.

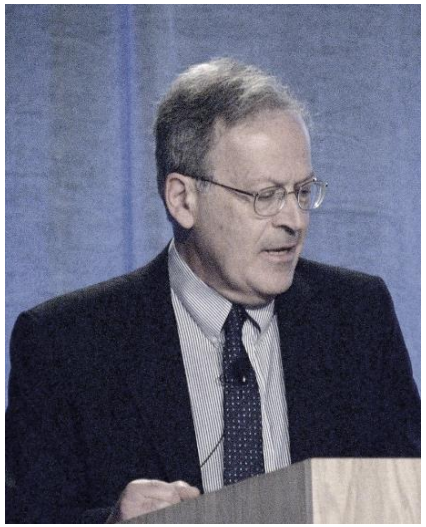


✓ **LUT-Based UC (LUC) can simulate one LUT type**

✓ **Varying UC (VUC) leak the LUTs' dimensions**

✓ **Open-source** implementation + Synthesis (MIT license)

$$UC(p_f, x) = f(x)$$



Leslie G. Valiant
1976

Reduce PFE to MPC by using a UC as public function.

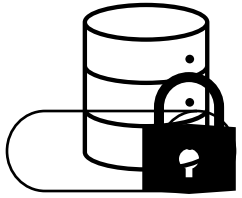
[DGS+23] Y. Disser, D. Günther, T. Schneider, M. Stillger, A. Wigandt, and **H. Yalame**. Breaking the Size Barrier: Universal Circuits Meet Lookup Tables. In ASIACRYPT, 2023. CORE rank A.

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Backup - VASA

Some Use Cases of Parallel AES

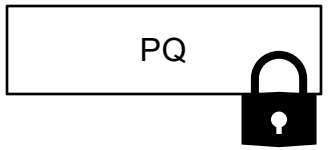


Disk Encryption / Transmission Encryption [DGK19]

Trivial parallelism

Solve once

Difficulty?

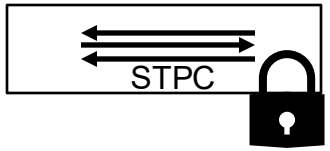


Post-Quantum Signatures [DG19a, DG19b, DGK21]

Accelerate PRFs

and PRGs

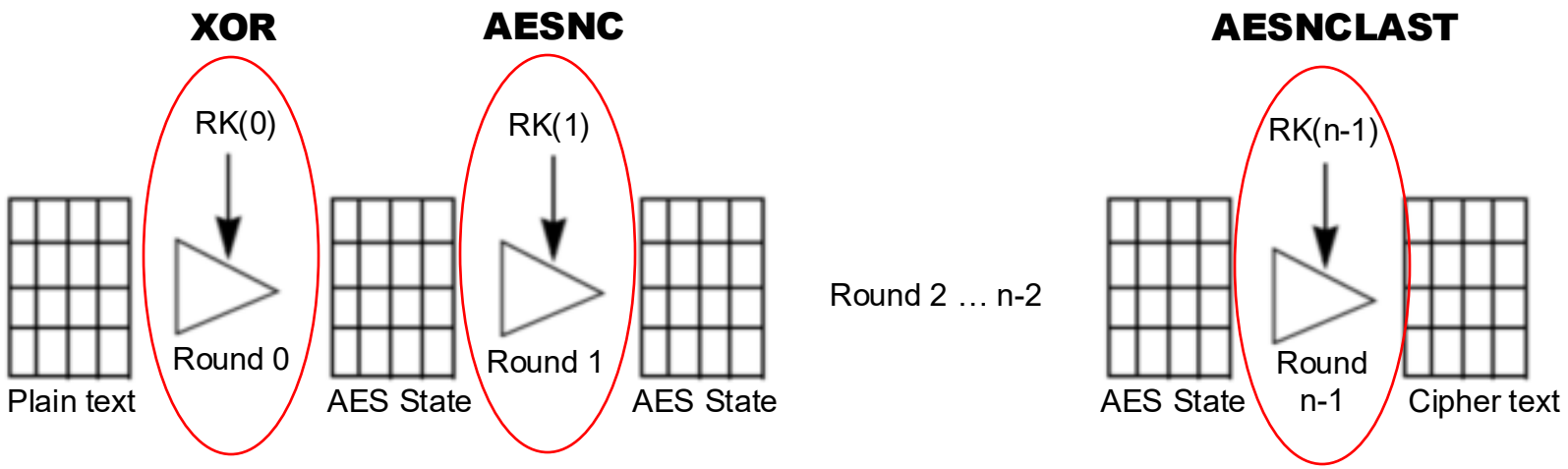
VASA:



Secure Two Party Computation

Complex data dependencies from circuits

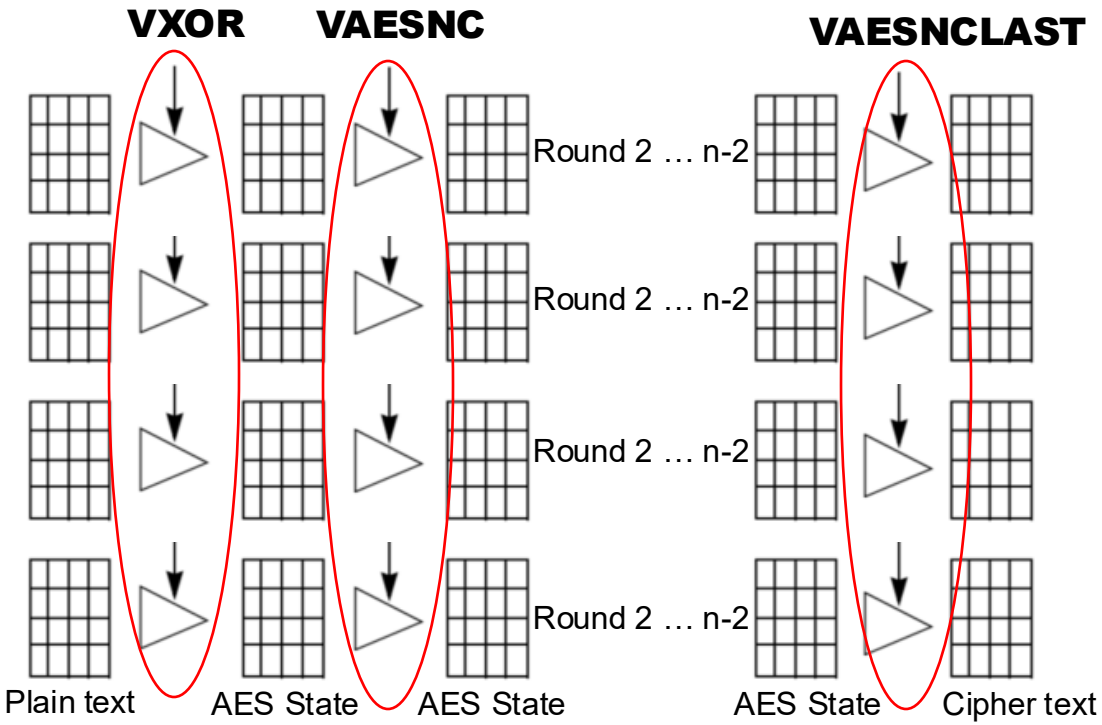
AES



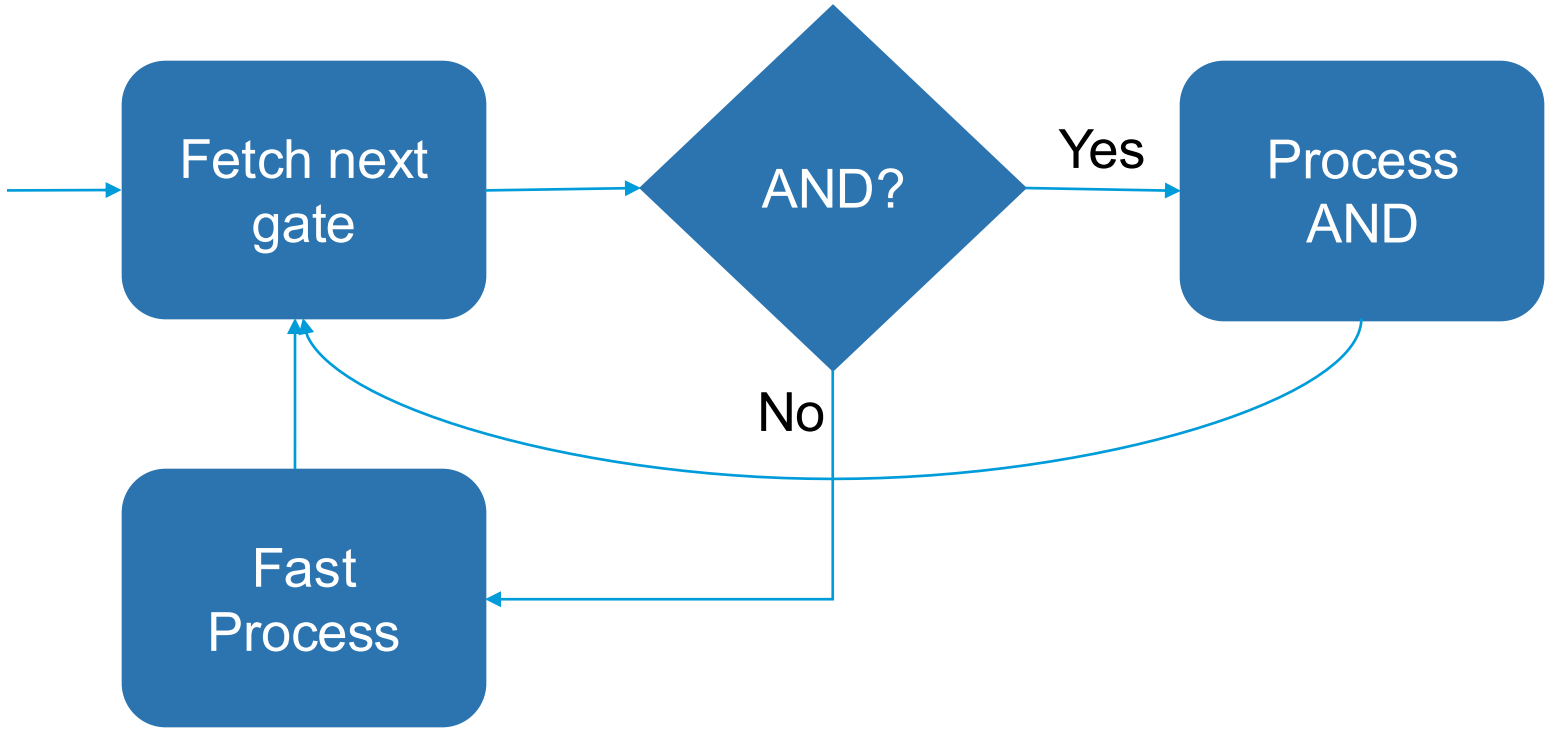
AES-128: n=10
AES-192: n=12
AES-256: n=14

Vectorized AES (VAES)

