



Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG



ISMB 2022 - Theory Session

Privacy-Enhancing Techniques

Overview

1. Why use privacy enhancing techniques ?
2. Outdated approaches (k-anonymity)
3. Differential Privacy (DP)
4. Secure Multi Party Computation (SMPC)
5. Homomorphic Encryption
6. Summary

Why use privacy enhancing techniques?



<https://emerging-europe.com/voices/gdpr-looking-back-and-looking-forward/>



<https://www.hxnwrk.com/verschiedene-typen-von-hackern/>

Outdated Approaches

De-identification

→ bad bad

K-anonymity (<https://opendp.github.io/cs208/spring2022/presentations/overview-reidentification.pdf>)

- Quasi-identifier fallacy (Netflix challenge)
- Other Attacks (composition, downcoding)
- Problems with summary statistics
- Membership attacks
 - Classical
 - Inference of sensitive attributes

→ also bad



Outdated Approaches

Basic Idea: De-Identification via Suppression

Name	Age	Height	Sex	Disease
Peter	46	1.70	M	N
Jane	27	1.72	F	N
Joe	30	1.85	M	Y
Liza	24	1.65	F	Y

Basic Idea: De-Identification via Suppression

Name	Age	Height	Sex	Disease
Peter	46	1.70	M	N
Jane	27	1.72	F	N
Joe	30	1.85	M	Y
Liza	24	1.65	F	Y



Name	Age	Height	Sex	Disease
-	46	1.70	M	N
-	27	1.72	F	N
-	30	1.85	M	Y
-	24	1.65	F	Y

Basic Idea: De-Identification via Generalization

Name	Age	Height	Sex	Disease
-	46	1.70	M	N
-	27	1.72	F	N
-	30	1.85	M	Y
-	24	1.65	F	Y



Name	Age	Height	Sex	Disease
-	41–50	1.70	M	N
-	21–30	1.72	F	N
-	21–20	1.85	M	Y
-	21–30	1.65	F	Y

Basic Idea: De-Identification via Generalization

Name	Age	Height	Sex	Disease
-	46	1.70	M	N
-	27	1.72	F	N
-	30	1.85	M	Y
-	24	1.65	F	Y



Name	Age	Height	Sex	Disease
-	41–50	1.7*	M	N
-	21–30	1.7*	F	N
-	21–20	1.8*	M	Y
-	21–30	1.6*	F	Y

K-Anonymity

Formally, we say that a dataset D satisfies k -Anonymity for a value of k if:

- For each row $r_1 \in D$, there exists at least $k - 1$ other rows $r_2 \dots r_k \in D$ such that

$$\prod_{qi(D)} r_1 = \prod_{qi(D)} r_2, \dots, \prod_{qi(D)} r_1 = \prod_{qi(D)} r_k$$

where $qi(D)$ is the quasi-identifiers of D , and $\prod_{qi(D)} r$ represents the columns

of r containing quasi-identifiers (i. e. the projection of the quasi-identifiers).

K-Anonymity

Formally, we say that a dataset D satisfies k -Anonymity for a value of k if:

- For each row $r_1 \in D$, there exists at least $k - 1$ other rows $r_2 \dots r_k \in D$ such that

$$\prod_{qi(D)} r_1 = \prod_{qi(D)} r_2, \dots, \prod_{qi(D)} r_1 = \prod_{qi(D)} r_k$$

where $qi(D)$ is the **quasi-identifiers** of D , and $\prod_{qi(D)} r$ represents the columns

of r containing quasi-identifiers (i. e. the projection of the quasi-identifiers).

Quasi-identifiers – ‘important’ features

- 2006 Netflix 1 Mio \$ movie-recommendation challenge.
- **100,480,507 movie ratings** of **480,189 Netflix subscribers** from 1999 to 2005
- FAQ: “Is there any customer information in the dataset that should be kept private?”

Answer: “**No**, all customer **identifying information** has been removed; all that remains are ratings and dates. This follows our privacy policy. [...] **Even** if, for example, you knew all **your own ratings** and their dates you probably **couldn’t identify** them reliably in the data because only a small sample was included [...] and that data was subject to perturbation.”

Quasi-identifiers – ‘important’ features

Narayanan-Shmatikov Set-Up (Narayanan & Shmatikov, 2008)

Dataset: x = set of records r (e.g. Netflix ratings)

Adversary’s inputs:

x' = subset of x , possibly distorted

aux = auxiliary information about record r (e.g. public IMDB ratings)

Adversary’s goals:

Output either r' that is close to r or output ‘no match’

