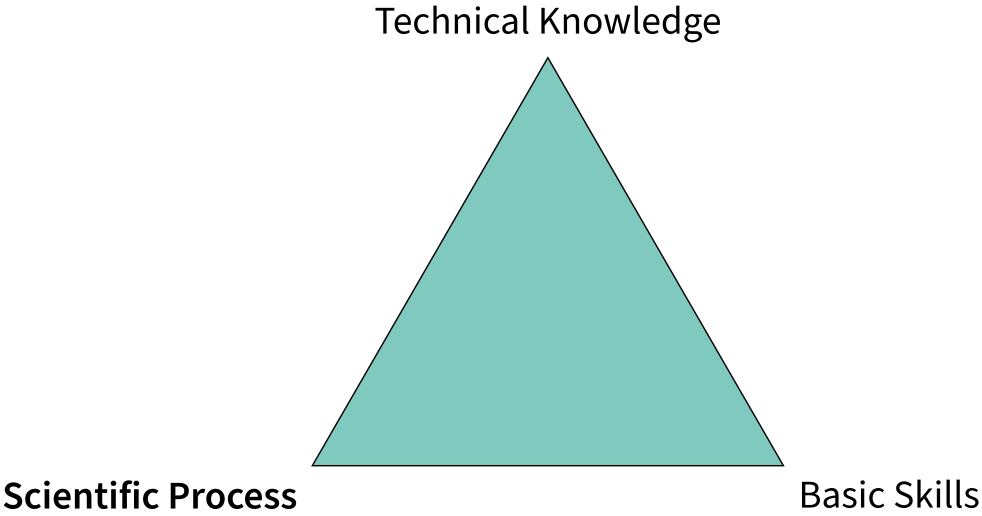
Karlsruhe Institute of Technology

# Privacy und Technischer Datenschutz
# Seminar SS2023
# Organisation & Topics

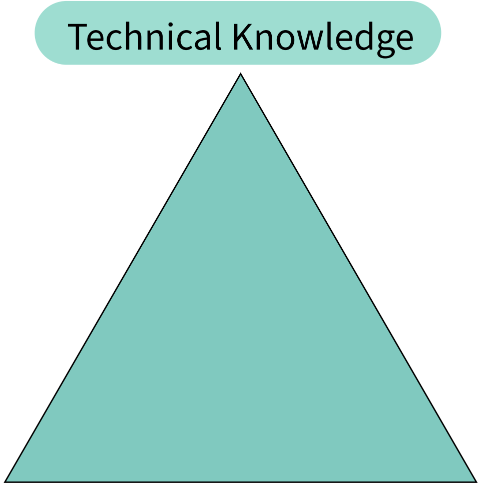
Patricia Guerra-Balboa

April 13, 2023

# Seminar goals



# Seminar goals

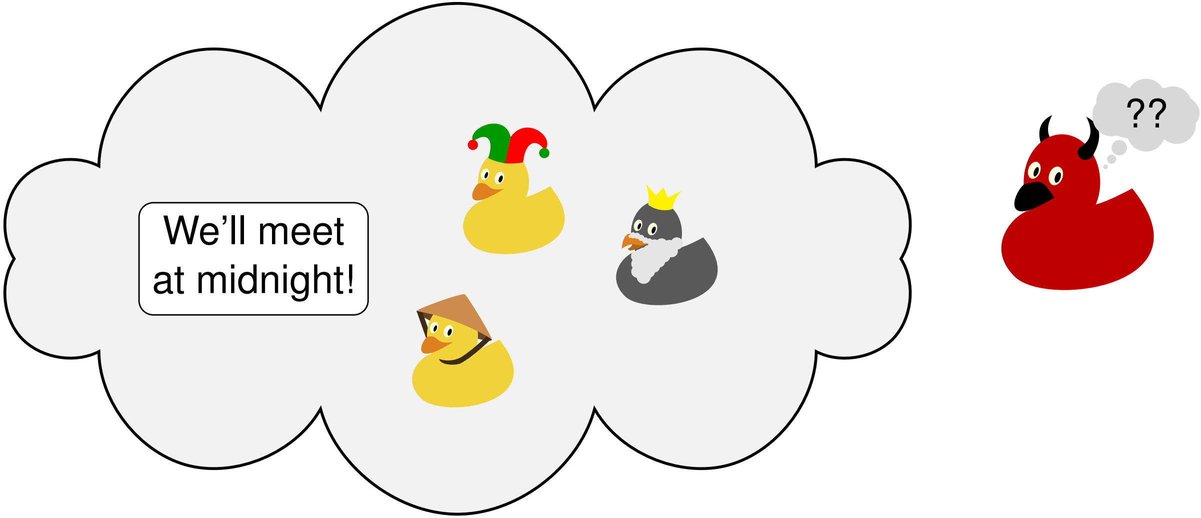


Technical Knowledge

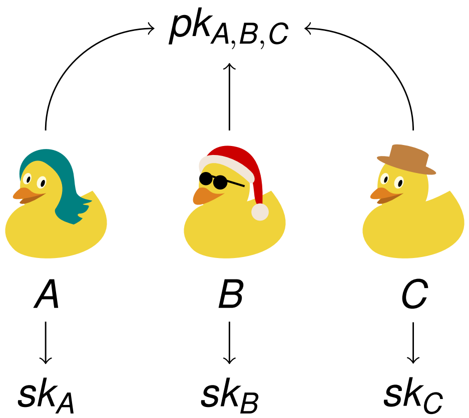
**Scientific Process**

Basic Skills

# Anonymous Communcation



# Topic 1: Distributed Key Generation (DKG)



- DKG allows group $A$, $B$, $C$ to collaboratively generate a key pair for their group.
- $pk_{A,B,C}$ represents all group members
- Each member has a share of the secret
- The entire secret $sk_{A,B,C}$ can only be reconstructed (e.g. for decryption) if all members participate.

