Karlsruhe Institute of Technology

Seminar on Privacy & Security

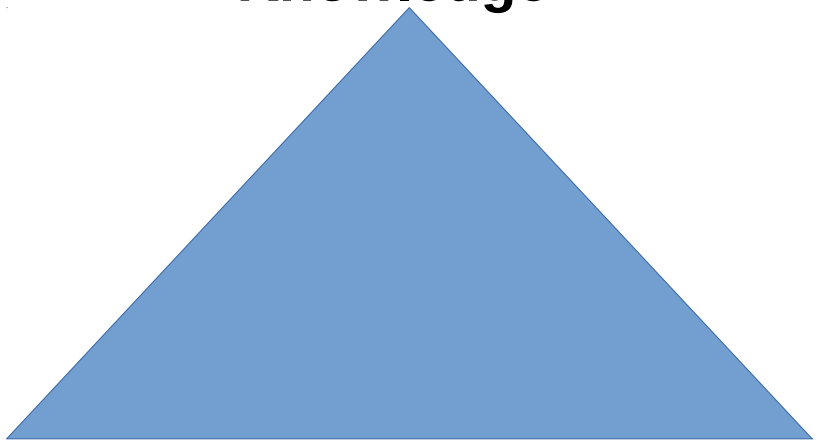
A conference style seminar

Patricia Guerra-Balboa <patricia.balboa@kit.edu>,
Christiane Kuhn <christiane.kuhn@kit.edu>

Helmholtz Center for Applied Security Technology

Seminar goals

Technical Knowledge



Scientific Process

Basic Skills (read, write, present)