Quasi-identifiers – ‘important’ features

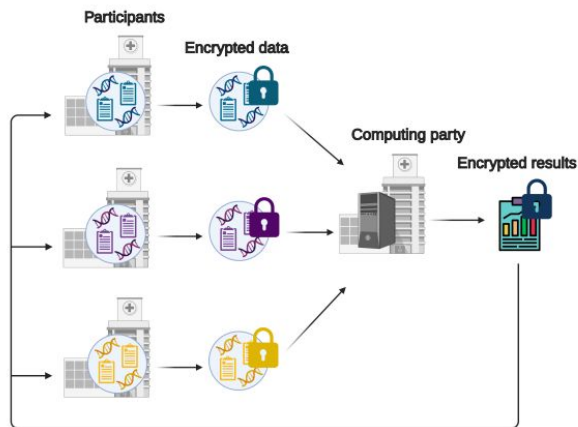
$$\text{score}(aux, r') = \underbrace{\sum_{a \in \text{supp}(aux)} \text{IMDB rating}}_{\text{IMDB rating}} \underbrace{\text{sim}(aux_a, r'_a)}_{\text{Similarity of rating and date}} * \underbrace{\frac{1}{\log |\{r' \in \hat{x} : a \in \text{supp}(r')\}|}}_{\text{Downweight popular movies}}$$

Sampled 50 IMDB users → identified 2 in Netflix dataset

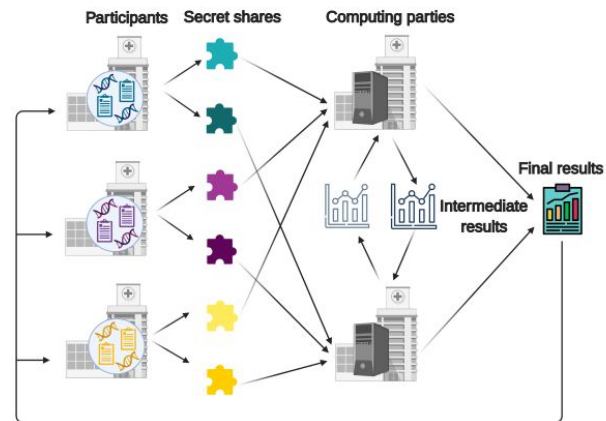
(→ Class action lawsuit, no Netflix Challenge II)

→ **every feature can be a quasi identifier!**

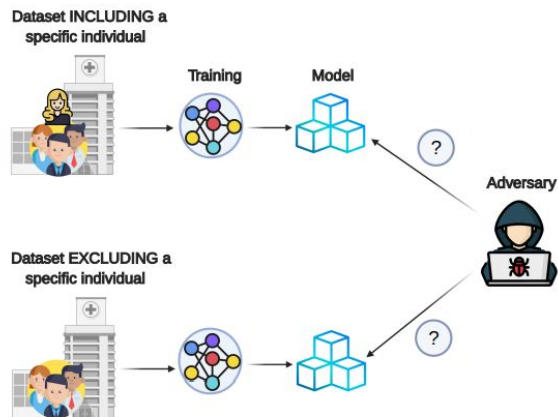
Better working approaches



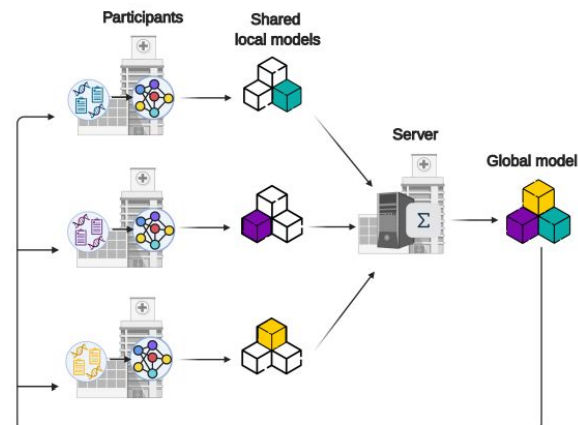
a) Homomorphic encryption



b) Secure multiparty computation



c) Differential privacy



d) Federated learning



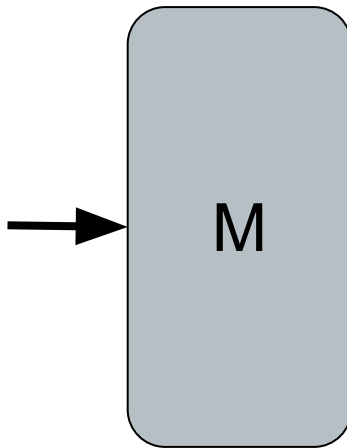
Differential privacy (<http://people.seas.harvard.edu/~salil/cs208/spring19/>)

- introduce concepts (<http://people.seas.harvard.edu/~salil/cs208/spring19/DP-foundations1-lecture.pdf>)
- And application examples (<http://people.seas.harvard.edu/~salil/cs208/spring19/DP-foundations2-lecture.pdf>)
- Programming example (?) (<https://gist.github.com/julianspaeth/5f410cd706fdf2d9bec73c8b794cd357>)
- Attack vectors (Privacy budget attack) (<https://css.csail.mit.edu/6.858/2013/readings/dp-under-fire.pdf>) (?)
- Pro/Con