# Topic 1: Distributed Key Generation

- DKG is very useful for anonymous communication (e.g., for threshold signature schemes)
- *To build anonymous communication protocols, we should understand the underlying building blocks!*

**Your Task**

Survey existing DKG approaches and categorize them, e.g., based on underlying assumptions, overhead, and additional functionality.

# Analyzing Riot Dynamics

Student protests in Hong Kong, 2014.
Source: [1]

Police arrest a man with a »No War« sign in Moscow, 2022.
Source: [2]

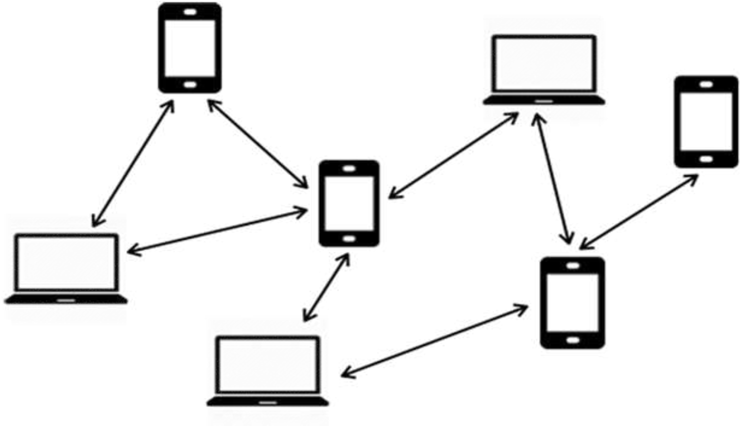
# Analyzing Riot Dynamics

- Our goals:
  - Create communication during protests *without central infrastructure*
  - Evaluate performance
  - Needs protesters' behavior

# Analyzing Riot Dynamics

- Our goals:
  - Create communication during protests *without central infrastructure*
  - Evaluate performance
  - Needs protesters' behavior
- This seminar:
  - Literature search for existing work (analysis, models, tools)
  - Summarize your findings
  - See for example [3, 4, 7, 9]

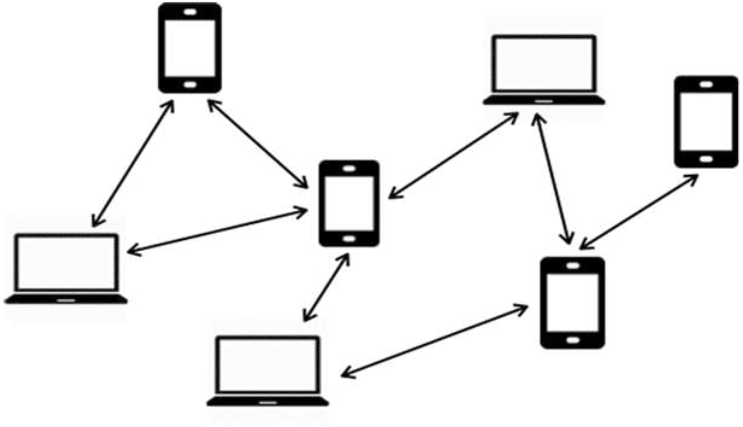
# A Survey of MANET Communication Approaches



Source: [5]

- »Mobile Ad-Hoc Network«
- Our goals:
  - Route information from device to device
  - Performance, security, anonymity in a protest

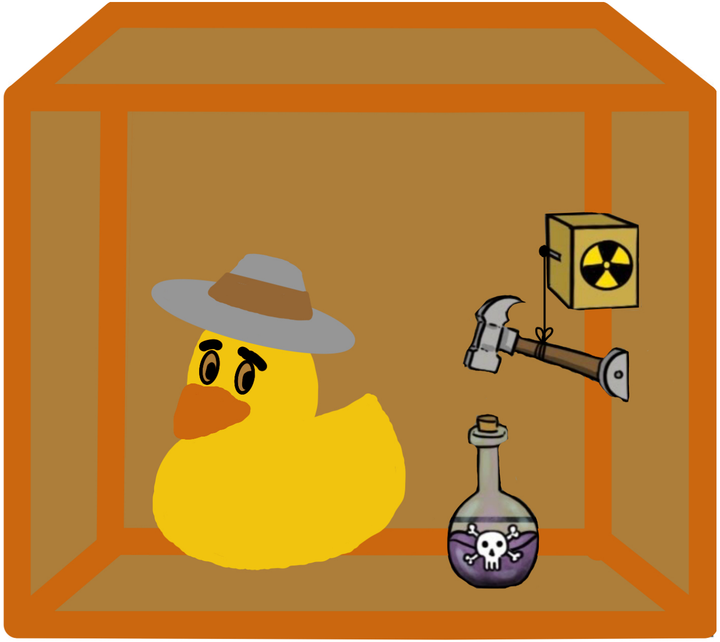
# A Survey of MANET Communication Approaches



Source: [5]

- »Mobile Ad-Hoc Network«
- Our goals:
  - Route information from device to device
  - Performance, security, anonymity in a protest
- This seminar:
  - Summarize existing approaches
  - Compare their (dis)advantages
  - See for example [6, 8, 10]

# Quantum Privacy



# Neighbouring Quantum States in QDP

- Neighbouring quantum states

- Quantum differential privacy

- Distinguishability measures:
  - Trace distance
  - Quantum fidelity
  - Quantum relative entropy

- Wasserstein distance

# Private Set Intersection

- PSI is a problem within the field of secure computation.

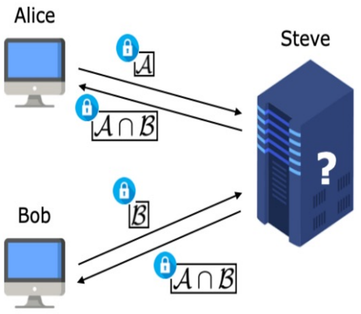
- Two-party PSI, hold a set of $m$ items:

  $A = \{a_1, \dots, a_m\}, B = \{b_1, \dots, b_m\}$

- The goal: obtain the intersection $A \cap B$.