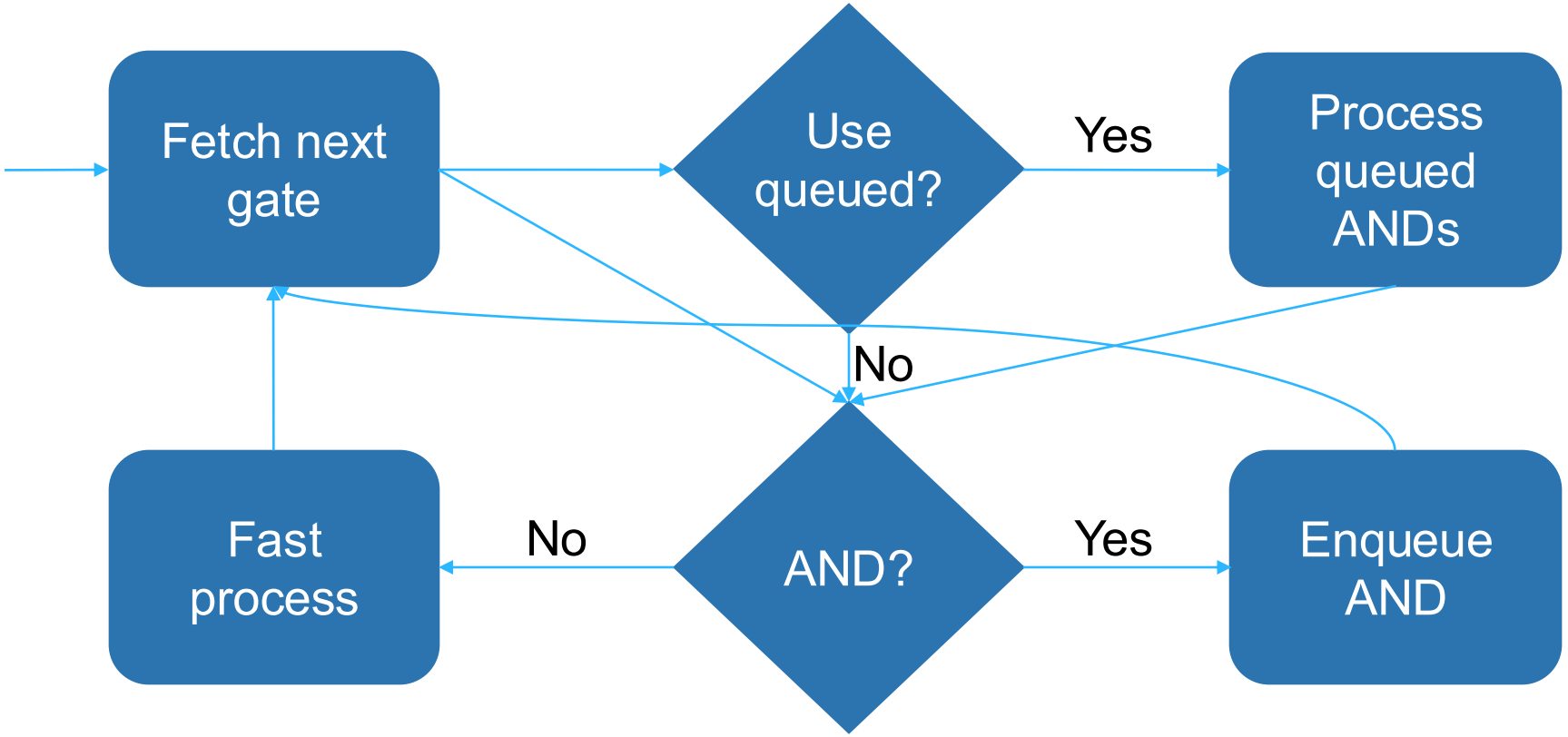
- Importance of batching data and microarchitectural properties [DGK19]
  - Block ciphers: AES-CTR, AES-CBC, AES-GCM, and AES-GCM-SI.
    - Up to 4×performance improvements



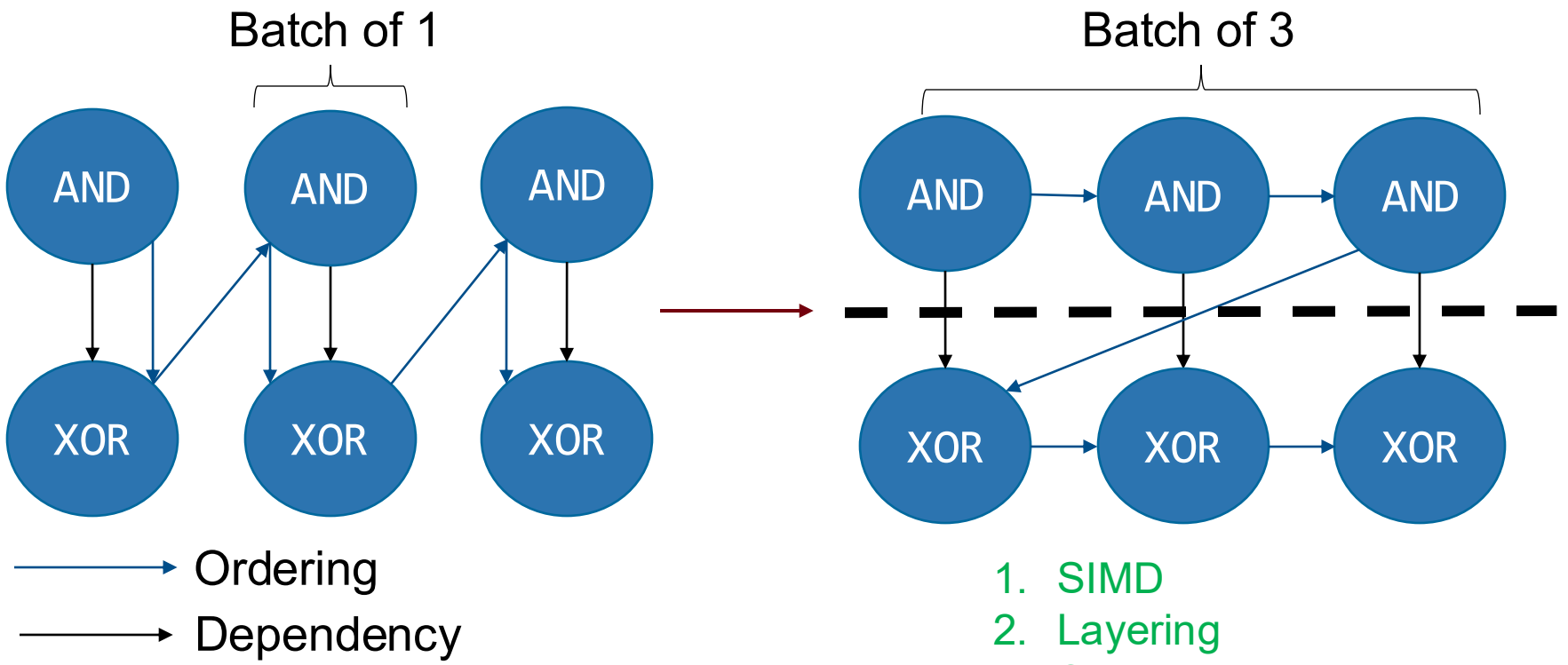
Parallelization - Baseline Scenario



Parallelization - Dynamic Batching

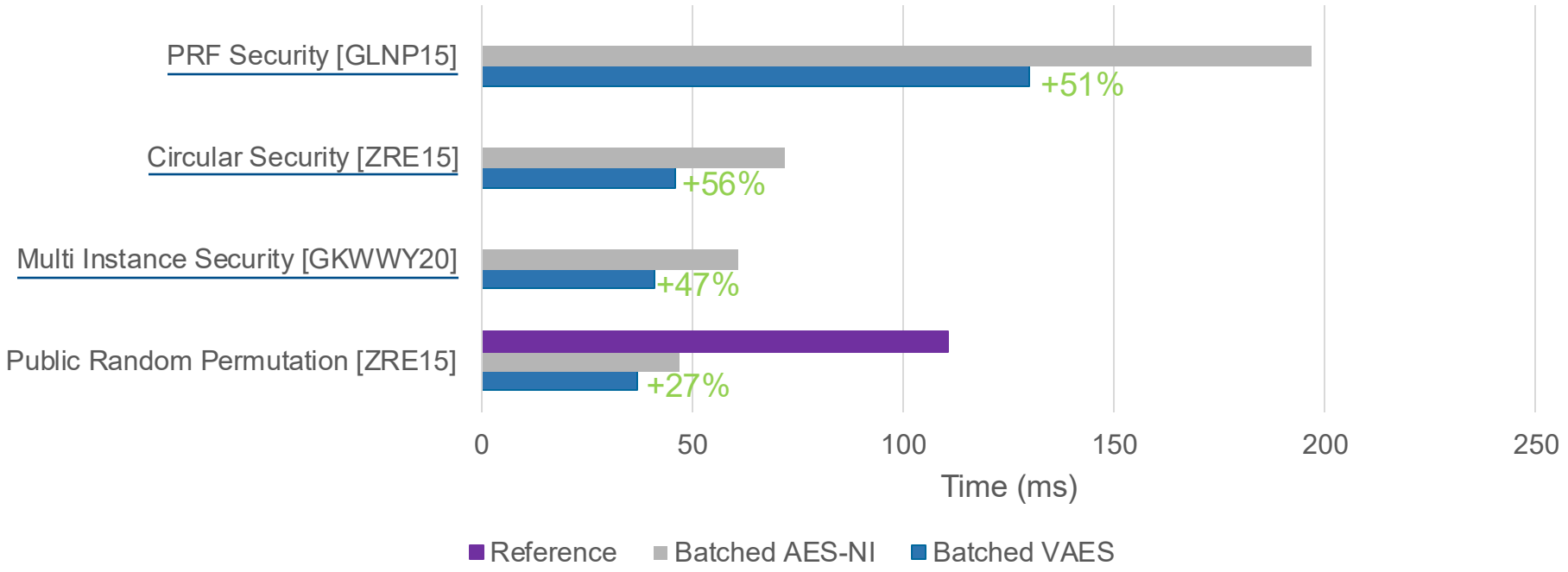


Parallelization - Static Batching



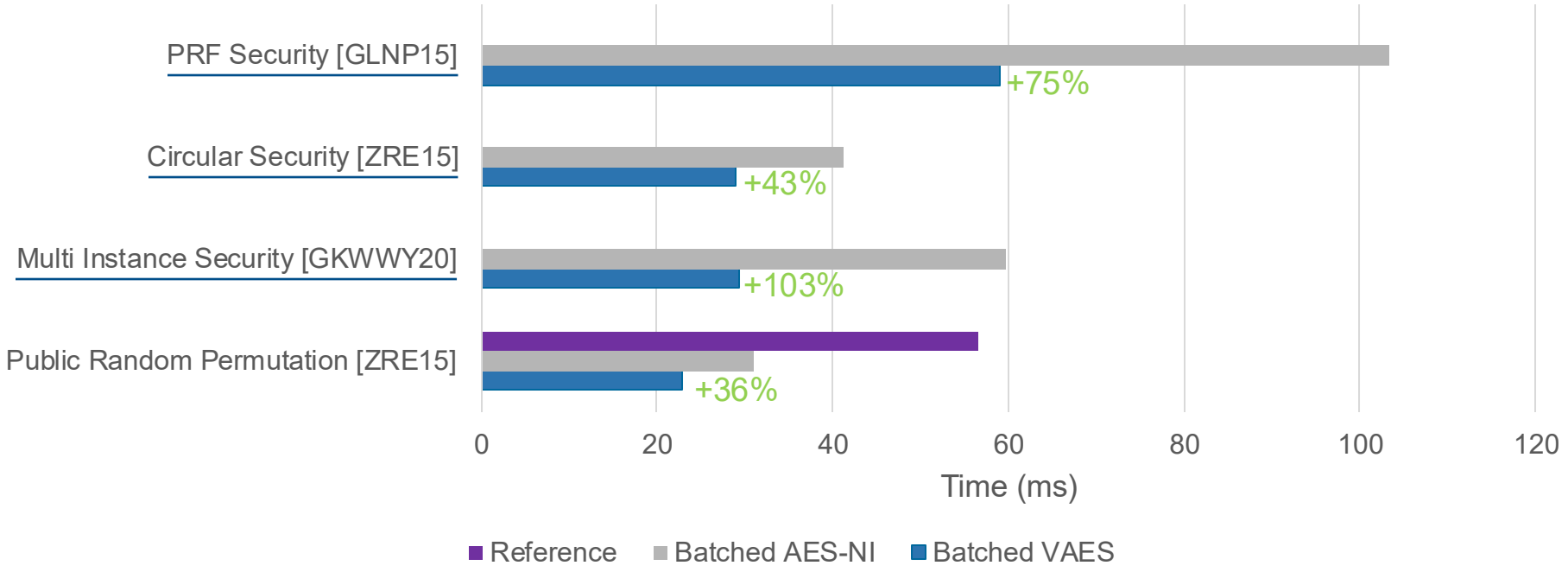
1. SIMD
2. Layering
3. Smart Arrangement