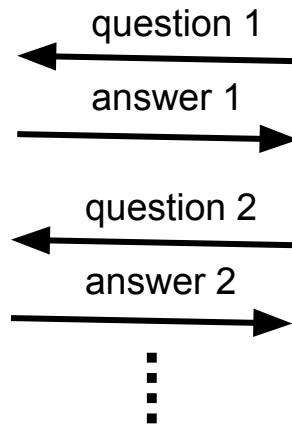
Differential Privacy

Differential Privacy

Age	Height	Sex	...	Disease
46	1.70	M	...	N
27	1.72	F	...	N
30	1.85	M	...	Y
24	1.65	F	...	Y
57	1.69	M	...	N
32	1.79	F	...	Y
40	1.58	F	...	Y



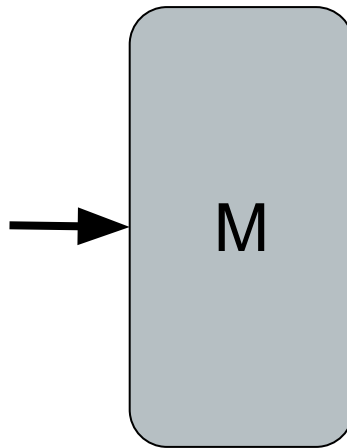
mechanism



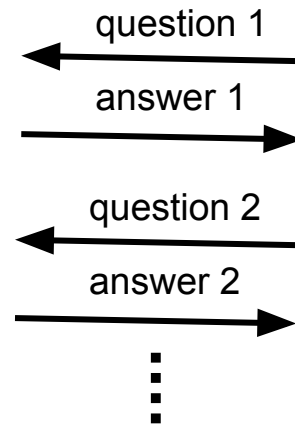
data scientists

Differential Privacy

Age	Height	Sex	...	Disease
46	1.70	M	...	N
27	1.72	F	...	N
30	1.85	M	...	Y
24	1.65	F	...	Y
57	1.69	M	...	N
32	1.79	F	...	Y
40	1.58	F	...	Y



mechanism

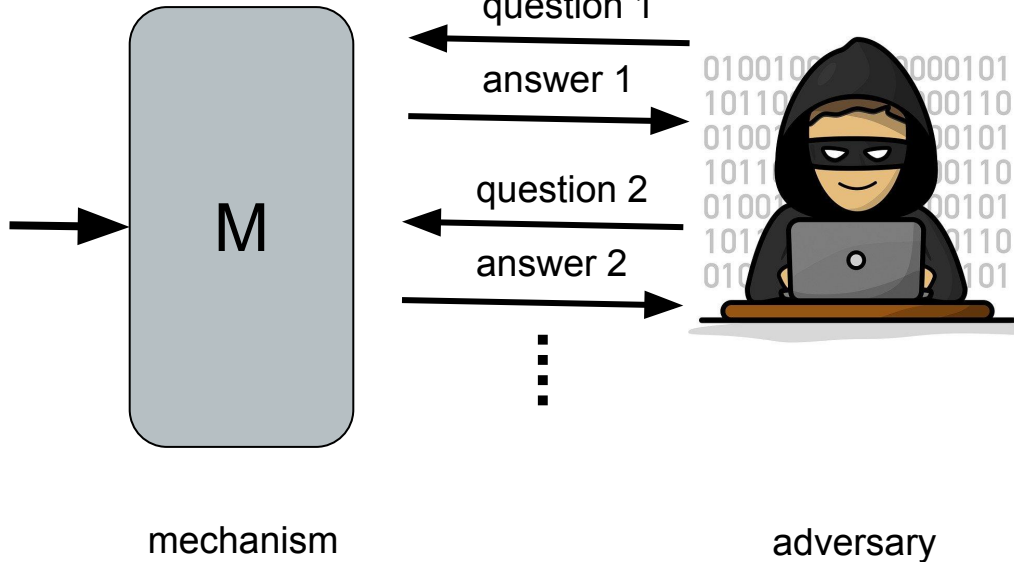


data scientists

→ effect of each individual should be 'hidden'

Differential Privacy

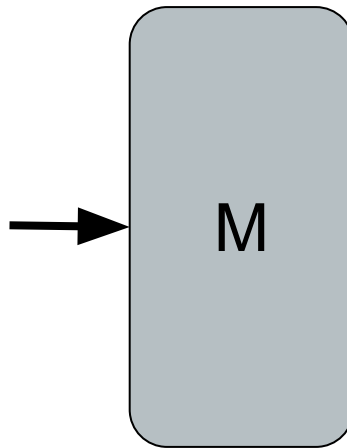
Age	Height	Sex	...	Disease
46	1.70	M	...	N
27	1.72	F	...	N
30	1.85	M	...	Y
24	1.65	F	...	Y
57	1.69	M	...	N
32	1.79	F	...	Y
40	1.58	F	...	Y



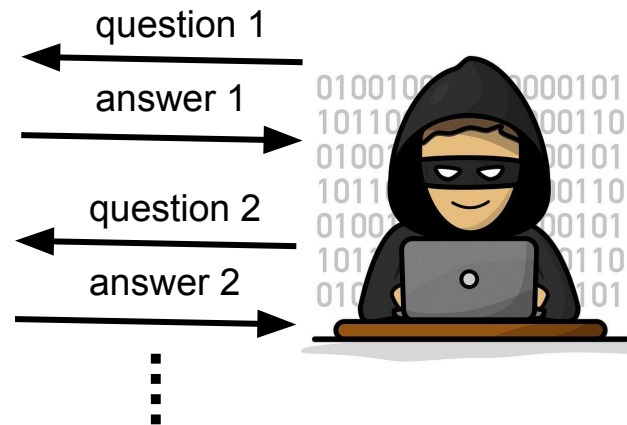
→ adversary shouldn't be able to tell if any one person's data were to change arbitrarily