- MPC

- Survey quantum approches


Alice
Steve
Bob
$\mathcal{A}$
$\mathcal{A} \cap \mathcal{B}$
$\mathcal{B}$
$\mathcal{A} \cap \mathcal{B}$
?

[3] Server-aided PSI

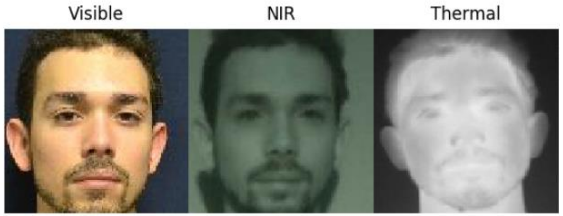
# Biometrics

*Topic:* *Supervisor: Julian Todt*

# A survey on privacy of ubiquitous EMR receivers

- EMR receivers are ubiquitous
- Privacy implications are known for some
  - Other receivers?

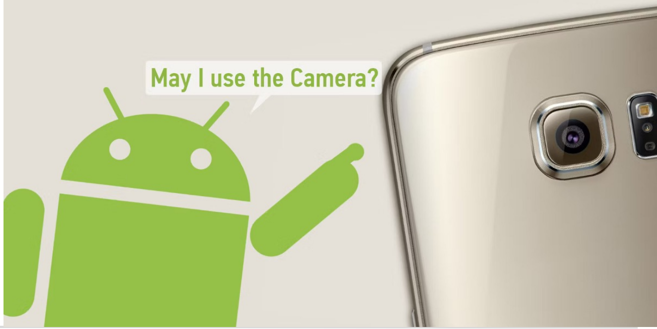
- Goal: Survey existing literature that analyses the privacy impact of EMR receivers



Anghelone, David, Cunjian Chen, Arun Ross, and Antitza Dantcheva. "Beyond the Visible: A Survey on Cross-Spectral Face Recognition."

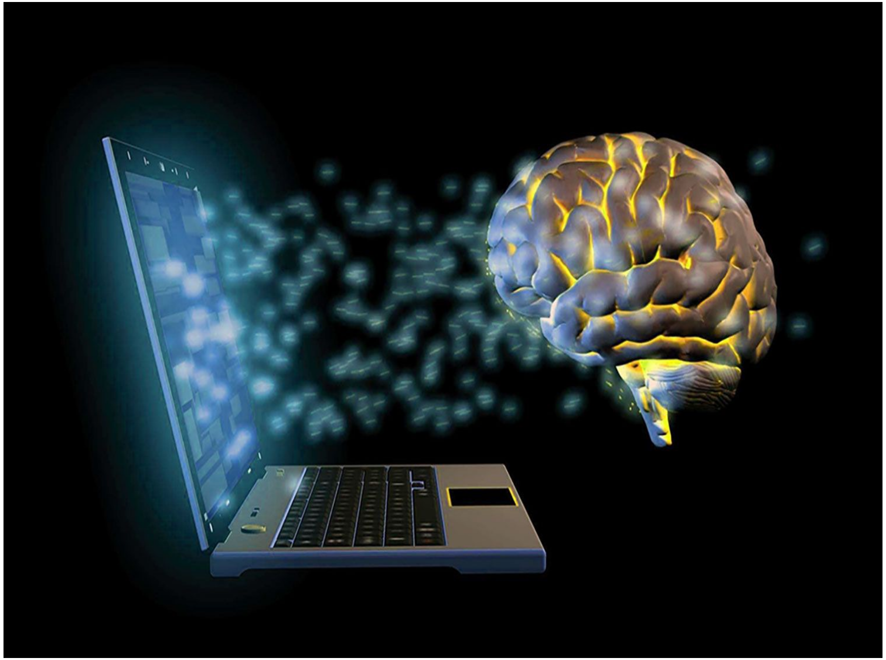
# Sensor Permission for AR & VR

- Augmented Reality (AR) and Virtual Reality (VR) capture a lot of data
- Existing permissions systems (e.g. as in Android, iOS) will fail to protect user privacy in AR/VR
- What are alternatives to design permission systems for sensors?
- How can we protect user privacy in AR/VR?

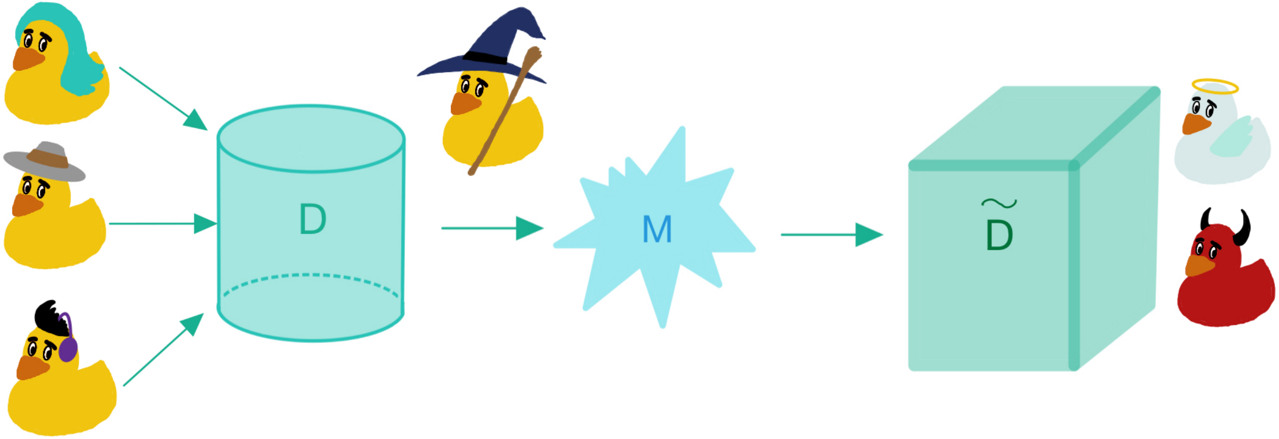


# Language Processing in the Brain

- Method?
- Limitations?