Improvement – Yao Garbling in ABY [DSZ15]



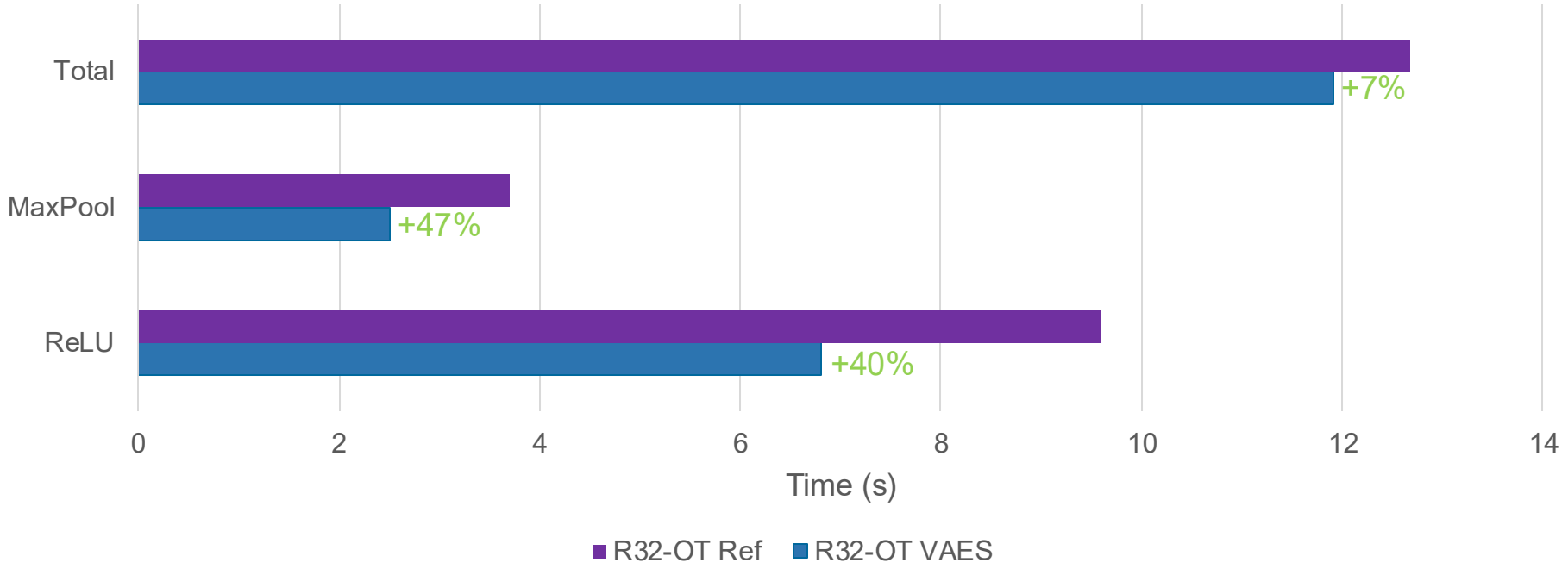
Average runtimes for applications AES, SHA-1, SCS-PSI, and Phasing-PSI.

Improvement - Yao Evaluation in ABY [DSZ15]



Average runtimes for applications AES, SHA-1, SCS-PSI, and Phasing-PSI.

Benchmarking – PPML in CrypTFlow2



Geometric mean of run-times using the SqueezeNetImgNet, SqueezeNetCIFAR, ResNet50, and DenseNet121 networks.

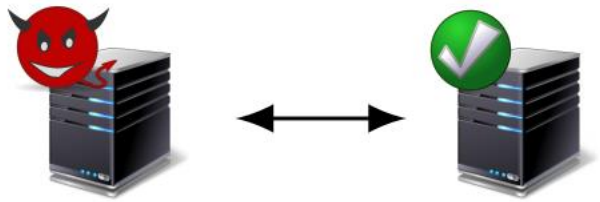
TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

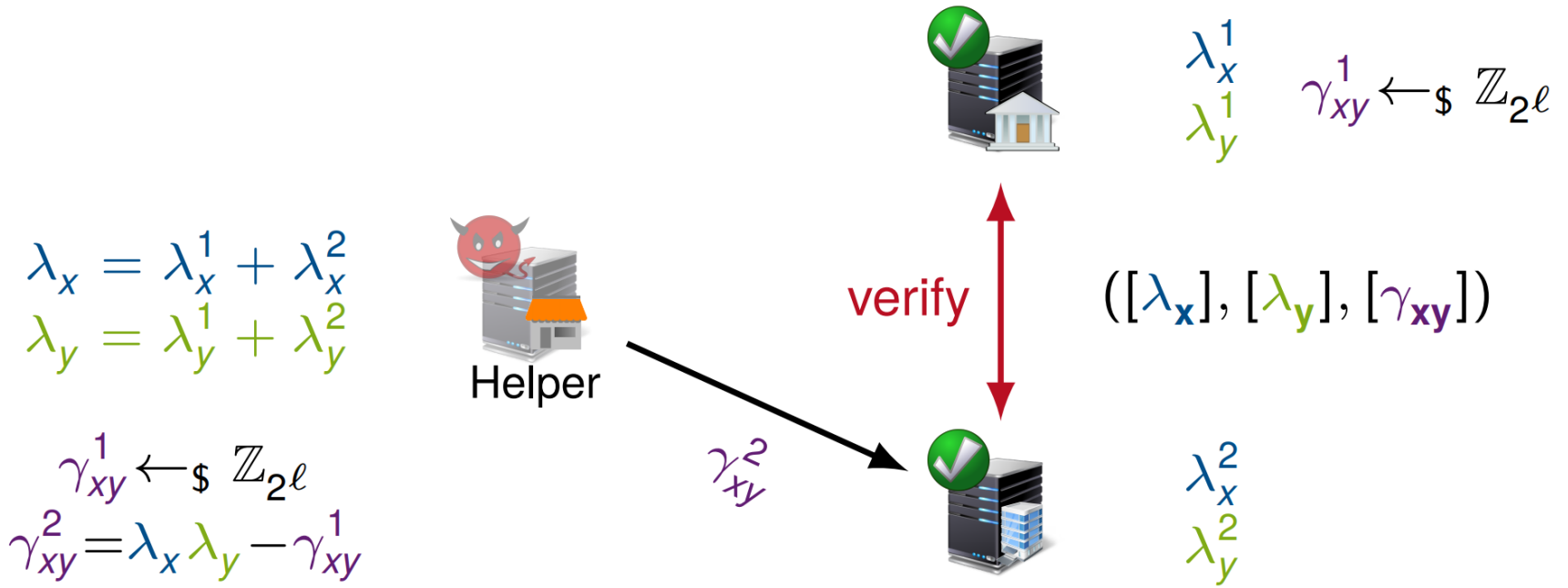
Backup - DETI

Prior Works

- Asymmetric 2PC ⇒ dishonest majority
  - Yao's garbled circuits [Yao86]
  - Secure inference with a malicious client [LMS+21; CGO+22]
  - Secure inference with a malicious server [DWL+23]



From ASTRA to AUXILIATOR



- Semi-honest parties verify correctness
- Helper provides additional triples or proof

Our Contributions (IEEE S&P'24)

Semi-honest security model: **Not sufficient**

Malicious security model: **Too inefficient**

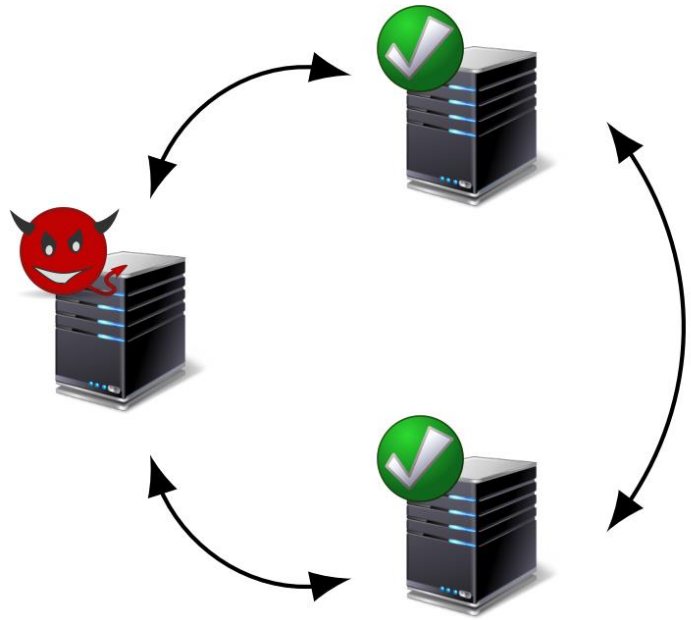
Trust in different people or institutions is commonly asymmetric

✓ Mixed model: **Auxiliator & Socium**

- ✓ **asymmetric 3PC**
- ✓ **one known** malicious party: honest majority
- ✓ multiple options for **efficient preprocessing**

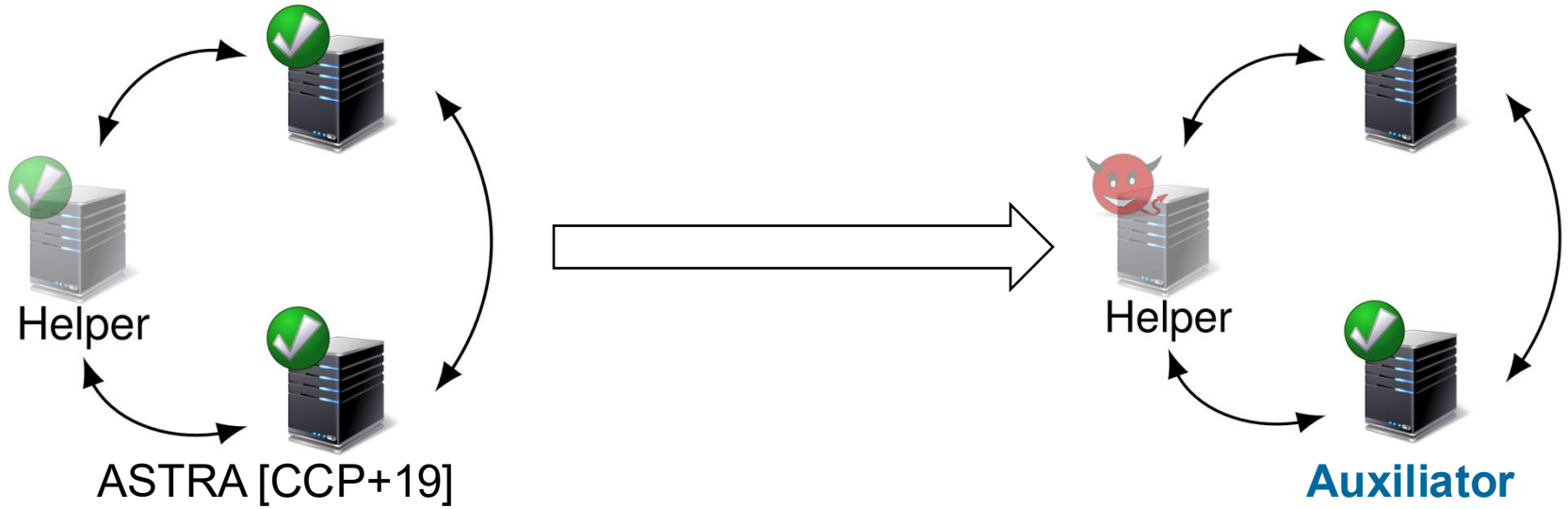
✓ **ML-friendly**, but multi-purpose design