Differential Privacy

Age	Height	Sex	...	Disease
46	1.70	M	...	N
27	1.72	F	...	N
30	1.85	M	...	Y
24	1.65	F	...	Y
57	1.69	M	...	N
32	1.79	F	...	Y
40	1.58	F	...	Y



mechanism

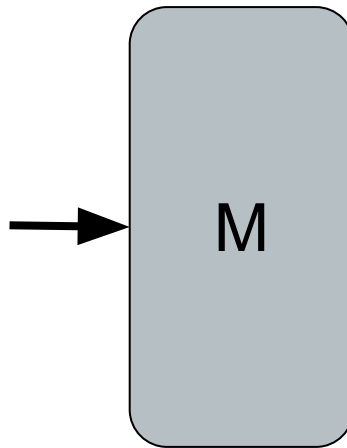


adversary

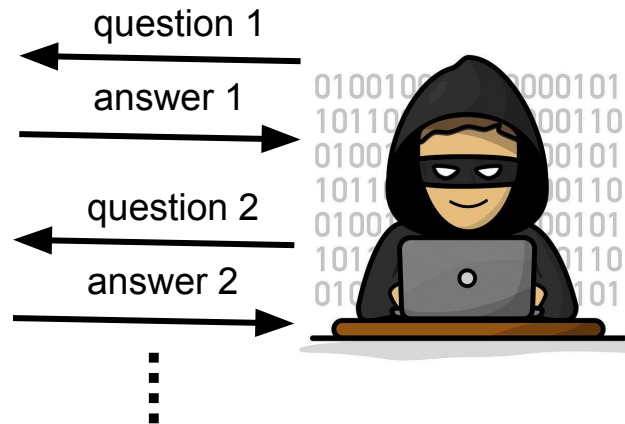
→ adversary shouldn't be able to tell if any one person's data were to change arbitrarily

Differential Privacy

Age	Height	Sex	...	Disease
46	1.70	M	...	N
27	1.72	F	...	N
24	1.65	F	...	Y
57	1.69	M	...	N
32	1.79	F	...	Y
40	1.58	F	...	Y



mechanism

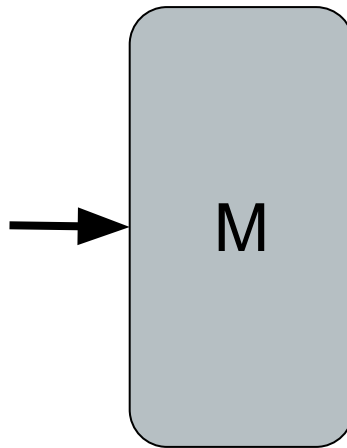


adversary

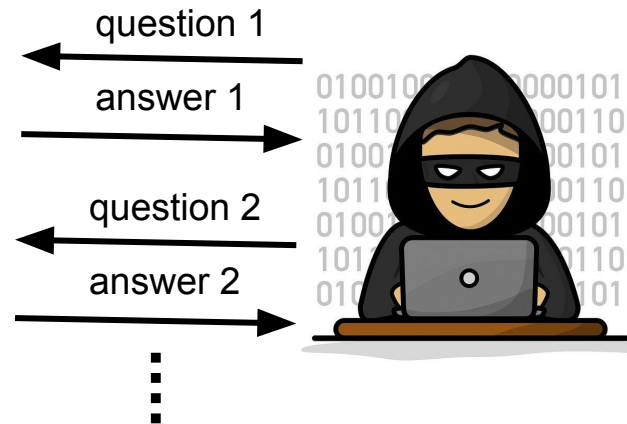
→ adversary shouldn't be able to tell if any one person's data were to change arbitrarily

Differential Privacy

Age	Height	Sex	...	Disease
46	1.70	M	...	N
27	1.72	F	...	N
66	1.55	F	...	N
24	1.65	F	...	Y
57	1.69	M	...	N
32	1.79	F	...	Y
40	1.58	F	...	Y