#1 Correlation framework in DP
#2 Topology of privacy

Supervisor: Patricia Guerra-Balboa

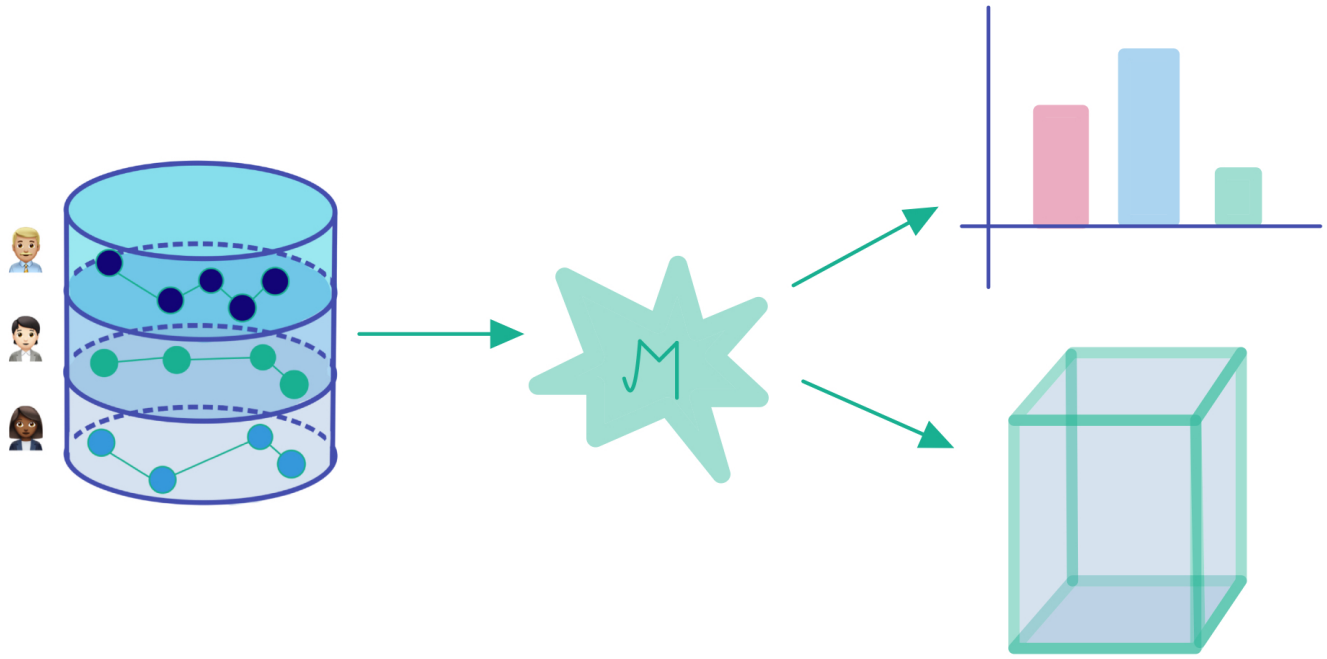
Karlsruhe Institute of Technology

Privacy and Security Seminar WS 2022/23

Patricia Guerra-Balboa

October 24, 2022

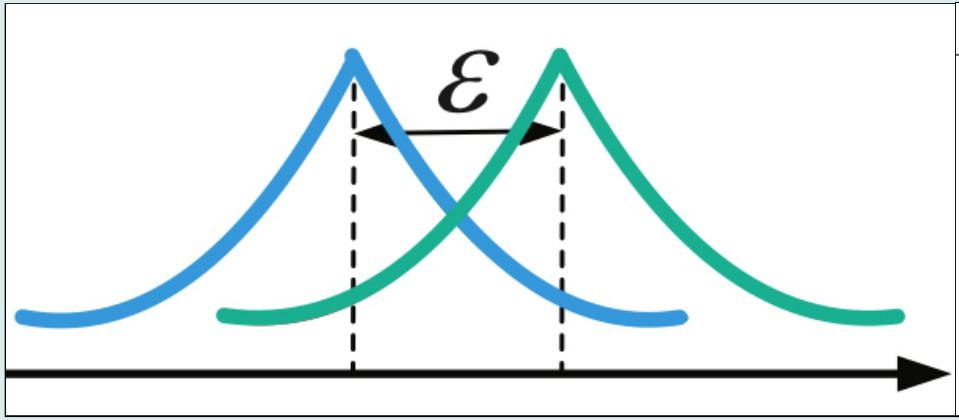
Statistical Disclosure Control



Proposed topics

topics

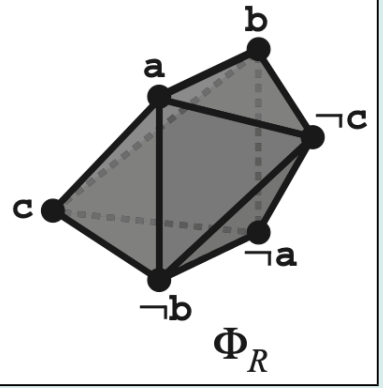
Semantic notions



Correlation framework in DP

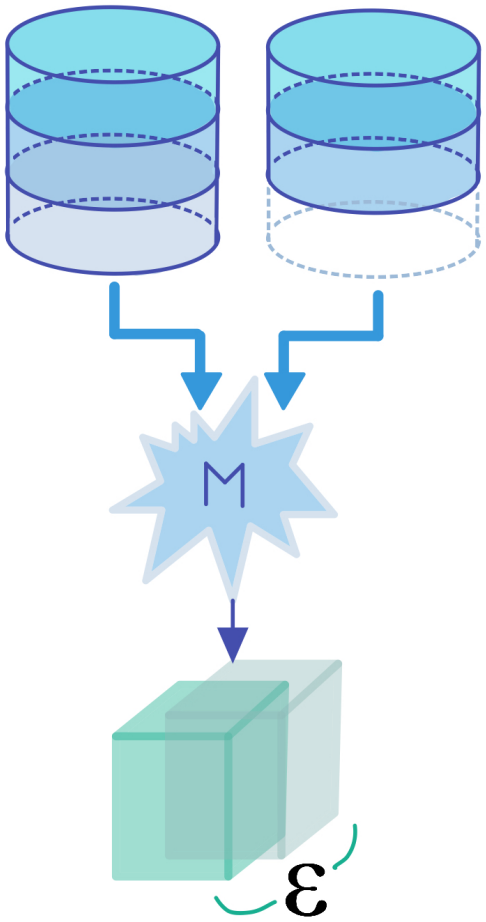
Syntactic notions

R	a	¬a	b	¬b	c	¬c
1	•		•		•	
2	•		•			•
3	•			•	•	
4	•			•		•
5		•	•		•	
6		•	•			•
7		•		•	•	
8		•		•		•



Topology of privacy

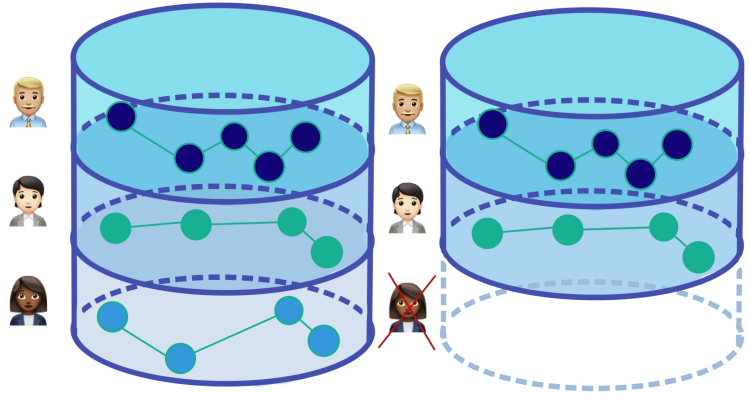
Topic 1: Correlation framework in DP



ε-Differential Privacy

A randomized algorithm M is said to be ε-*differentially private* if for all *neighboring* databases D, D' and all $\mathcal{S} \subseteq Range(M)$,

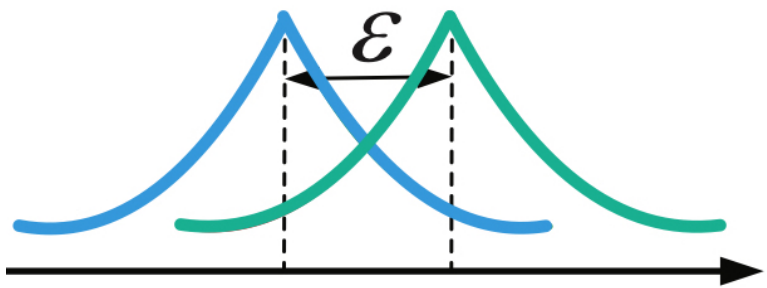
$$\mathbb{P}\{M(D) \in \mathcal{S}\} \leq e^{\varepsilon}\, \mathbb{P}\{M(D') \in \mathcal{S}\}.$$



Topic 1: Correlation framework in DP

Privacy Loss (by observing r)