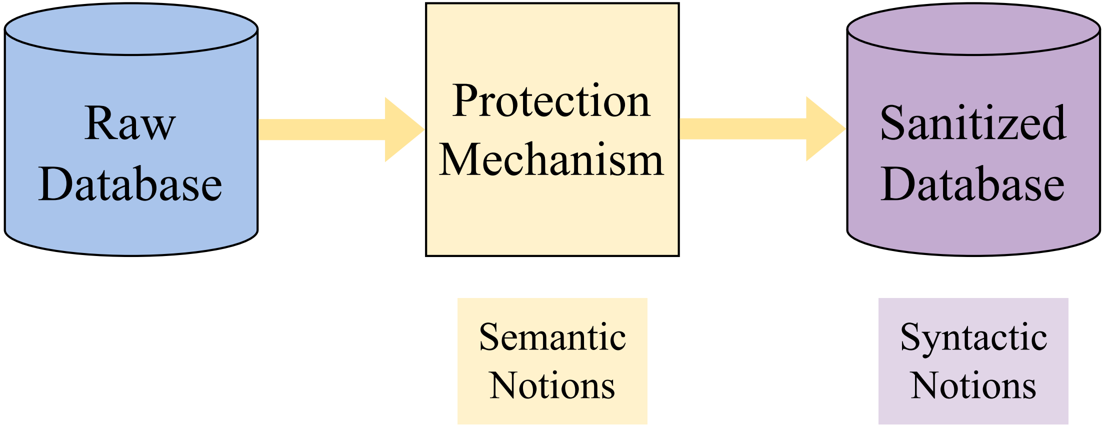


# Statistical Disclosure Control



# A Relationship Between Syntactic and Semantic Privacy

Àlex Miranda-Pascual



Raw Database

Protection Mechanism

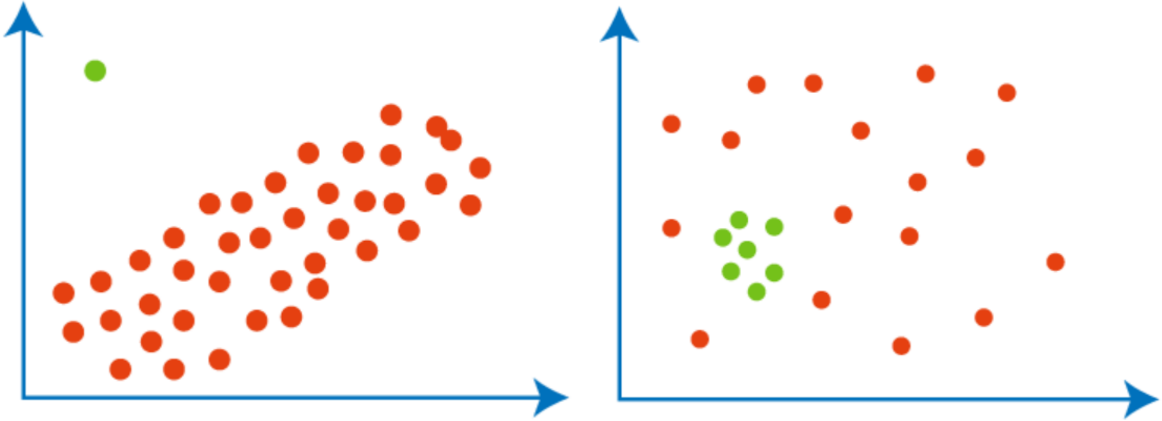
Sanitized Database

Semantic Notions

Syntactic Notions

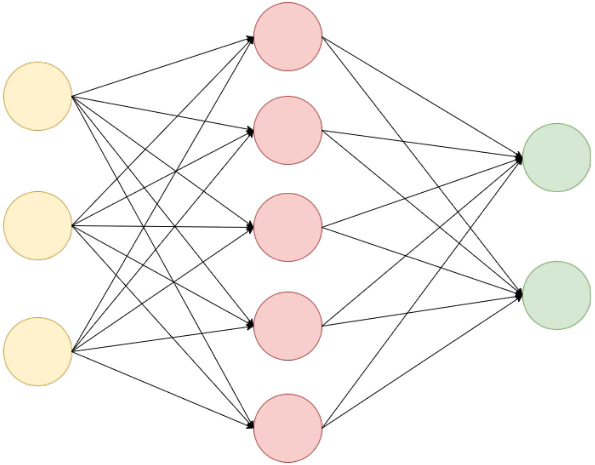
# Differentially Private Outlier Detection