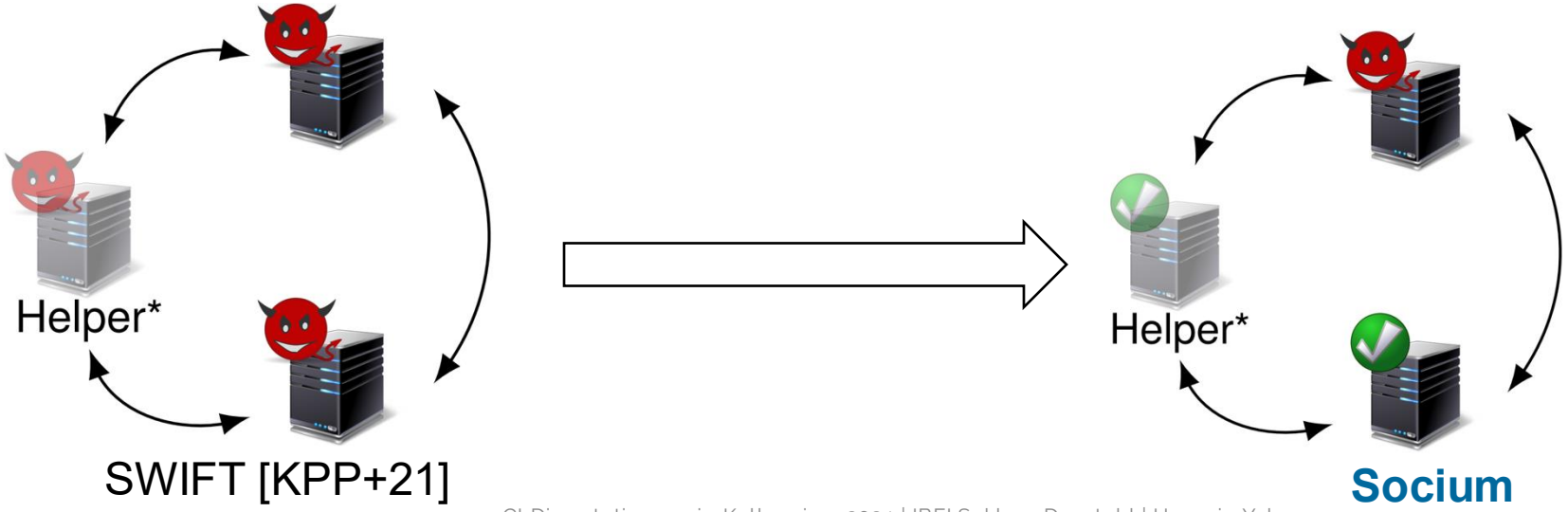
✓ **Open-source** implementation (MIT license)



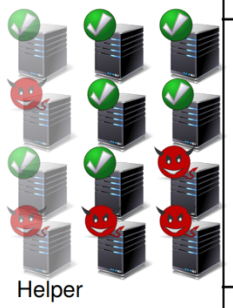
[BSS+24] A. Brüggemann, O. Schick, T. Schneider, A. Suresh, and **H. Yalame**. Don't Eject the Impostor: Fast Three-Party Computation with A Known Cheater. In IEEE S&P, 2024. CORE rank A*.

Bridging the Gap Between Semi-Honest and Malicious Model



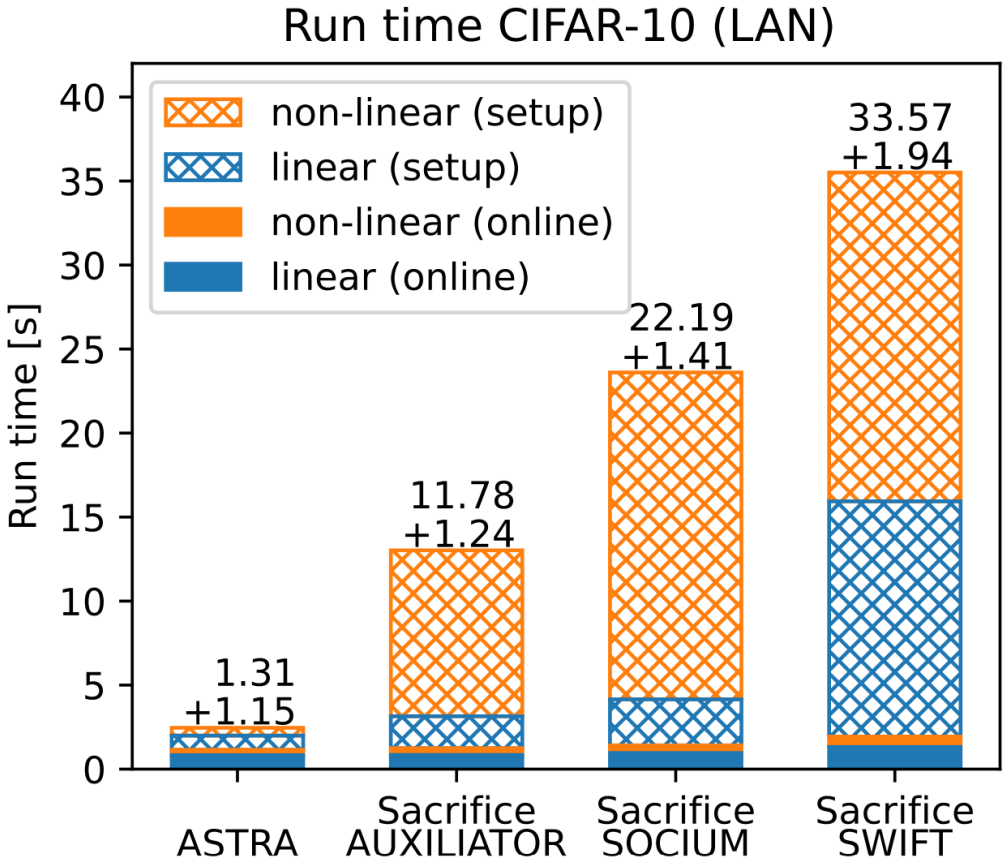


ASTRA => AUXILIATOR
SWIFT => SOCIUM



ℓ: ring size σ: statistical security parameter

Communication per Multiplication		
Verification	Sacrifice	DZKP
Preprocessing		
ASTRA [CCP+19]	$1 \times \mathbb{Z}_\ell$	
AUXILIATOR	$4 \times \mathbb{Z}_{\ell+\sigma}$	$1 \times \mathbb{Z}_\ell$
SOCIUM	$5 \times \mathbb{Z}_{\ell+\sigma}$	$2 \times \mathbb{Z}_\ell$
SWIFT [KPP+21]	$9 \times \mathbb{Z}_{\ell+\sigma}$	$3 \times \mathbb{Z}_\ell$
Online		
ASTRA/AUXILIATOR	$2 \times \mathbb{Z}_\ell$	
SWIFT/SOCIUM	$3 \times \mathbb{Z}_\ell$	



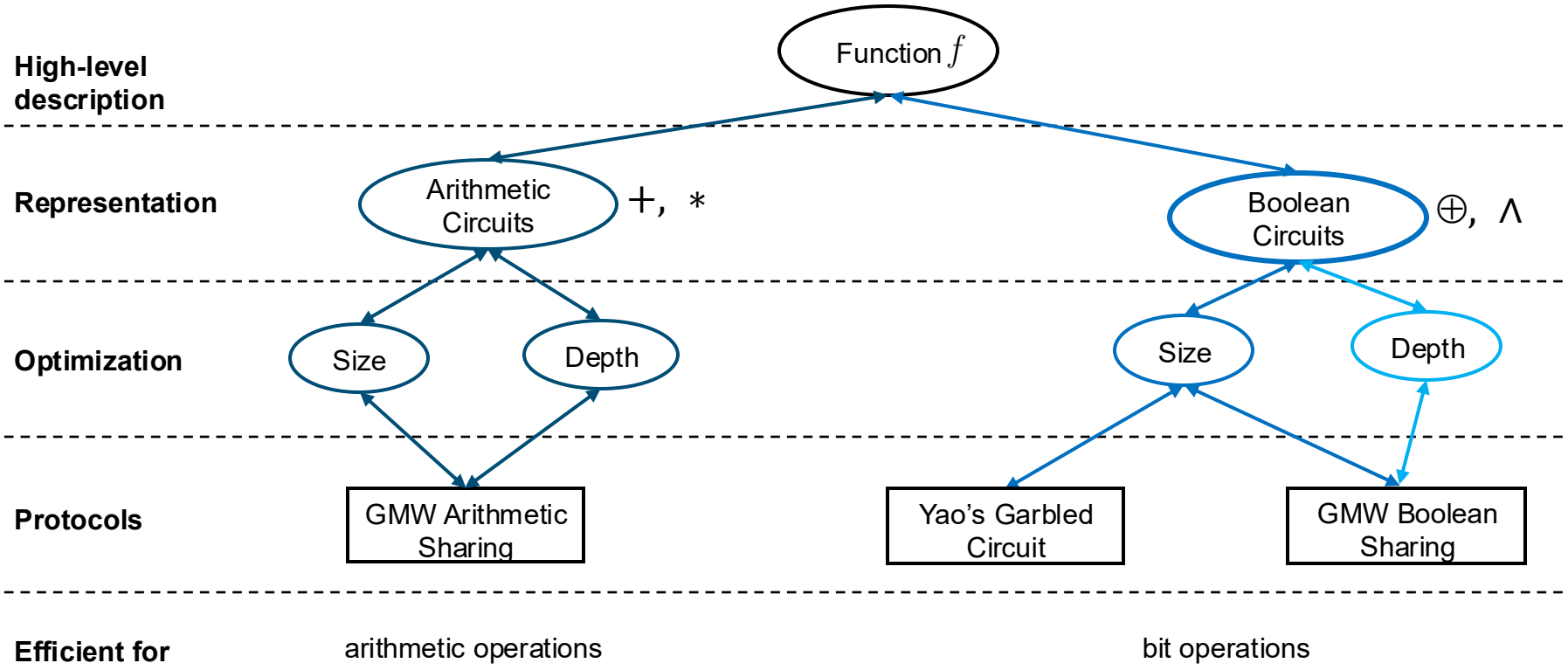
using the 7-layer CNN from MiniONN [LJL+17] trained on the CIFAR-10 dataset