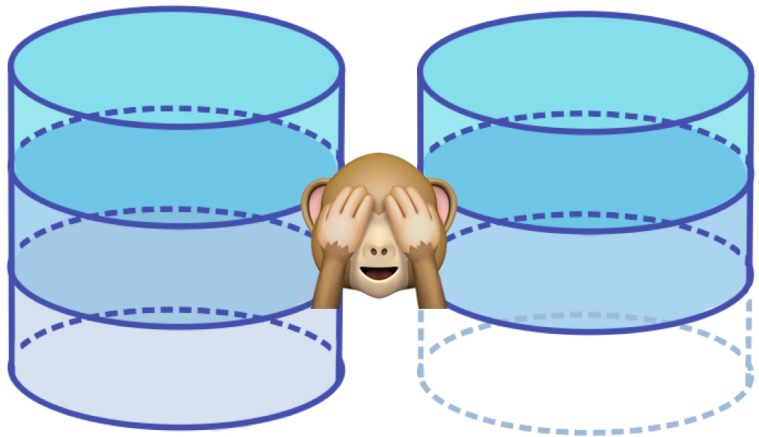
$$\mathcal{L}^{r}_{M(D)||M(D')} = ln\left(\frac{\mathbb{P}(M(D)=r)}{\mathbb{P}(M(D')=r)}\right) \leq \varepsilon$$



Topic 1: Correlation framework in DP

Privacy Loss (by observing r)

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



Topic 1: Correlation framework in DP

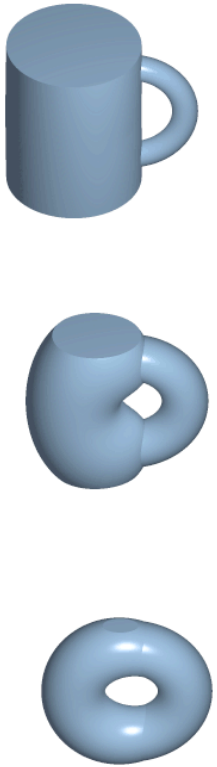
Privacy Loss (by observing r)

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

FALSE

CORRELATED DATABASE

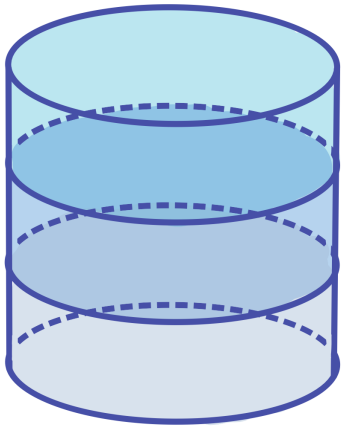
Topic 2: Topology of Privacy



In mathematics:

topology = geometric properties

Topic 2: Topology of Privacy



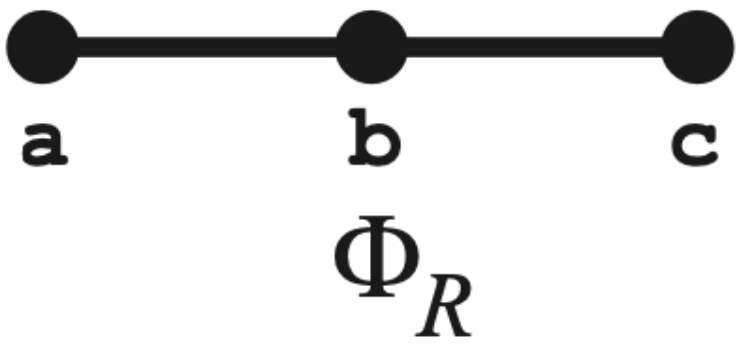
H	SMOKES	HAS_CANCER	DRINKS_SODA
👨🏼‍💼	●	●	
👩🏻‍💼		●	●
👩🏾			●
👩🏽‍🔬			●