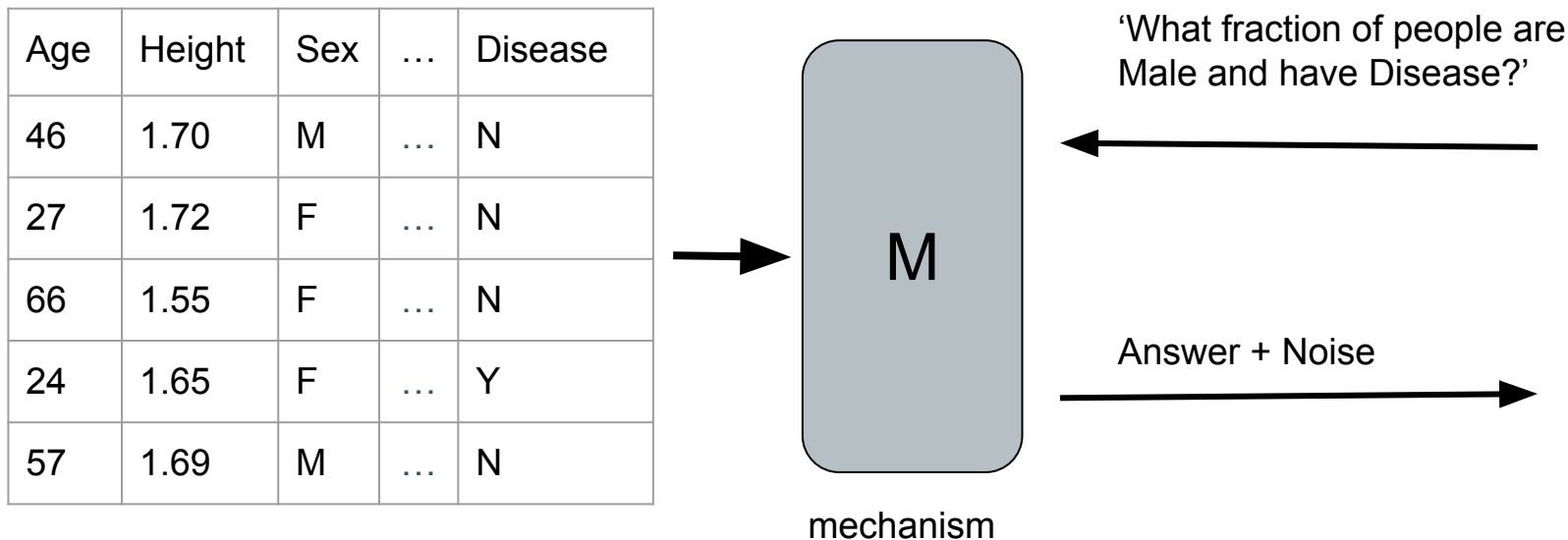
mechanism



adversary

→ adversary shouldn't be able to tell if any one person's data were to change arbitrarily

Differential Privacy – output perturbation



- Very little noise needed as number of entries $n \rightarrow \infty$.
- This is just for **one** query

Differential Privacy – Laplace Mechanism

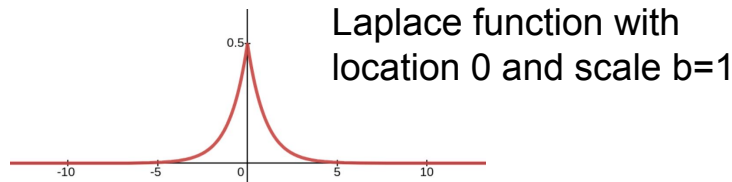
For a function $f(x)$ that returns a number, this definition of $F(x)$ satisfies ϵ -differential privacy:

$$F(x) = f(x) + \text{Lap}\left(\frac{s}{\epsilon}\right)$$

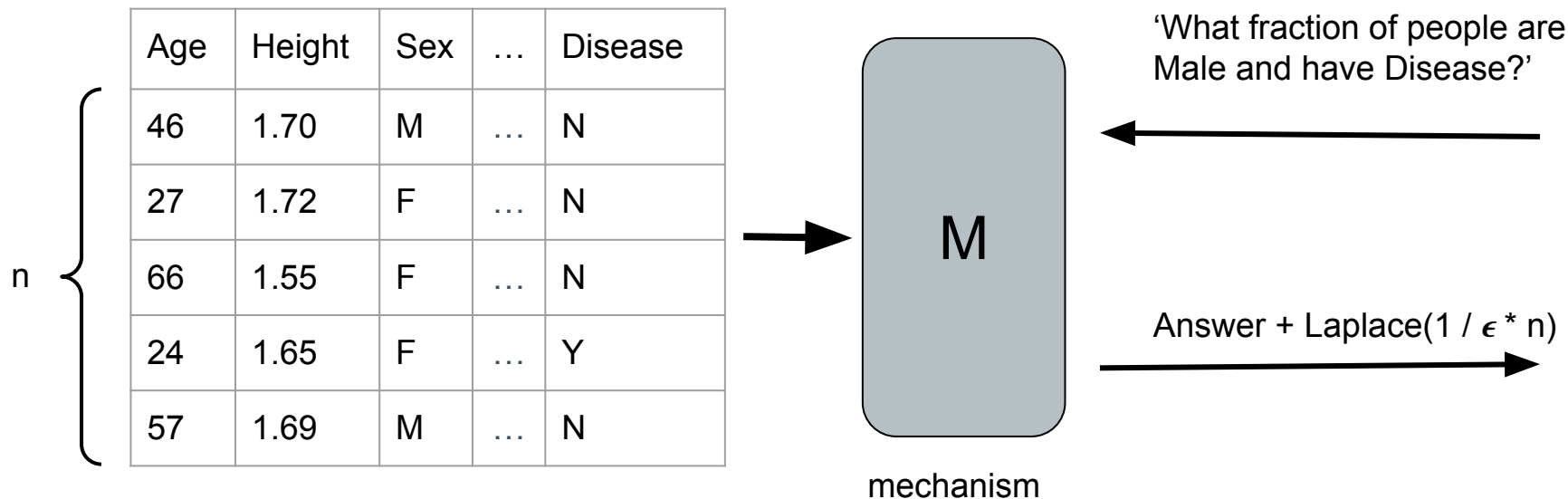
where $\text{Lap}(S)$ samples from the Laplace distribution and s is the sensitivity of f . The sensitivity s of f denotes the amount f 's output changes when its input changes by 1.