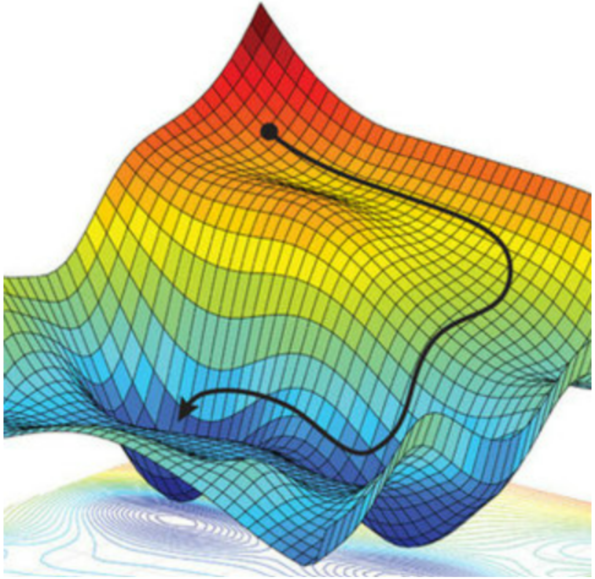
Àlex Miranda-Pascual



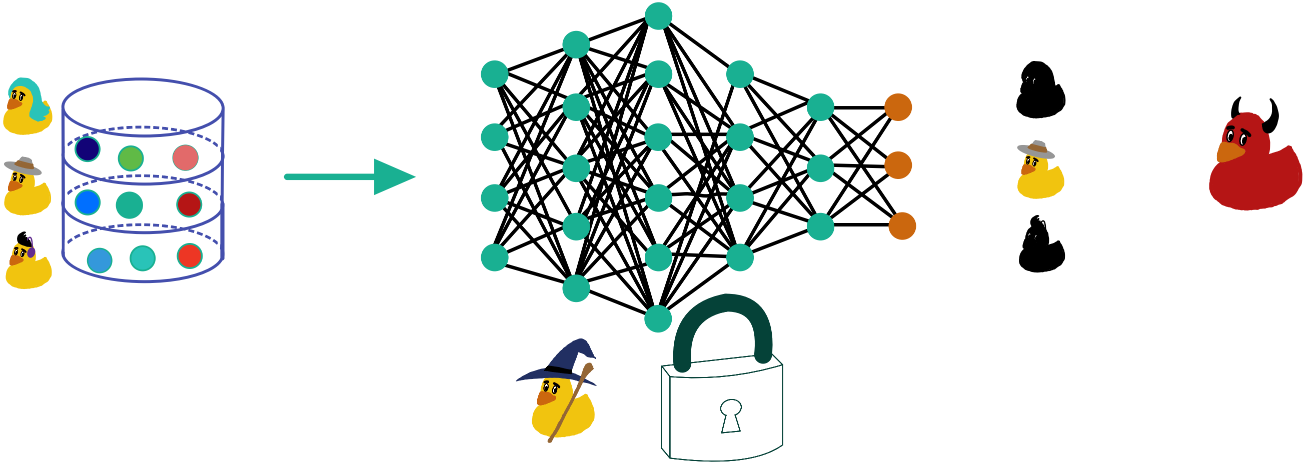
# An Introduction to DP Stochastic Gradient Descent

Àlex Miranda-Pascual





# Topic 1: Correlation framework in DP



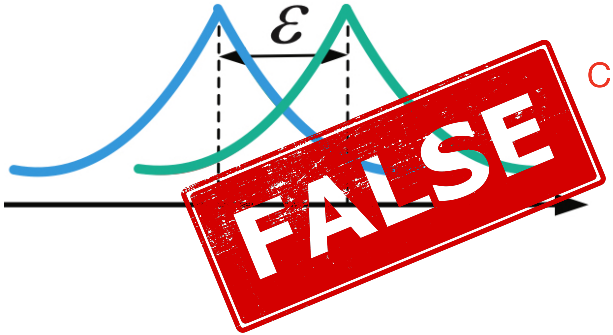
# Topic 1: Correlation framework in DP

**Privacy Loss (by observing r)**

$$\mathcal{L}^{r}_{M(D)||M(D')} = ln\left(\frac{\mathbb{P}(M(D)=r)}{\mathbb{P}(M(D')=r)}\right) \le \varepsilon$$