Topic 2: Topology of Privacy

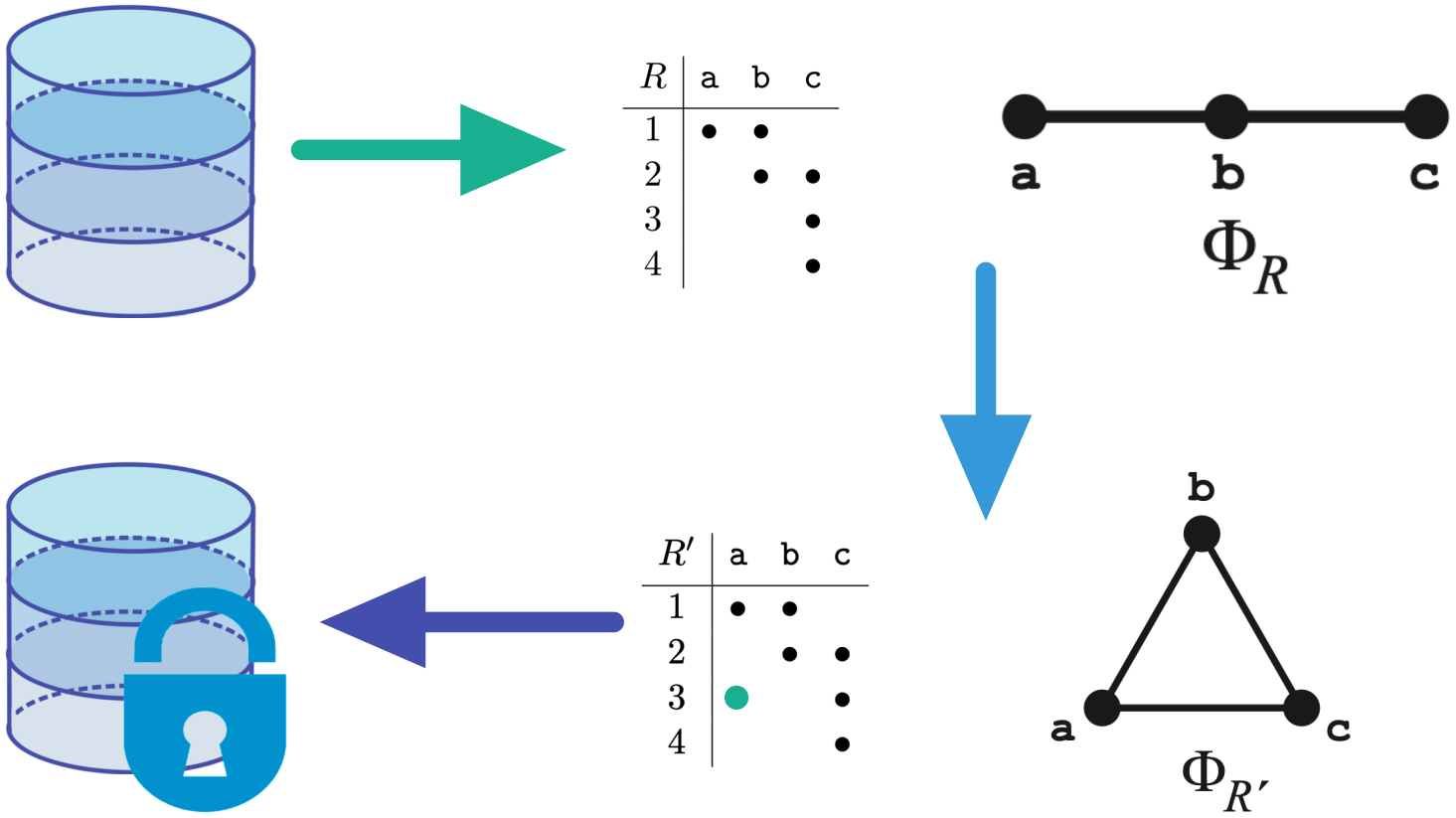
R	a	b	c
1	●	●	
2		●	●
3			●
4			●

Topic 2: Topology of Privacy

R	a	b	c
1	•	•	
2		•	•
3			•
4			•



Topic 2: Topology of Privacy



#3 Inference Attacks on Machine Learning Models using Auxiliary Knowledge

Supervisor: Felix Morsbach

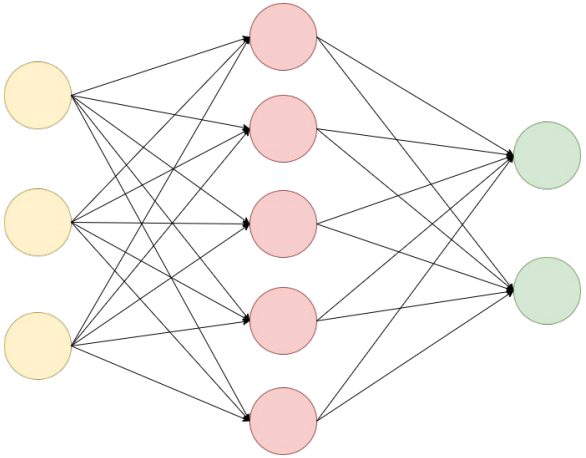
Inference Attacks on Machine Learning Models using Auxiliary Knowledge (1/2)

Motivation

- Training machine learning (ML) models can entail privacy risks as (information about) the training data can be inferred from a trained model

- Other privacy attacks often utilize auxiliary data. For example, the de-anonymization of the Netflix Prize dataset incorporated public IMDB profiles

- However, the most **prominent** attacks on ML models don't incorporate such auxiliary knowledge into their attacks



Inference Attacks on Machine Learning Models using Auxiliary Knowledge (2/2)

Aims & Objectives

- Survey the existing literature on inference attacks on ML models and analyze their (potential) use of auxiliary knowledge

- Identify and discuss knowledge sources that (could) function as auxiliary knowledge. For example, this knowledge could either be related to the training data itself (e.g., data distributions) or be about the ML algorithm's configuration (e.g., hyperparameter values or a hyperparameter optimization history)

- (Possibly) propose promising avenues for (improving) inference attacks on ML models that utilize auxiliary knowledge

Karlsruhe Institute of Technology

KASTEL

#4 A relation between syntactic and semantic privacy notions
#5 Measuring similarity of trajectories using learning methods
#6 How to adapt trajectory data into road networks