The Laplace function with location 0 and scale b has the density:

$$p(x) = \frac{1}{2b} \exp\left(-\frac{|x|}{b}\right)$$



Differential Privacy – output perturbation



- Very little noise needed as number of entries $n \rightarrow \infty$.

Differential Privacy – Privacy Budget

- If M is ϵ -DP for one query, it is $k\epsilon$ -DP for k queries.
- To maintain global privacy loss at most ϵ_{global} , can set $\epsilon = \epsilon_{\text{global}} / k$ and stop answering after k queries.
- More queries \rightarrow smaller $\epsilon \rightarrow$ less accuracy
Some tradeoff is necessary

Typical recommendation for ‘good’ privacy guarantee:

$$0.01 \leq \epsilon \leq 1$$

Differential Privacy – Summary

- Whatever an adversary learns **about me**, it could have been learned **from everyone** else's data
- No leakage of data **specific to individuals**
- This holds regardless of **computational power** or **auxiliary information**

But:

- **No guarantee** that adversary won't **infer sensitive attributes**.
- **No guarantee** that subjects won't be '**harmed**' by results of analysis
- **No protection** for information that is not localized to a few rows

- Concept
- Programming example (?) (<https://github.com/OpenMined/SyMPC>, <https://github.com/iamaldi/smpc>)
- attack vectors (<https://eprint.iacr.org/2020/300.pdf>, <https://arxiv.org/pdf/1005.5020.pdf>) (?)
- Pro/Con




Secure Multi Party Computation (SMPC)

Secure Multiparty Computation – Example

→ Average salary

	Salary k€/year
Niklas	50
Mohammad	60
Jan	100
<hr/>	
$210 / 3 = 70$	

Secure Multiparty Computation – Example



	Salary k€/year
Niklas	50
Mohammad	60
Jan	100
	$210 / 3 = 70$

→ Average salary
without sharing

Secure Multiparty Computation

	Salary k€/year	Shard 1	Shard 2	Shard3
Niklas	50			
Mohammad	60			
Jan	100			

Secure Multiparty Computation

	Salary k€/year	Shard 1	Shard 2	Shard3
Niklas	50	-20	0	70
Mohammad	60	40	70	-50
Jan	100	60	30	10



Secure Multiparty Computation

Niklas	Mohammad	Jan
-20	0	70
40	70	-50
60	30	10

Secure Multiparty Computation

Niklas	Mohammad	Jan
-20	0	70
40	70	-50
60	30	10
80	100	30

Secure Multiparty Computation

Niklas	Mohammad	Jan
-20	0	70
40	70	-50
60	30	10
80	100	30

$$210 / 3 = 70$$



Universität Hamburg

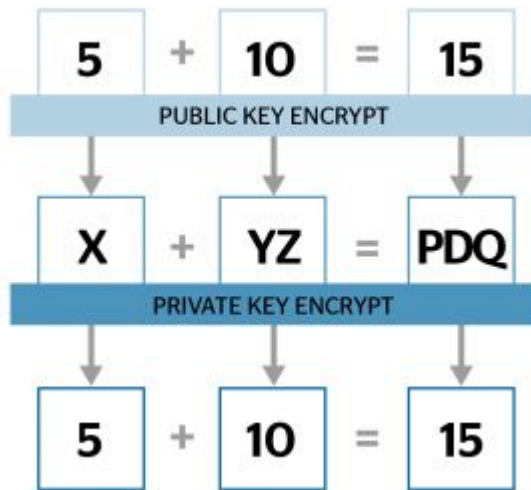
DER LEHRSTUHL FÜR INFORMATIK UND RECHNUNGSWISSENSCHAFT

Homomorphic encryption (?)