TECHNISCHE UNIVERSITÄT DARMSTADT

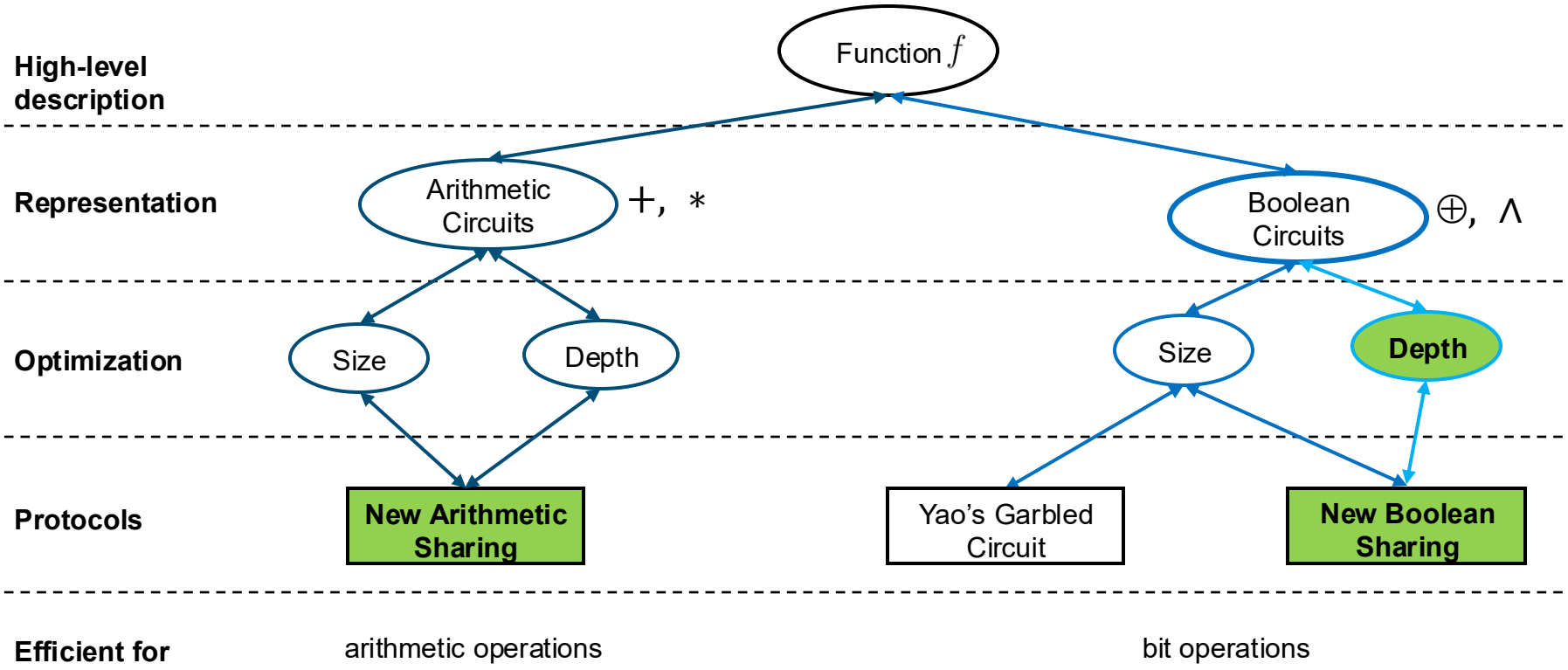
ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Backup – ABY2.0 & FLUTE

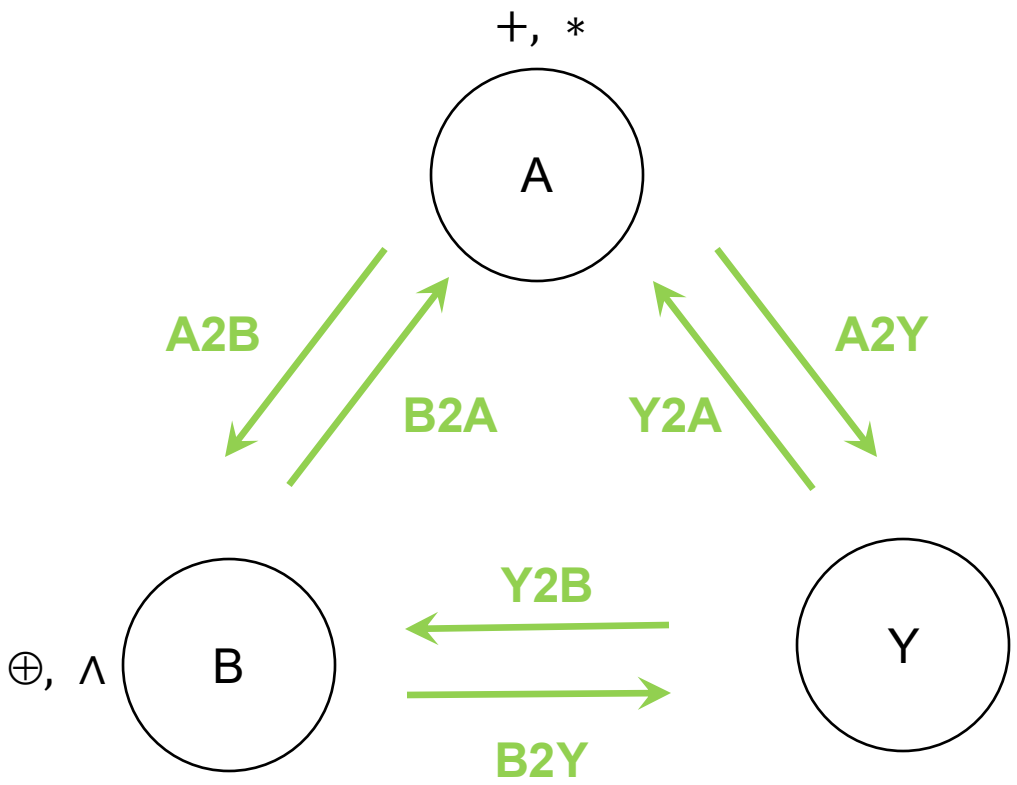
2PC in ABY


High-level description
Function f
Representation
Arithmetic Circuits
$+$, $*$
Boolean Circuits
$\oplus$, $\wedge$
Optimization
Size
Depth
Size
Depth
Protocols
GMW Arithmetic Sharing
Yao's Garbled Circuit
GMW Boolean Sharing
Efficient for
arithmetic operations
bit operations

2PC in ABY2.0


High-level description
Function f
Representation
Arithmetic Circuits
$+$, $*$
Boolean Circuits
$\oplus$, $\wedge$
Optimization
Size
Depth
Size
Depth
Protocols
New Arithmetic Sharing
Yao's Garbled Circuit
New Boolean Sharing
Efficient for
arithmetic operations
bit operations

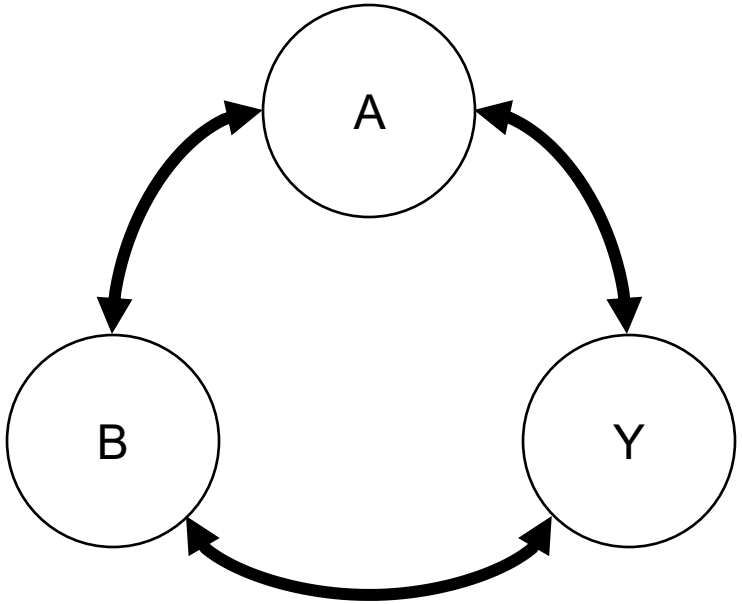
ABY2.0: New Mixed World Conversions



SOTA => ABY2.0 Improvements

κ: computational security parameter
ℓ: bitlength of numbers

Conversion	Setup Communication [bits]	Online Communication [bits]	Online Rounds
Y2B	$0 \Rightarrow \ell$	$0 \Rightarrow \ell$	$0 \Rightarrow 1$
B2Y	$2\ell\kappa \Rightarrow 2\ell\kappa$	$\ell\kappa + \ell \Rightarrow \ell\kappa$	$2 \Rightarrow 1$
A2Y	$4\ell\kappa \Rightarrow 4\ell\kappa$	$2\ell\kappa + \ell \Rightarrow \ell\kappa$	$2 \Rightarrow 1$
Y2A	$2\ell\kappa \Rightarrow 3\ell\kappa + 2\ell$	$(\ell^2 + 3\ell)/2 \Rightarrow \ell$	$2 \Rightarrow 1$
A2B	$4\ell\kappa \Rightarrow 4\ell\kappa + \ell$	$2\ell\kappa + \ell \Rightarrow \ell\kappa + \ell$	$2 \Rightarrow 2$
B2A	$\ell\kappa \Rightarrow \ell\kappa + \ell^2$	$(\ell^2 + \ell)/2 \Rightarrow 2\ell$	$2 \Rightarrow 1$



ABY2.0: LR Inference

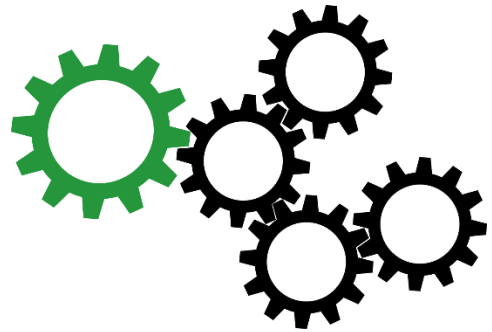
	Runtime (ms)	
	LAN	WAN
SecureML [MZ17]	1.69	504.96
ABY2.0	**0.29**	**308.16**
Improvement	**5.6x**	**1.6x**
	Throughput (queries/min)	
	LAN	WAN
SecureML [MZ17]	1193	3.58
ABY2.0	**42371**	**39.88**
Improvement	**35.5x**	**11.1x**

Over Gisette dataset with 5000 features and up to 1,000,000 samples

How to Use Lookup Tables

- **Manual** utilization of LUTs during circuit design, e.g., SecFloat [RBS+22], SiRnn [RRG+21]

- **Automatic** replacement sub-circuits of existing circuits by LUTs, e.g., [DKS+17]

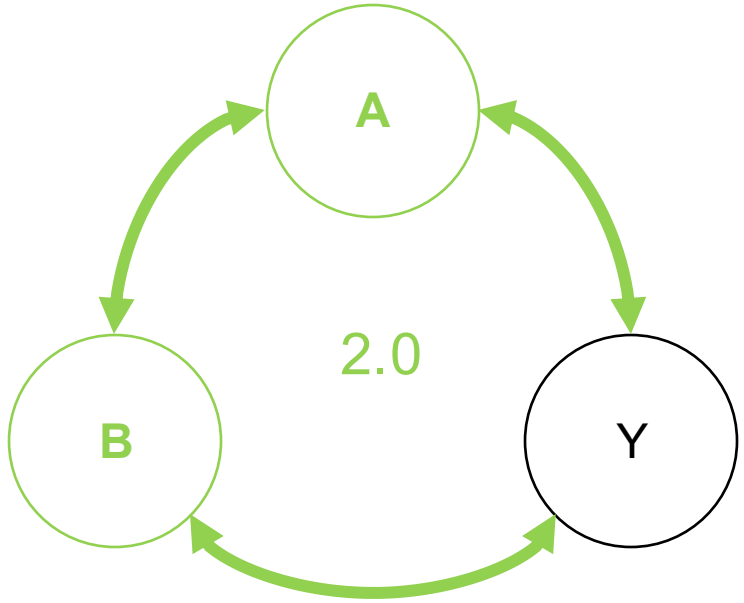


ABY2.0 Protocol

- Passively secure **2PC protocol**
- Preprocessing Model
  - **Function-dependent** preprocessing phase
  - Online phase

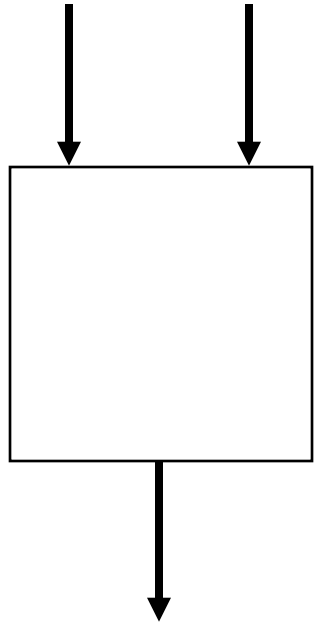
❑ input-independent computation
❑ relatively slow and expensive