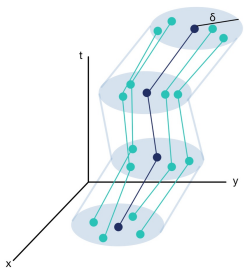
Supervisor: Alex Miranda Pascual

A relation between syntactic and semantic privacy notions

Àlex Miranda-Pascual

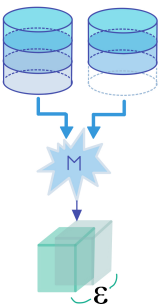
Syntactic Notions

t-closeness



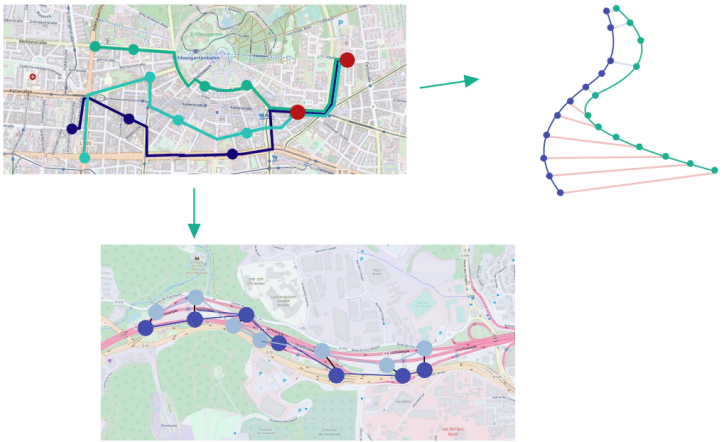
Semantic Notions

ϵ-differential privacy



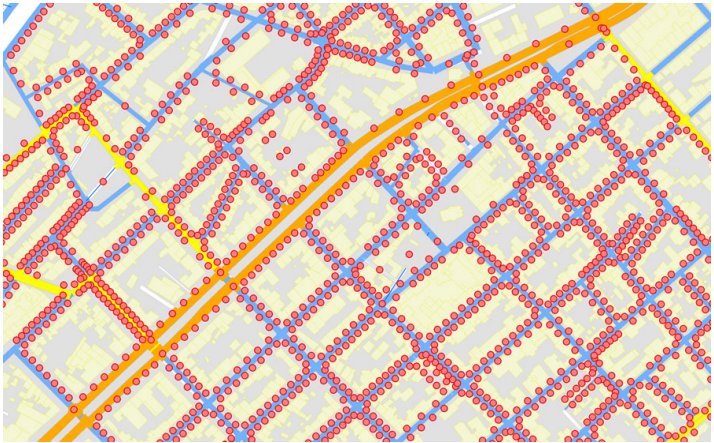
Measuring similarity of trajectories using learning methods

Àlex Miranda-Pascual



How to adapt trajectory data into road networks

Àlex Miranda-Pascual



Karlsruhe Institute of Technology

KASTEL

#7 Anonymous Key Exchange

Supervisor: Christoph Coijanovic + Marcel Tiepelt

Topic 7: Anonymous Key Exchange

- Encrypted communication needs key exchange
- **But**: Key exchange discloses link between communication partners

To achieve anonymous *communication*, key exchange also needs to be anonymous!

Topic 7: Anonymous Key Exchange

- There are anonymous key exchange protocols for many settings:
  - Instant Messaging
  - Smart Grids
  - Vehicular Networks
  - Quantum Networks
- **Missing**: Overview and systemization of all these approaches.

Your Task

Survey the existing approaches for anonymous key exchange. Analyze and categorize each approach based on its notion of anonymity, adversary model, provided functionality, etc.

Karlsruhe Institute of Technology

KASTEL

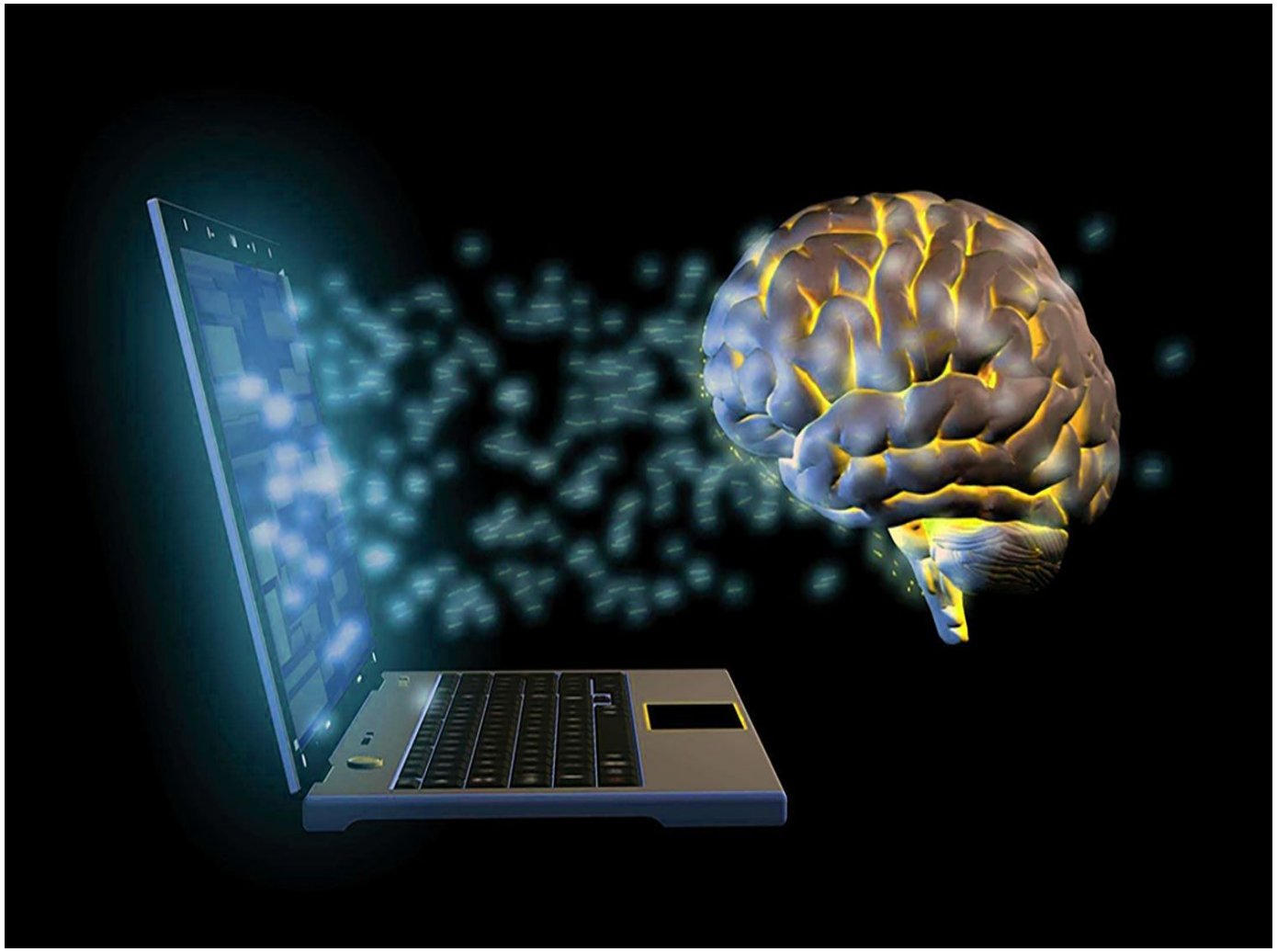
#8 A survey on brainwaves computer interface (BCI)
#9 Privacy-preserving biometric authentication(PPBA): third-party approach
#10 Explainable machine learning for brainwaves