- Concept (<https://www.ibm.com/security/digital-assets/fhe/unlock-value-of-sensitive-data-without-decryption/>)
- Application (in FL) (<https://developer.nvidia.com/blog/federated-learning-with-homomorphic-encryption/>)
- Pro/Con

Homomorphic Encryption

Homomorphic encryption



<https://atos.net/en/lp/cybersecurity-magazine-enter-a-new-cybersecurity-era/the-challenges-of-homomorphic-encryption>

Pre FHE timeline

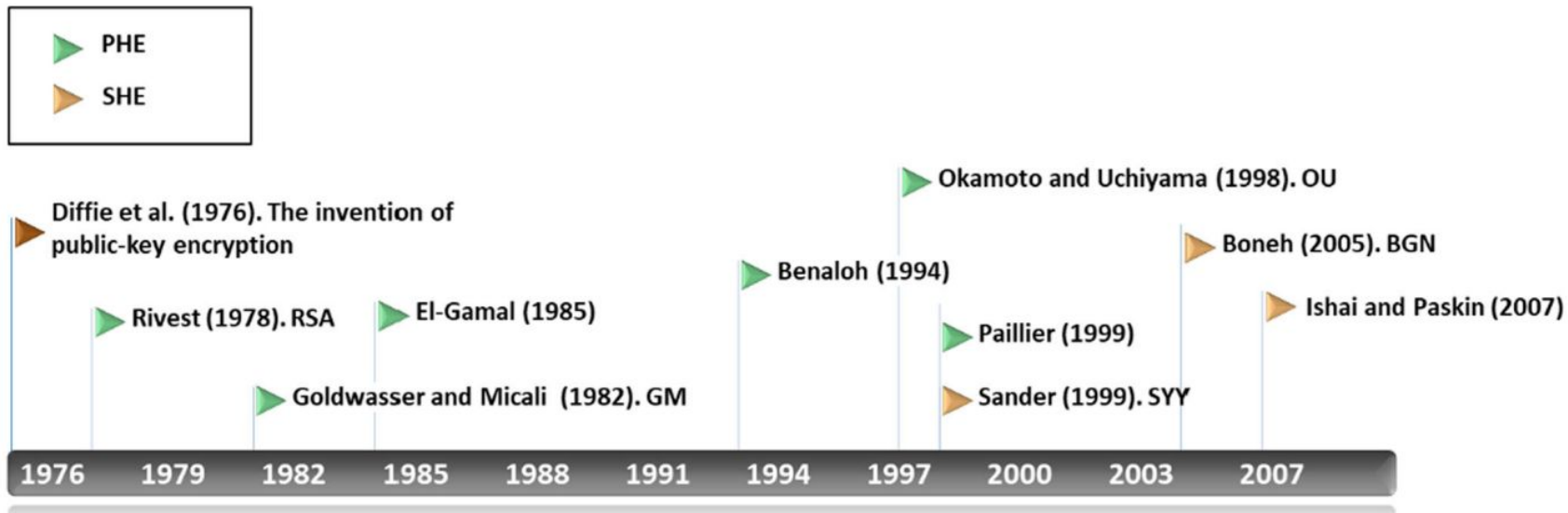


Fig. 1 Homomorphic encryption timeline

FHE timeline

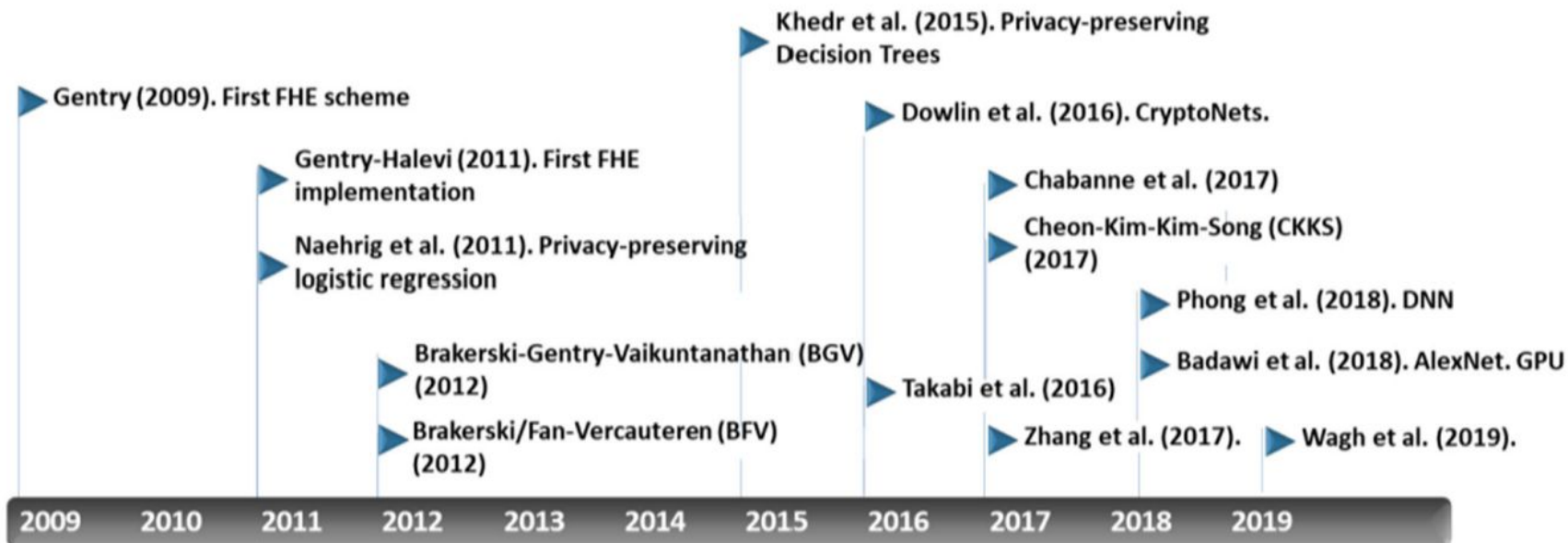


Fig. 2 Fully Homomorphic Encryption timeline

So why aren't we using it?