❑ input-dependent computation
❑ super fast



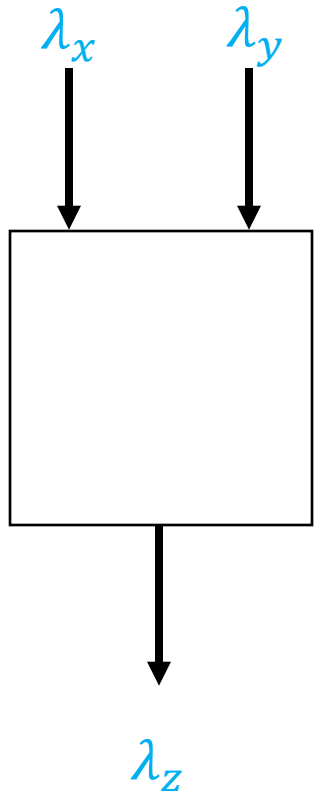
ABY2.0: Sharing Semantics

- Masked Evaluation: $m_x = x + \lambda_x$



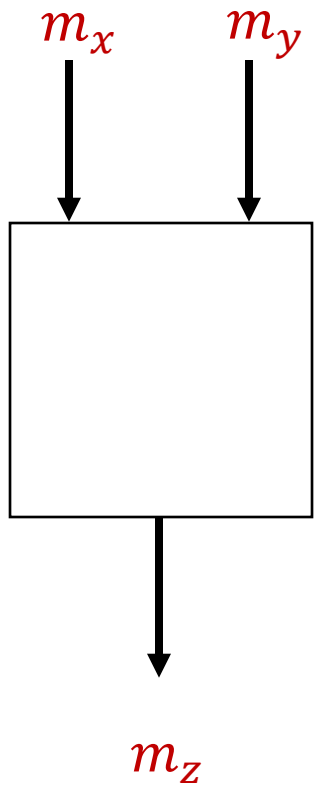
ABY2.0: Sharing Semantics

- Masked Evaluation: $m_x = x + \lambda_x$
  - Preprocessing - λ_x values



ABY2.0: Sharing Semantics

- Masked Evaluation: $m_x = x + \lambda_x$
  - Preprocessing - λ_x values
  - Online - m_x values

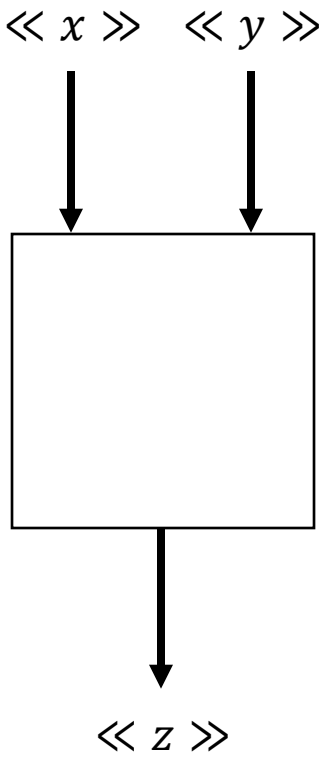


ABY2.0: Sharing Semantics

- Masked Evaluation: $m_x = x + \lambda_x$
  - Preprocessing - λ_x values
  - Online - m_x values

- Secret Sharing : $\lambda_x = \lambda_{x1} + \lambda_{x2}$
  - $P_1 : (\lambda_{x1}, m_x)$
  - $P_2 : (\lambda_{x2}, m_x)$

$\ll x \gg$

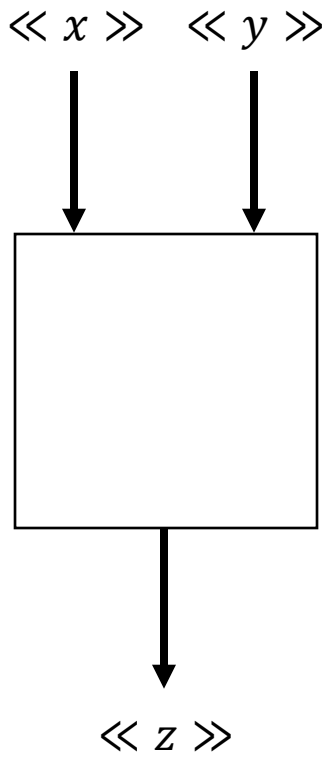


ABY2.0: Sharing Semantics

$\ll x \gg$ $\ll y \gg$

Inputs

- $P_1 : (\lambda_{x1}, m_x)$, (λ_{y1}, m_y)
- $P_2 : (\lambda_{x2}, m_x)$, (λ_{y2}, m_y)



ABY2.0: Sharing Semantics

$\ll x \gg$ $\ll y \gg$

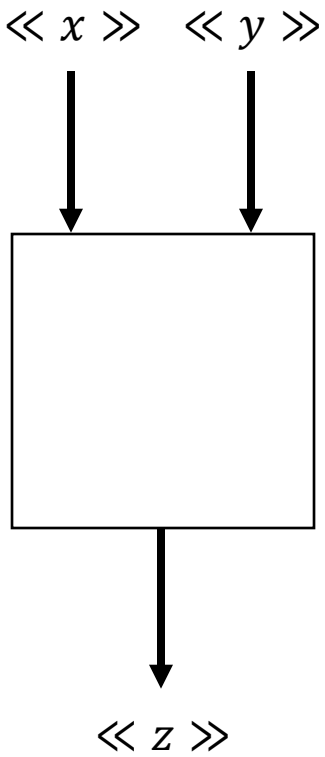
Inputs

- $P_1 : (\lambda_{x1}, m_x)$, (λ_{y1}, m_y)
- $P_2 : (\lambda_{x2}, m_x)$, (λ_{y2}, m_y)

Output

- $P_1 : (\lambda_{z1}, m_z)$
- $P_2 : (\lambda_{z2}, m_z)$

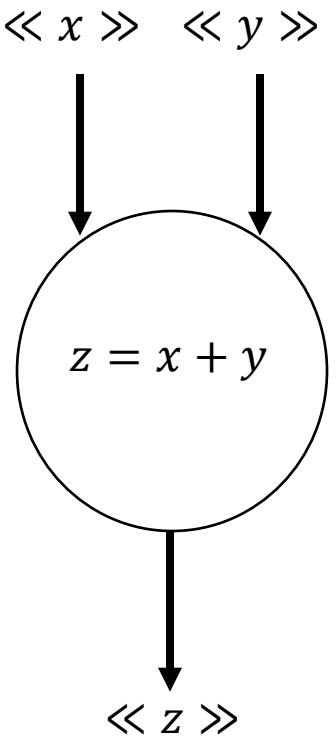
$\ll z \gg$



ABY2.0: Addition

Addition: $z = x + y$

$= (m_x - \lambda_x) + (m_y - \lambda_y)$



- $P_1 : (\lambda_{x1}, m_x), (\lambda_{y1}, m_y)$
- $P_2 : (\lambda_{x2}, m_x), (\lambda_{y2}, m_y)$

ABY2.0: Addition

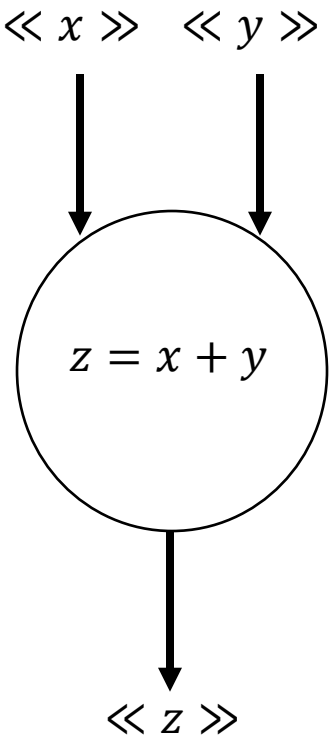
Addition: $z = x + y$

$$= (m_x - \lambda_x) + (m_y - \lambda_y)$$

$$= (m_x + m_y) - (\lambda_x + \lambda_y)$$

$$= m_z - \lambda_z$$

- $P_1 : m_z = m_x + m_y, \lambda_{z1} = \lambda_{x1} + \lambda_{y1}$
- $P_2 : m_z = m_x + m_y, \lambda_{z2} = \lambda_{x2} + \lambda_{y2}$

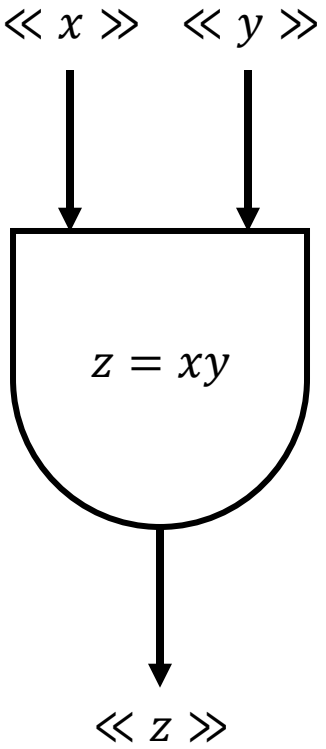


- $P_1 : (\lambda_{x1}, m_x), (\lambda_{y1}, m_y)$
- $P_2 : (\lambda_{x2}, m_x), (\lambda_{y2}, m_y)$

ABY2.0: Multiplication

Multiplication: $z = xy$

$= (m_x - \lambda_x)(m_y - \lambda_y)$



- $P_1 : (\lambda_{x1}, m_x), (\lambda_{y1}, m_y)$
- $P_2 : (\lambda_{x2}, m_x), (\lambda_{y2}, m_y)$

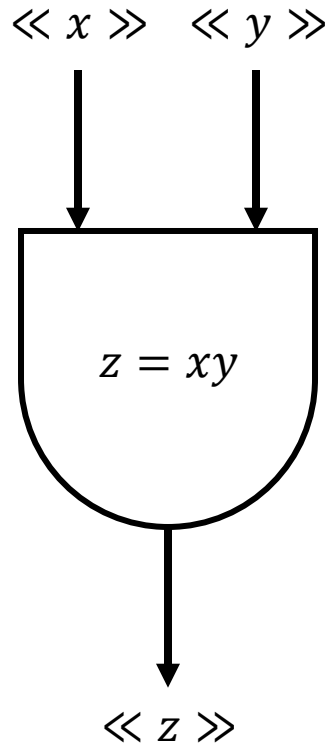
ABY2.0: Multiplication

Multiplication: $z = xy$

$$= (m_x - \lambda_x)(m_y - \lambda_y)$$

$$= m_x m_y - m_x \lambda_y - m_y \lambda_x + \lambda_x \lambda_y$$

$$m_z = m_x m_y - m_x \lambda_y - m_y \lambda_x + \lambda_x \lambda_y + \lambda_z$$

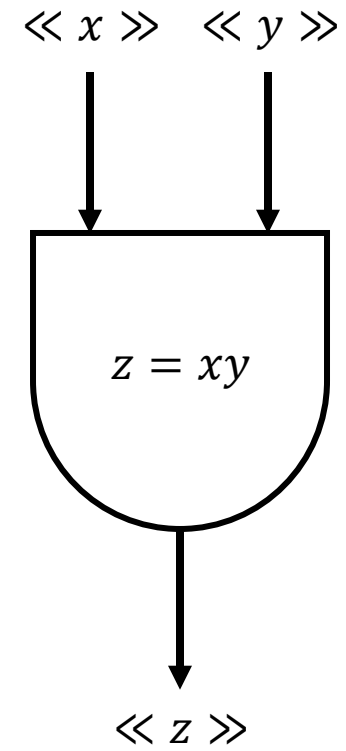


- $P_1 : (\lambda_{x1}, m_x), (\lambda_{y1}, m_y)$
- $P_2 : (\lambda_{x2}, m_x), (\lambda_{y2}, m_y)$

ABY2.0: Multiplication

- Preprocessing : P_1 : λ_{z1} P_2: λ_{z2}
- Online: m_z ?

$$m_z = m_x m_y - m_x \lambda_y - m_y \lambda_x + \lambda_x \lambda_y + \lambda_z$$



- $P_1 : (\lambda_{x1}, m_x), (\lambda_{y1}, m_y)$
- $P_2 : (\lambda_{x2}, m_x), (\lambda_{y2}, m_y)$