FALSE

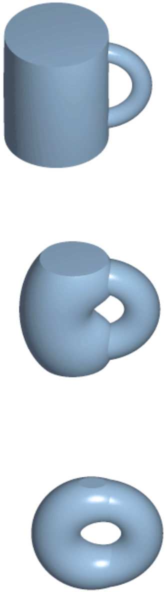
BREAKING NEWS



FALSE

CORRELATED DATABASE

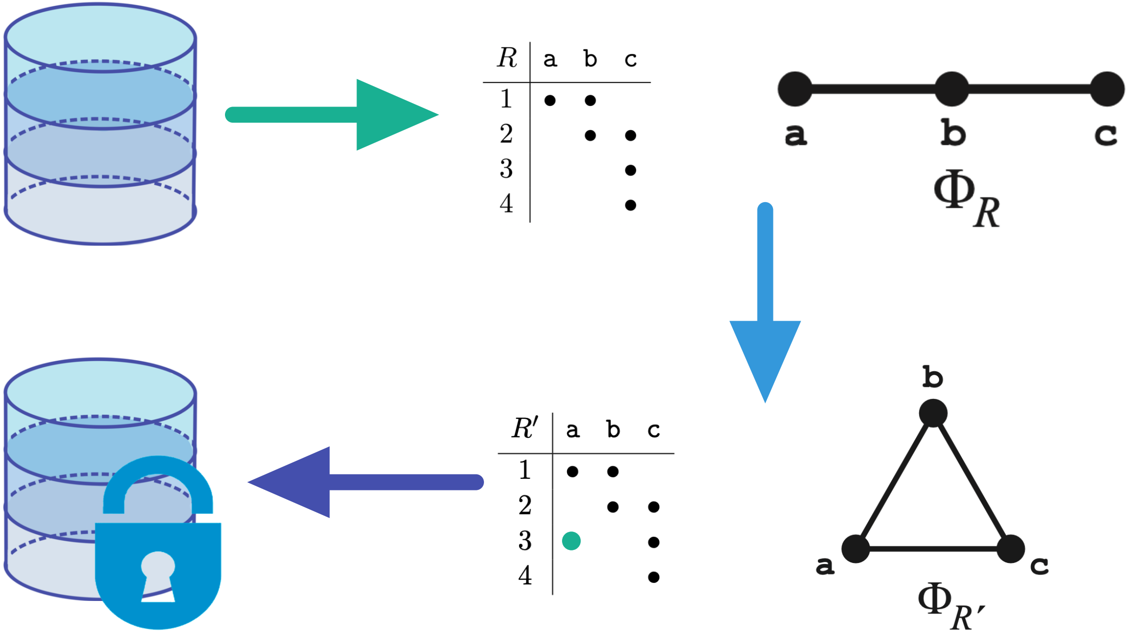
# Topic 2: Topology of Privacy



**In mathematics:**

topology = geometric properties

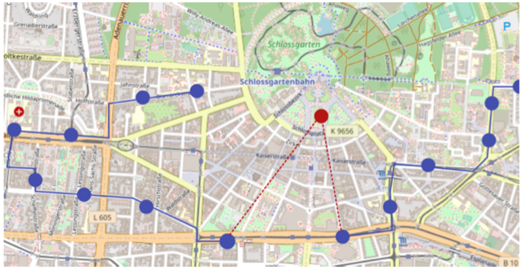
# Topic 2: Topology of Privacy

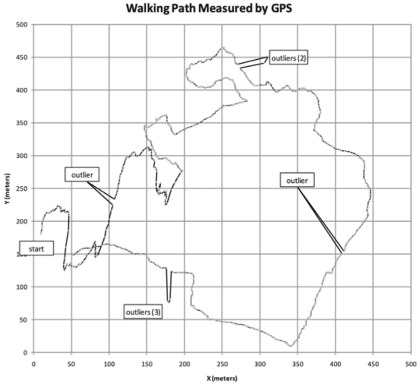


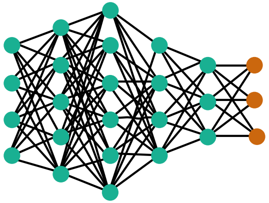
| $R$ | a | b | c |
|---|---|---|---|
| 1 | ● | ● | |
| 2 | | ● | ● |
| 3 | | | ● |
| 4 | | | ● |

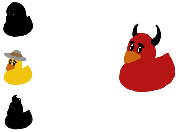
| $R'$ | a | b | c |
|---|---|---|---|
| 1 | ● | ● | |
| 2 | | ● | ● |
| 3 | ● | | ● |
| 4 | | | ● |

# Topic 3: Correlation-based Attacks



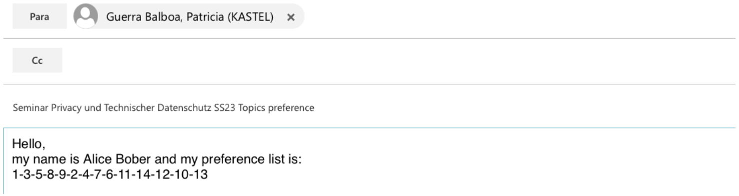






# Topic Preferences list

- Send a list by mail to: `patricia.balboa@kit.edu`
- Deadline: 23.04.2023
- The mail should include:
  - Your complete name
  - The name of the seminar
  - A list of topic numbers ordered by preference (first been your first option an so on)



Para: Guerra Balboa, Patricia (KASTEL)

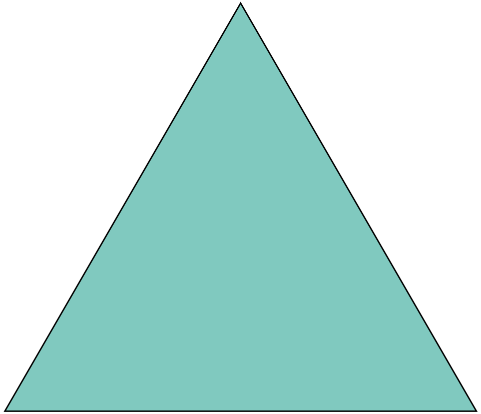
Cc:

Seminar Privacy und Technischer Datenschutz SS23 Topics preference

Hello,
my name is Alice Bober and my preference list is:
1-3-5-8-9-2-4-7-6-11-14-12-10-13

**Figure 1:** Numbers can be checked in our web page `https://ps.tm.kit.edu/139_814.php`

# Seminar goals



Technical Knowledge

**Scientific Process**

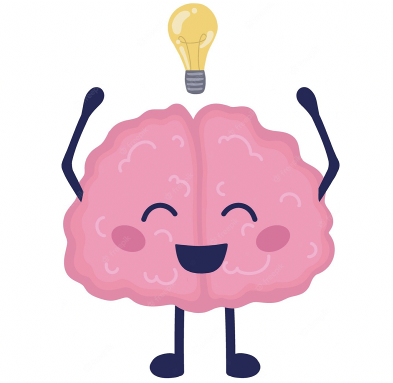
Basic Skills

# About scientific conferences

1. Pick topic
2. Make a contribution
3. Write and submit a paper
4. Get reviews from peers
5. Revise paper (and get accepted)
6. Present contribution at the conference

# About scientific conferences

1. Pick topic
2. Make a contribution
3. Write and submit a paper
4. Get reviews from peers
5. Revise paper (and get accepted)
6. Present contribution at the conference



# About scientific conferences

1. Pick topic
2. Make a contribution
3. Write and submit a paper
4. Get reviews from peers
5. Revise paper (and get accepted)
6. Present contribution at the conference

# About scientific conferences

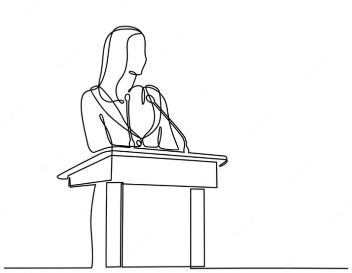
1. Pick topic
2. Make a contribution
3. Write and submit a paper
4. Get reviews from peers
5. Revise paper (and get accepted)
6. Present contribution at the conference

# About scientific conferences

1. Pick topic
2. Make a contribution
3. Write and submit a paper
4. Get reviews from peers
5. Revise paper (and get accepted)
6. Present contribution at the conference

# About scientific conferences

1. Pick topic
2. Make a contribution
3. Write and submit a paper
4. Get reviews from peers
5. Revise paper (and get accepted)
6. Present contribution at the conference