Supervisor: Matin Fallahi

Survey on Brainwaves Computer Interface(BCI)

Karlsruhe Institute of Technology

- Applications of BCI
- Data acquisition protocols



KASTEL

Privacy-Preserving Biometric Authentication(PPBA)

- Third-party approach in PPBA
- How homomorphic encryption can be use in biometrics with high variability?

Explainable machine learning for brainwaves

- Explainable AI for EEG in general
- Explainable AI for EEG for recognition , in particular

#11 A survey on privacy of ubiquitous EMR receivers
#12 A survey on video anonymization

Supervisor: Julian Todt

Topic 11: *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."

Topic 12: *Supervisor: Julian Todt*

A survey on video anonymization

- Significant research on anonymization for images
- More and more data are videos
  - Additional challenges?

- Goal: Survey anonymization methods for video

bauta.io


brighter.ai

#13 Modelling and Synthesizing Human Motion

Supervisor: Simon Hanisch

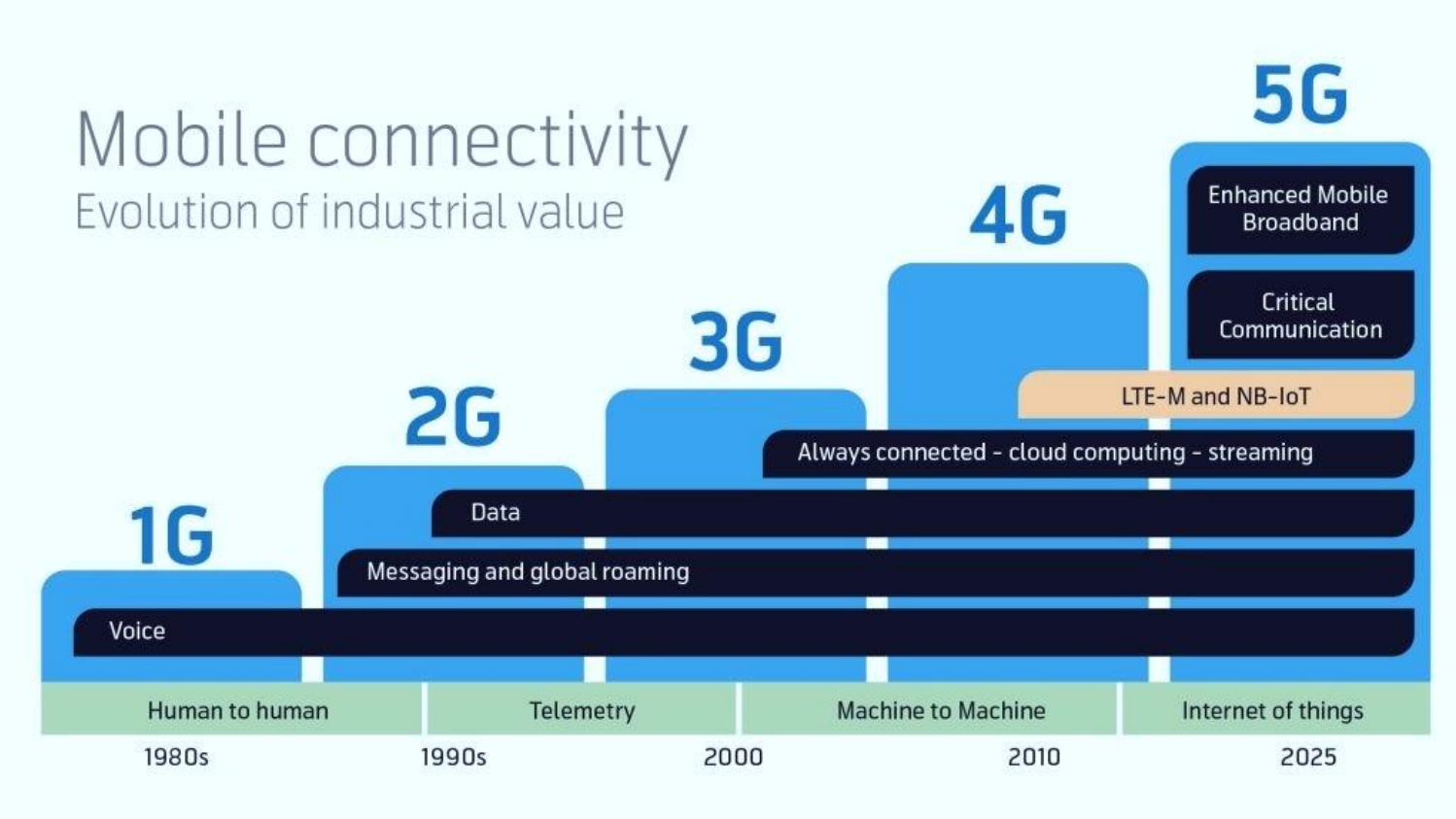
Modelling and Synthesizing Human Motion

- How to generate new human motions?
- What approaches exist?
- What models of human physiology can be used?