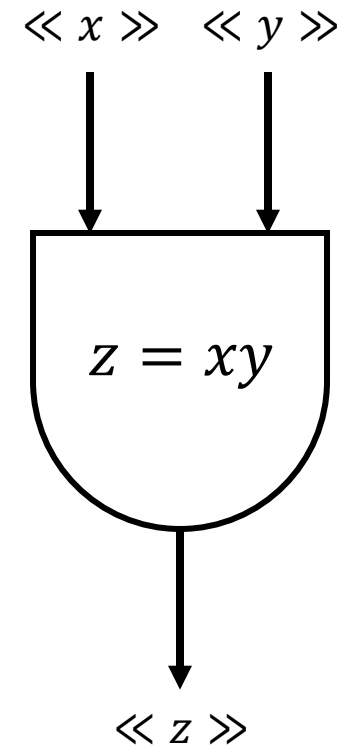
ABY2.0: Multiplication

- Preprocessing : P_1 : λ_{z1} P_2: λ_{z2}
- Online: m_z ?

$$m_z = m_x m_y - m_x \lambda_y - m_y \lambda_x + \lambda_x \lambda_y + \lambda_z$$

Beaver Triple

$$\lambda_x \lambda_y = (\lambda_{x1} + \lambda_{x2})(\lambda_{y1} + \lambda_{y2}) = (\lambda_x \lambda_y)_1 + (\lambda_x \lambda_y)_2$$



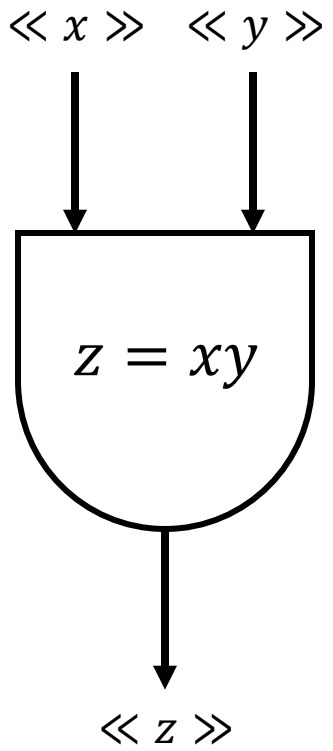
- $P_1 : (\lambda_{x1}, m_x), (\lambda_{y1}, m_y)$
- $P_2 : (\lambda_{x2}, m_x), (\lambda_{y2}, m_y)$

ABY2.0: Multiplication

- Preprocessing : $P_1 : \lambda_{z1}$ $P_2: \lambda_{z2}$
- Online: m_z ?

$$m_z = m_x m_y - m_x \lambda_y - m_y \lambda_x + \lambda_x \lambda_y + \lambda_z$$

- $P_1 : m_{z1} = m_x m_y - m_x \lambda_{y1} - m_y \lambda_{x1} + (\lambda_x \lambda_y)_1 + \lambda_{z1}$
- $P_2 : m_{z2} = -m_x \lambda_{y2} - m_y \lambda_{x2} + (\lambda_x \lambda_y)_2 + \lambda_{z2}$



- $P_1 : (\lambda_{x1}, m_x), (\lambda_{y1}, m_y), (\lambda_x \lambda_y)_1$
- $P_2 : (\lambda_{x2}, m_x), (\lambda_{y2}, m_y), (\lambda_x \lambda_y)_2$

ABY2.0: Multiplication

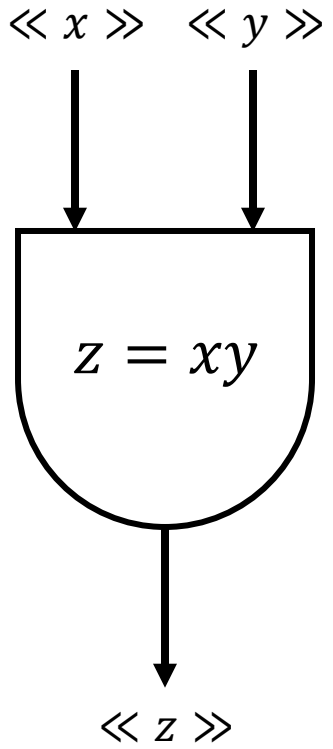
- Preprocessing : $P_1 : \lambda_{z1} \quad P_2 : \lambda_{z2}$
- Online: m_z ?

$$m_z = m_x m_y - m_x \lambda_y - m_y \lambda_x + \lambda_x \lambda_y + \lambda_z$$

- $P_1 : m_{z1} = m_x m_y - m_x \lambda_{y1} - m_y \lambda_{x1} + (\lambda_x \lambda_y)_1 + \lambda_{z1}$
- $P_2 : m_{z2} = -m_x \lambda_{y2} - m_y \lambda_{x2} + (\lambda_x \lambda_y)_2 + \lambda_{z2}$

$P_1 \rightarrow P_2 : m_{z1}$

$P_2 \rightarrow P_1 : m_{z2}$



- $P_1 : (\lambda_{x1}, m_x), (\lambda_{y1}, m_y), (\lambda_x \lambda_y)_1$
- $P_2 : (\lambda_{x2}, m_x), (\lambda_{y2}, m_y), (\lambda_x \lambda_y)_2$

ABY2.0: Multiplication

- Preprocessing : $P_1 : \lambda_{z1} \quad P_2 : \lambda_{z2}$
- Online: m_z ?

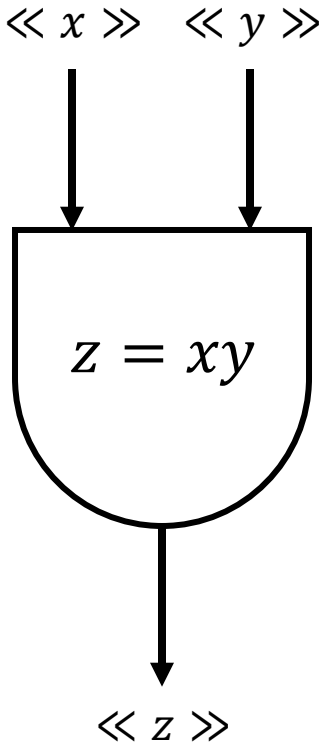
$$m_z = m_x m_y - m_x \lambda_y - m_y \lambda_x + \lambda_x \lambda_y + \lambda_z$$

- $P_1 : m_{z1} = m_x m_y - m_x \lambda_{y1} - m_y \lambda_{x1} + (\lambda_x \lambda_y)_1 + \lambda_{z1}$
- $P_2 : m_{z2} = -m_x \lambda_{y2} - m_y \lambda_{x2} + (\lambda$

$P_1 \rightarrow P_2 : m_{z1}$

$P_2 \rightarrow P_1 : m_{z2}$

Online
(2 elements communication)



- $P_1 : m_z = m_{z1} + m_{z2}$
- $P_2 : m_z = m_{z1} + m_{z2}$

- $P_1 : (\lambda_{x1}, m_x), (\lambda_{y1}, m_y), (\lambda_x \lambda_y)_1$
- $P_2 : (\lambda_{x2}, m_x), (\lambda_{y2}, m_y), (\lambda_x \lambda_y)_2$

ABY2.0: Multiplication

	Pre-processing Communication		Online Communication (#elements)
SOTA [DSZ15]	|Triples|	Function-independent	4
ABY2.0	|Triples|	Function-dependent	**2**

|Triples|: cost for generating one Beaver triple via OT or HE

ABY2.0: Multi-Input Multiplication

		Pre-processing Communication	Online Communication (#elements)
3-input Multiplication	SOTA [DSZ15]	2·|Triples|	8
	ABY2.0	4·|Triples|	**2** ⟵ Independent of fan-in!
4-input Multiplication	SOTA [DSZ15]	3·|Triples|	12
	ABY2.0	11·|Triples|	**2** ⟵ Independent of fan-in!

|Triples|: cost for generating one Beaver triple via OT or HE

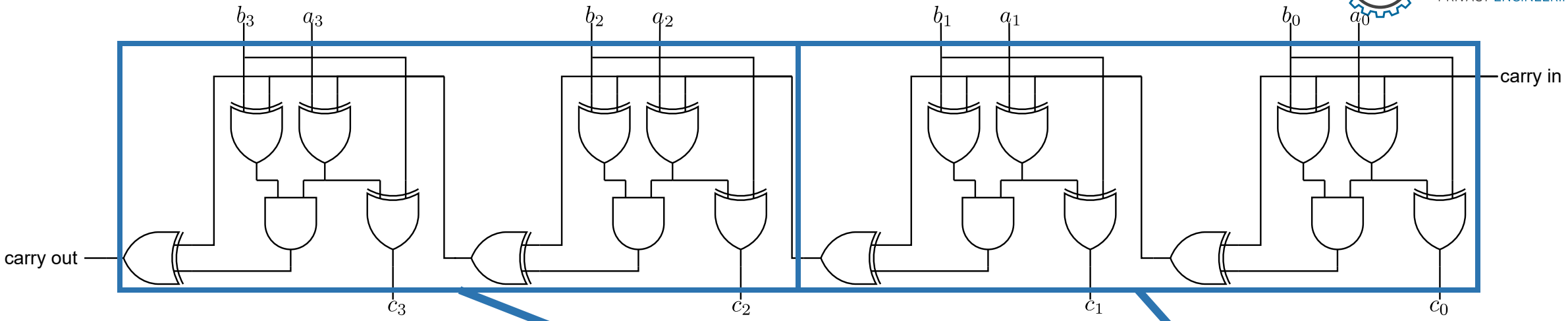
ABY2.0: Dot Product

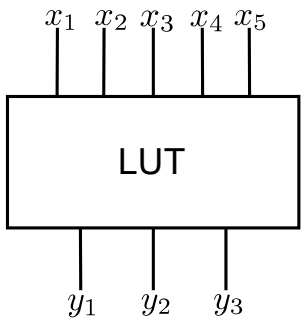
$$X \cdot Y = \sum_{i=1}^{d} x_i \cdot y_i$$

	Pre-processing Communication	Online Communication (#elements)
SOTA [DSZ15]	d·|Triples|	4d
ABY2.0	d·|Triples|	**2** ← Independent of dimension!

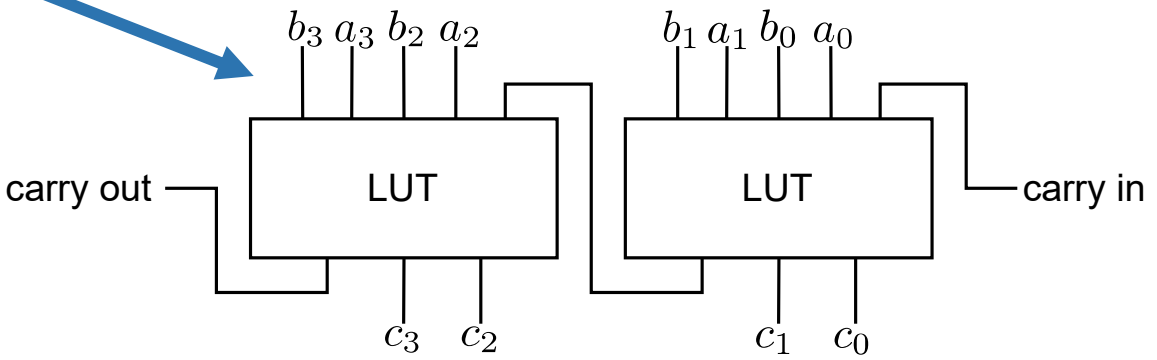
d: dimension of vector
|Triples|: cost for generating one Beaver triple

Lookup Tables



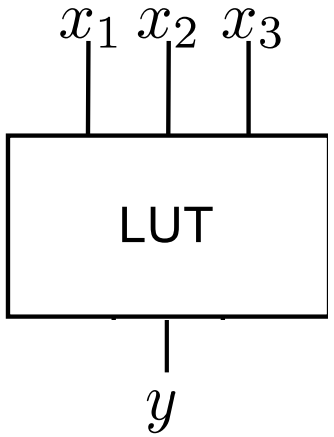


x_1	x_2	x_3	x_4	x_5	y_1	y_2	y_3
0	0	0	0	0	0	0	0
0	0	0	0	1	0	1	0
0	0	0	1	0	0	1	0
0	0	0	1	1	0	0	1
0	0	1	0	0	1	0	0
0	0	1	0	1	1	1	0
0	0	1	1	0	1	1	0
0	0	1	1	1	1	0	1
0	1	0	0	0	1	0	0
0	1	0	0	1	1	1	0
.....							