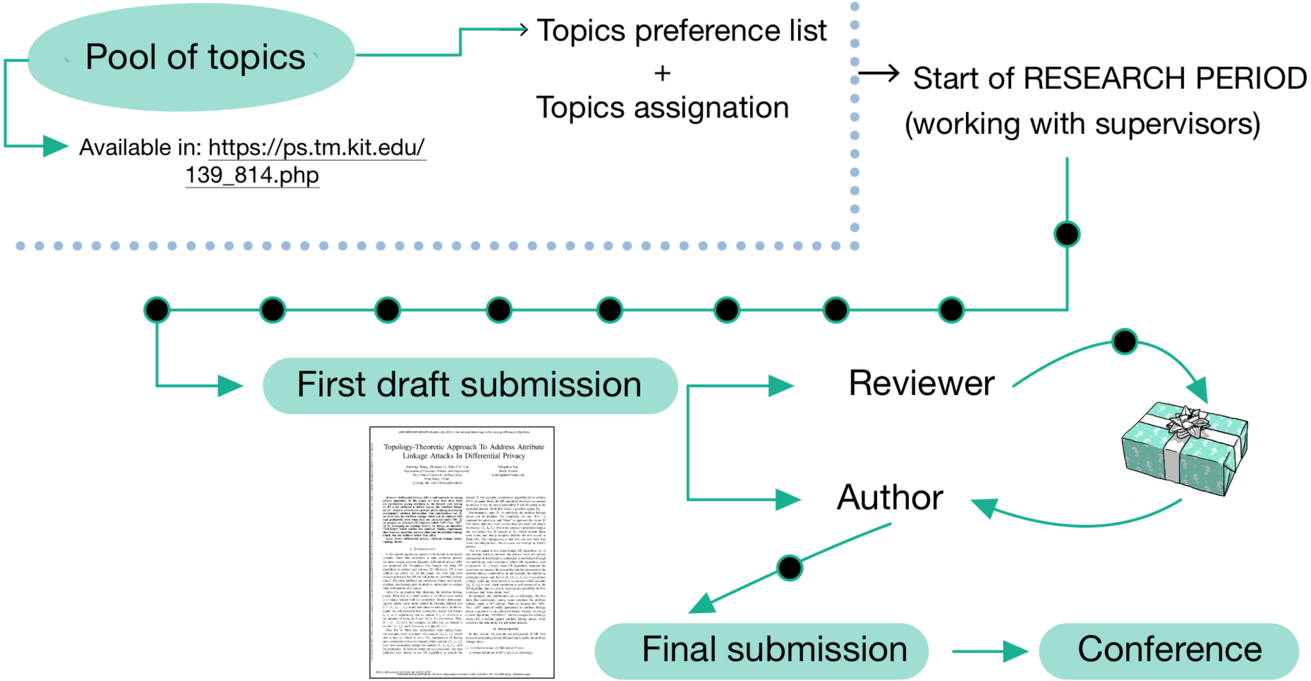
# Our scientific conference

1. Pick topic ( Choose from our selection )
2. Make a contribution: Find and read literature on your topic. Understand and analyze! Be critical! Obtain results!
3. Write and submit a paper. Think about structure, writing style. . .
4. Get reviews from peers Review other students’ work
5. Revise paper (and get accepted)
6. Present contribution at the conference

# Our scientific conference

1. Pick topic ( Choose from our selection )
2. Make a contribution: Find and read literature on your topic. Understand and analyze! Be critical! Obtain results! ? → Slide 10
3. Write and submit a paper. Think about structure, writing style…
4. Get reviews from peers Review other students' work
5. Revise paper (and get accepted)
6. Present contribution at the conference

# Seminar Structure



Pool of topics

Available in: https://ps.tm.kit.edu/139_814.php

Topics preference list
+
Topics assignation

Start of RESEARCH PERIOD
(working with supervisors)

First draft submission

Topology-Theoretic Approach To Address Attribute Linkage Attacks In Differential Privacy

Reviewer

Author

Final submission

Conference

# Your Paper

- English
- No template
- No required number of pages (typically something between 6-10 pages)

**Possible contributions:**

systematization and comparison of existing results, discover flaws in existing works, suggest and argue ideas for new solutions or research directions and more…

# Submitting and Reviewing

**Figure 1:** Web-based conference management system (EasyChair)

- Register: 2 roles (you can switch between). Author and Program Committee Member (after you accept our invitation).
- Submit (author role) via: `https://easychair.org/conferences/?conf=ptd23`
- Review (PC member role): Access to papers via EasyChair.
- Submitting reviews via EasyChair ("Reviews" → "My papers" → “Add review”)