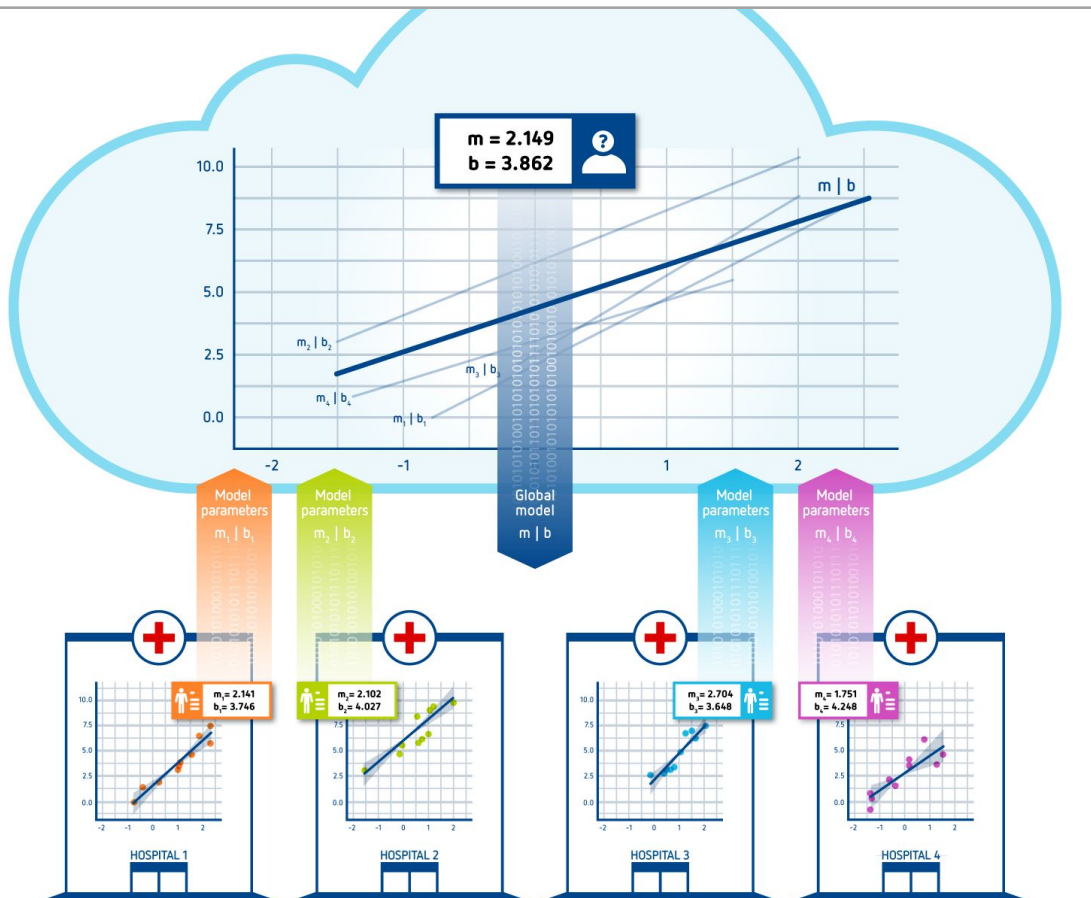
- Speed.
- Fastest FHE algorithm still factor 1 Mio slower than normal operation
- Normal calculation of 1 sec -> $\sim 11 \frac{1}{2}$ days of FHE calculation



Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Summary

Federated Machine Learning



Summary

	HE	SMPC	DP	FL	FL+DP	FL+HE	FL+SMPC
Accuracy	2	6	1	5	3	4	5
Computational efficiency	1	2	NA	6	5	3	4
Network communication efficiency	5	4	NA	3	3	2	1
Privacy of exchanged traffic	4	3	NA	1	2	4	3
Exchanging low sensitive traffic	✗	✗	NA	✓	✓	✓	✓
Privacy guarantee	✗	✗	✓	✗	✓	✗	✗

Comparison of Privacy Enhancing Techniques



a) All



b) HE



c) SMPC



d) DP



e) FL



f) FL+DP



g) FL+HE



h) FL+SMPC



Universität Hamburg

DER FACHSCHULE FÜR INFORMATIK

Synthetic Data (?)

- General concepts (<https://research.aimultiple.com/synthetic-data/>)
- Example Methods:
 - VAE (<https://towardsdatascience.com/understanding-variational-autoencoders-vaes-f70510919f73>)
 - GAN (<https://wiki.pathmind.com/generative-adversarial-network-gan>)

Sources

<https://arxiv.org/abs/2105.05734>

<https://arxiv.org/abs/2007.11621>

Inspired by CS208: Applied Privacy for Data Science – School of Engineering & Applied Sciences, Harvard University