FLUTE

1.



x_1	x_2	x_3	y
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

2. disjunctive normal form

$$(\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}) \vee (\overline{x_1} \wedge x_2 \wedge x_3) \vee (x_1 \wedge \overline{x_2} \wedge x_3)$$

3.

$$(\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}) \oplus (\overline{x_1} \wedge x_2 \wedge x_3) \oplus (x_1 \wedge \overline{x_2} \wedge x_3)$$

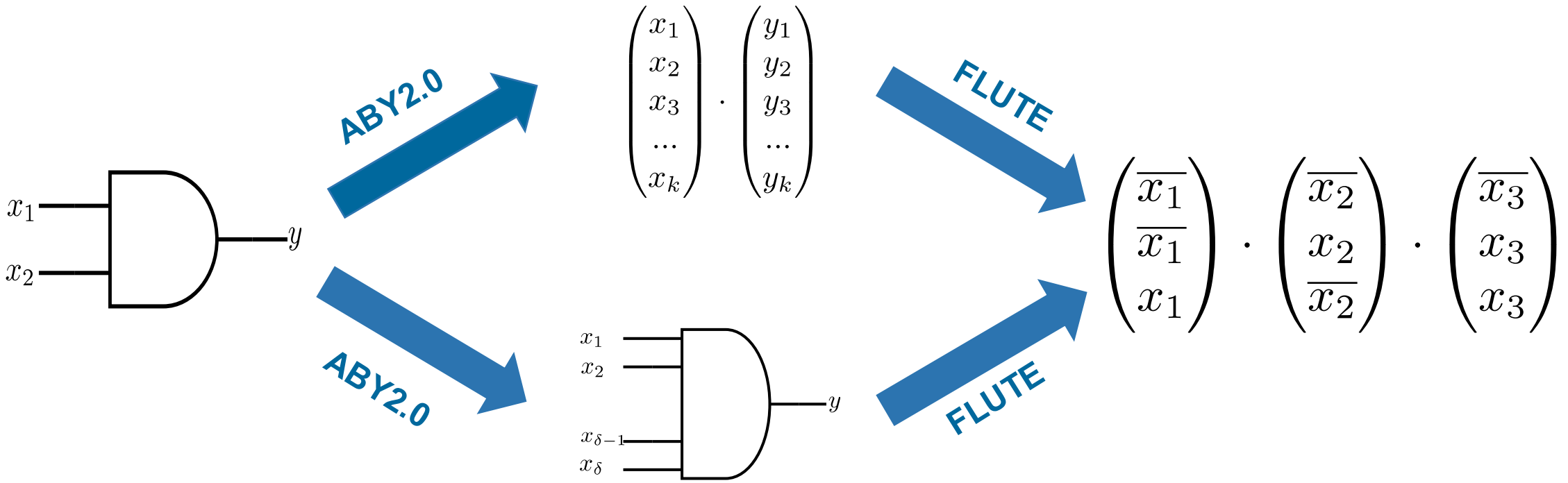
4.

$$(\overline{x_1} \cdot \overline{x_2} \cdot \overline{x_3}) + (\overline{x_1} \cdot x_2 \cdot x_3) + (x_1 \cdot \overline{x_2} \cdot x_3) \quad \text{in } \mathbb{F}_2$$

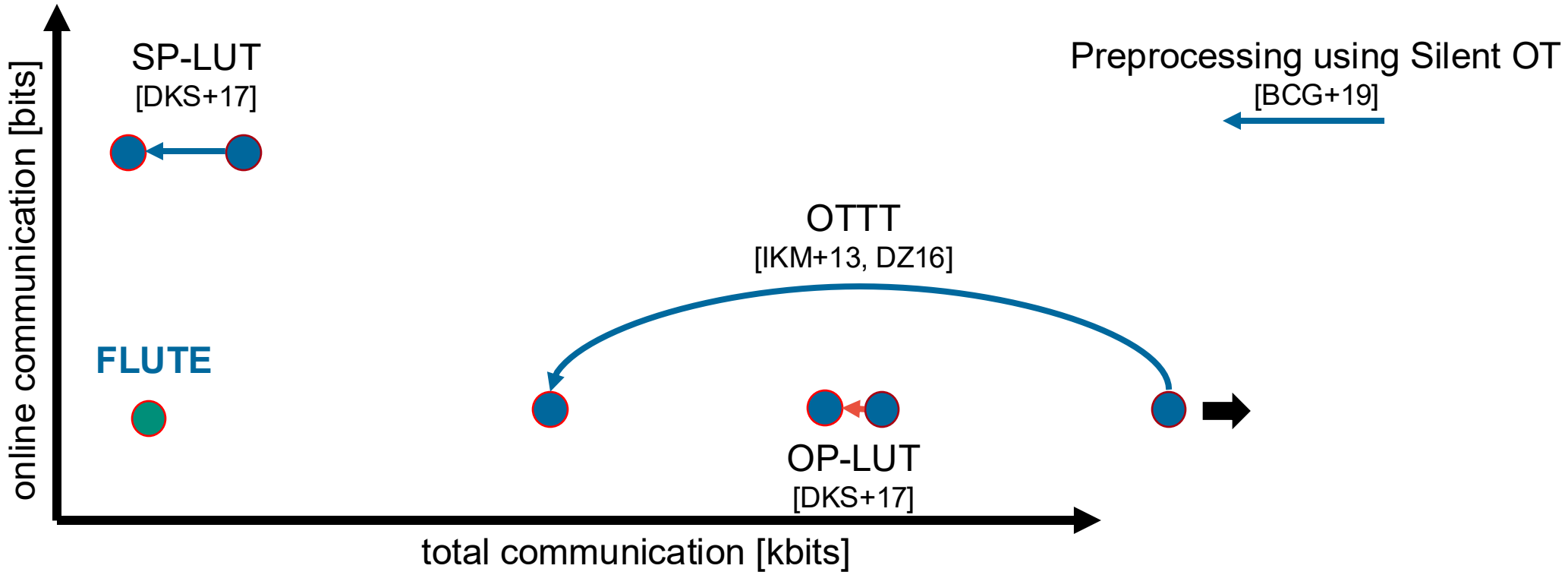
5.

$$\begin{pmatrix} \overline{x_1} \\ \overline{x_1} \\ x_1 \end{pmatrix} \cdot \begin{pmatrix} \overline{x_2} \\ x_2 \\ \overline{x_2} \end{pmatrix} \cdot \begin{pmatrix} \overline{x_3} \\ x_3 \\ x_3 \end{pmatrix}$$

From ABY2.0 To FLUTE



SOTA => FLUTE Improvements



LUT Communication

TECHNISCHE UNIVERSITÄT DARMSTADT

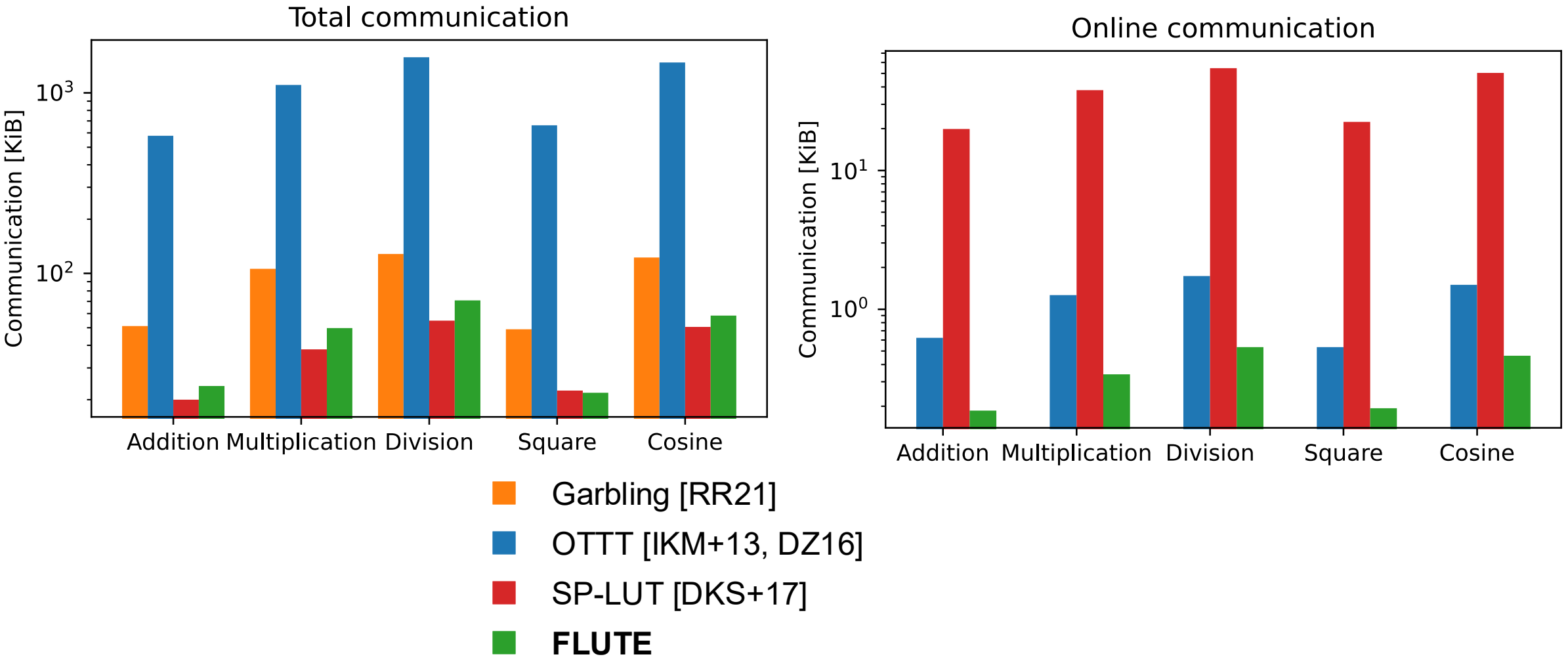
ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

LUT with δ inputs and σ outputs, $\kappa = 128$: symmetric security parameter

Protocol	Setup Communication [bits]	Online Communication [bits]	Online Rounds	Total 2-input LUT $\delta = 2, \sigma = 1$	Total 3-input LUT $\delta = 3, \sigma = 1$	Total 4-input LUT $\delta = 4, \sigma = 1$
OTTT [IKM+13,DZ16]	$4.2(\delta - 1)2^{\delta}\sigma$	2δ	1	21 bits	74 bits	210 bits
OP-LUT [DKS+17]	$0.1\delta + 2^{2\delta} + \sigma$	2δ	1	22 bits	72 bits	266 bits
SP-LUT [DKS+17]	0.1δ	$2^{\delta}\sigma + \delta$	1	7 bits	12 bits	21 bits
FLUTE	$\mathbf{4.2(2^{\delta} - \delta - 1)}$	$\mathbf{2\sigma}$	**1**	**7 bits**	**19 bits**	**49 bits**
Garbled LUT [MNPS04]	$\kappa(2^{\delta} - 1)\sigma$	0	0	384 bits	896 bits	1,920 bits
Garbled 2-input gates [RR21]	$1.5\kappa(2^{\delta-1} - 1)\sigma$	0	0	192 bits	576 bits	1,344 bits

All complexities calculated with Silent OT [BCG+19] for preprocessing.

FLUTE: FP32 Operations



ABY2.0 vs. FLUTE