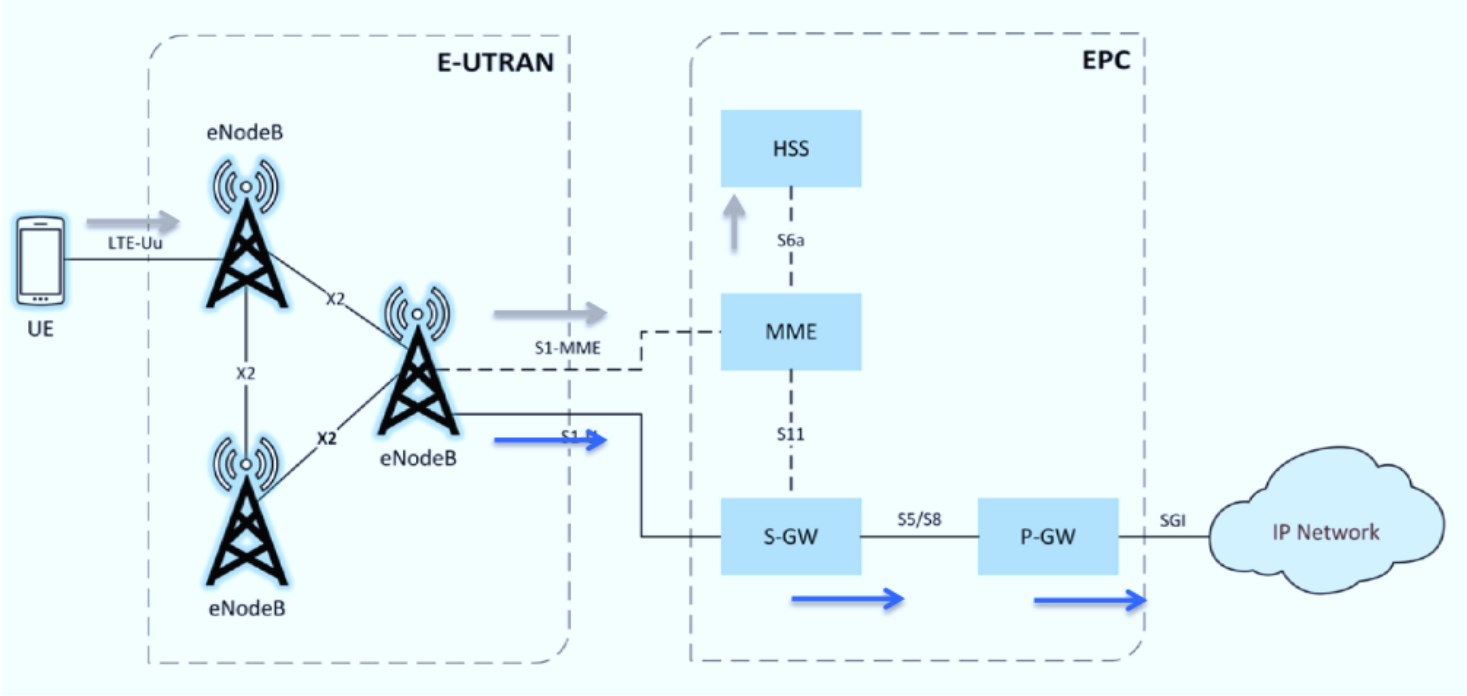
#14 Survey on 5G Security and beyond

Supervisor: Kamyar Abedi

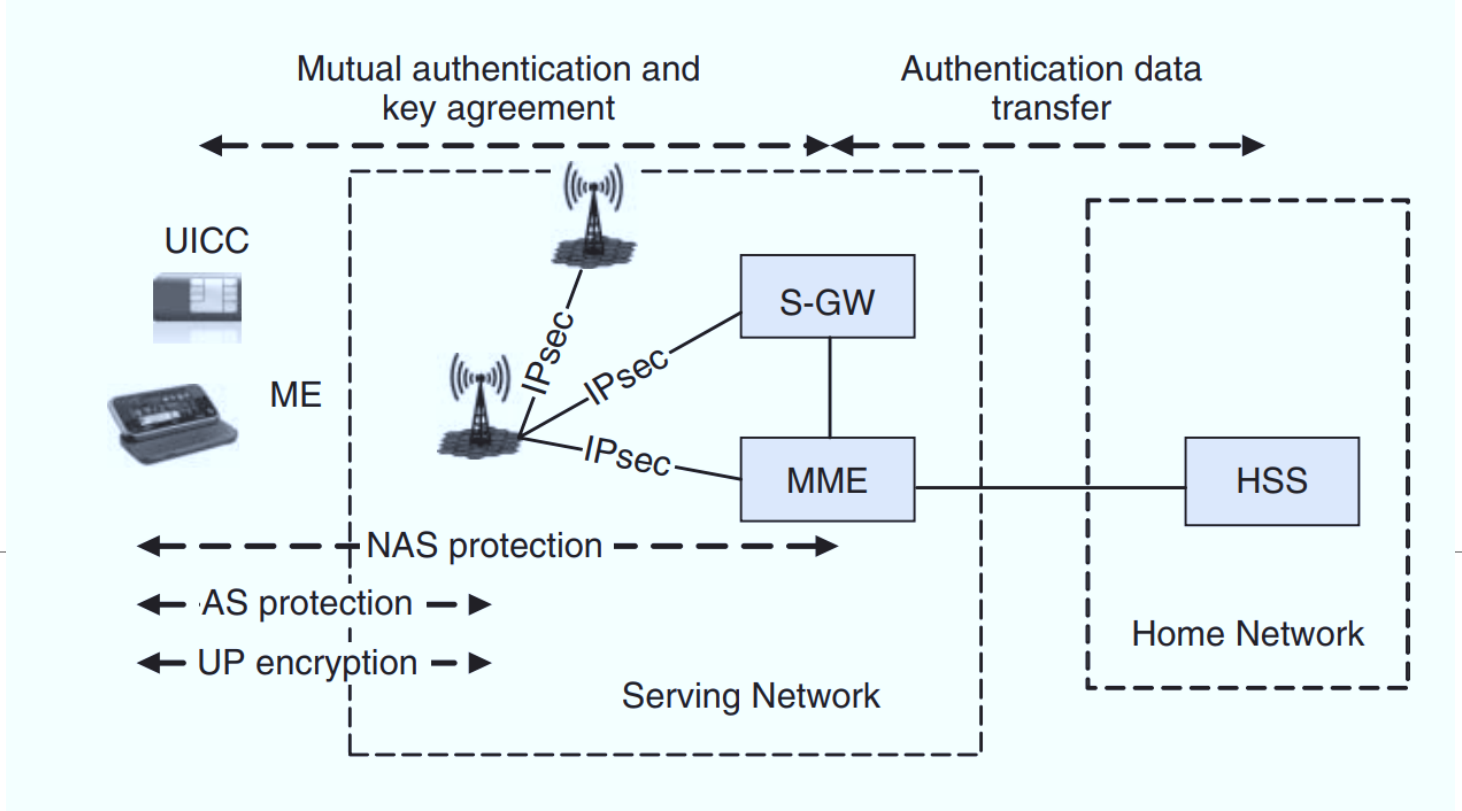
Mobile Network Evolution



LTE Network Architect

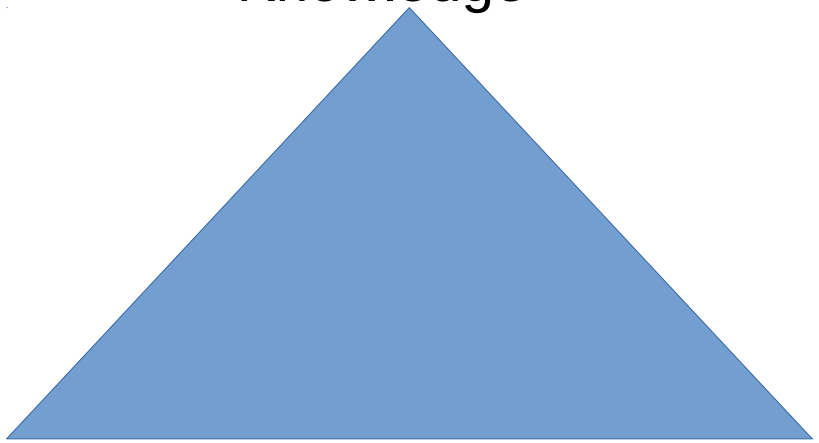


LTE Security Architect



Seminar goals

Technical Knowledge



Scientific Process

Basic Skills (read, write, present)

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 conference

Our conference

1) Pick topic
   - Choose from our selection
2) Make a contribution
   - Find and read literature to your topic
     (first references on our website)
   - Understand, compare, analyze! Be critical!
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 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

- Web-based conference management system (EasyChair)

- Register: 2 roles (you can switch between)
  - Author
  - Program Commitee Member (after you accept our invitation)
- Submit (author role)

  Via EasyChair (will be shared in time)
- Review (PC member role)
  - Access to papers via EasyChair
  - Submitting reviews via EasyChair ("Reviews" → "My papers" → “Add review”)

Giving and Receiving Feedback

Explicit: What's done above average
what's done below average

Common goal: improve each work as much as possible and learn the most

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

Timeplan

Date	Milestone
October 25	Topic presentation
November 1	**Topic preferences due**
November 4	Topic assignment **(contact your mentor!)**
November 8	Basic Skills
January 22	**Paper submission deadline**