# Giving & Receiving Feedback

**Giving:**

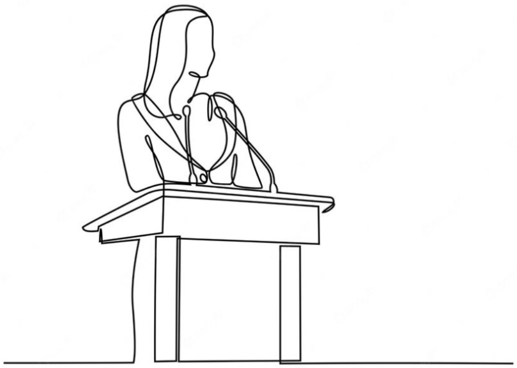
You will review 2 papers

**Receiving**

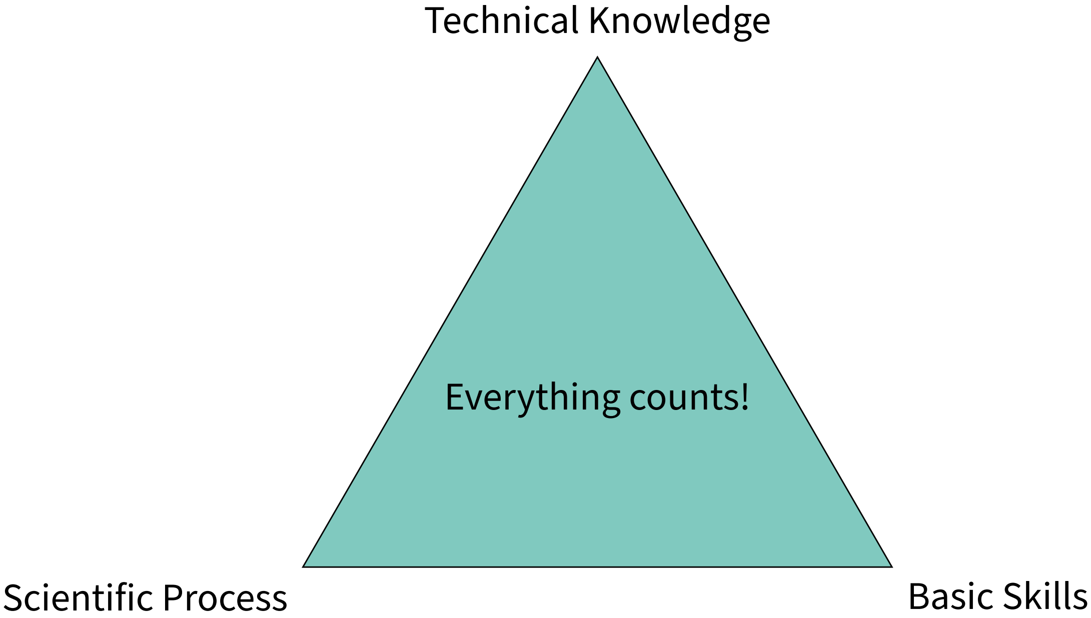
You will receive 3 reviews

# Presentations

- English with slides
- 20 or 30 minutes of presentation (depends on the number of participants)
- 10 or 15 minutes of discussion (depends on the number of participants)
- Participate actively in the discussion of other topics



# Evaluation & Grades



Technical Knowledge

Everything counts!

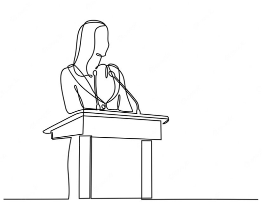
Scientific Process

Basic Skills

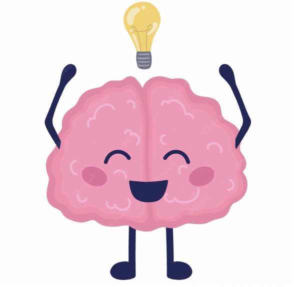
# Evaluation & Grades

$X_1$ = written paper

$X_2$ = Reviews



$X_3$ = Presentation



$X_4$ = Participation in the Q&A

**Final Grade:**

$$0.4 * X_1 + 0.3 * X_3 + 0.2 * X_2 + 0.1 * X_4$$

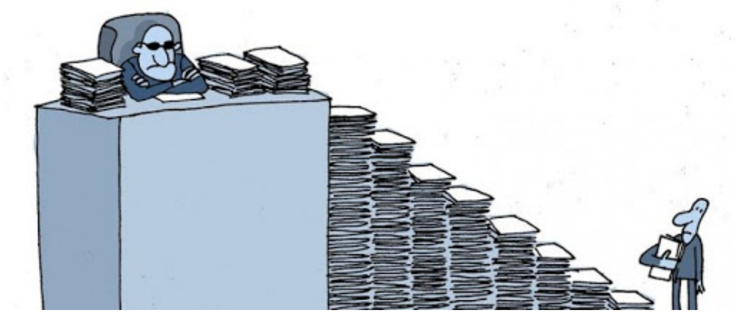
# Timeplan

| Date | Milestone |
|---|---|
| 18.4.2023 | Topic presentation |
| 25.4.2023 | Basic Skills |
| 23.4.2023 | Topic preferences due |
| 24.4.2023 | Topic assignment (contact your mentor!) |
| 25.6.2023 | Paper submission deadline |
| 02.7.2023 | Reviews deadline |
| 09.7.2023 | Revised paper deadline |
| ∼17.7.2023 | Presentation at our conference |

**Table 1:** Timeplan updates in our webpage `https://ps.tm.kit.edu/139_814.php`

# Bureaucracy

- Always inform if you decide to drop out!
- The deadline for abandoning the seminar is 25.6.2023. After this date, you will start to be evaluated and therefore it is not possible to quit.
- In case of problems with the campus system contact our secretary: hildegard.sauer@kit.edu

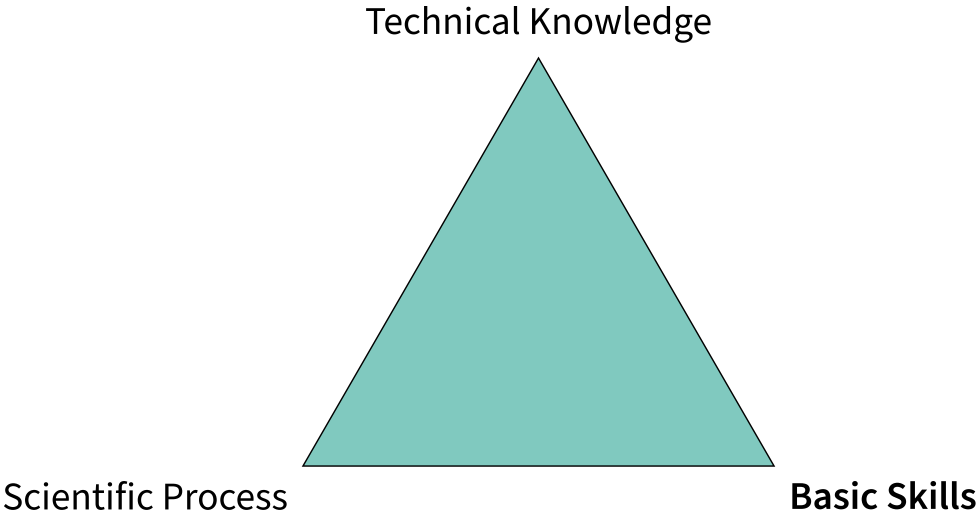


# Getting information

- **Organization:**
  - These slides
  - Email: patricia.balboa@kit.edu
  - Course website `https://ps.tm.kit.edu/139_814.php`

- **Topic:**
  - Course website `https://ps.tm.kit.edu/139_814.php`
  - Email to potential supervisors: `https://ps.tm.kit.edu/english/21.php`

# Seminar Goals



Technical Knowledge

Scientific Process

**Basic Skills**