January 29	**Reviews deadline**
February 5	**Revised paper deadline**
TBD (~February 13)	**Presentation at our conference**

Grade

Includes performance on every part of the seminar:

Written paper + reviews + way of working with supervisor etc.: X
Presentation + participation in discussion etc.: Y

Final grade: 2/3 X + 1/3 Y

Getting Information

- Organization:
  - These slides
  - Email
  - Course website: https://ps.tm.kit.edu/139_602.php
  - Course coordinator: christiane.kuhn@kit.edu, patricia.balboa@kit.edu
- Topic:
  - Overview follows
  - Specific: your supervisor
    https://ps.tm.kit.edu/members.php, https://crypto.iti.kit.edu/staff.php

Topic Overview

	Topic	Supervisor
1	Correlation framework in DP	Patricia Guerra-Balboa
2	Topology of privacy	Patricia Guerra-Balboa
3	Inference Attacks on ML Models using Auxiliary Knowledge	Felix Morsbach
4	A relation between syntactic and semantic privacy notions	Alex Miranda Pascual
5	Measuring similarity of trajectories using learning methods	Alex Miranda Pascual
6	How to adapt trajectory data into road networks	Alex Miranda Pascual
7	Anonymous Key Exchange	Christoph Coijanovic + Marcel Tiepelt
8	A survey on brainwaves computer interface (BCI)	Matin Fallahi
9	Privacy-pres. biometric authentication(PPBA): third-party approach	Matin Fallahi
10	Explainable machine learning for brainwaves	Matin Fallahi
11	A survey on privacy of ubiquitous EMR receivers	Julian Todt
12	A survey on video anonymization	Julian Todt
13	Modelling and Synthesizing Human Motion	Simon Hanisch
14	Survey on 5G Security and beyond	Kamyar Abedi

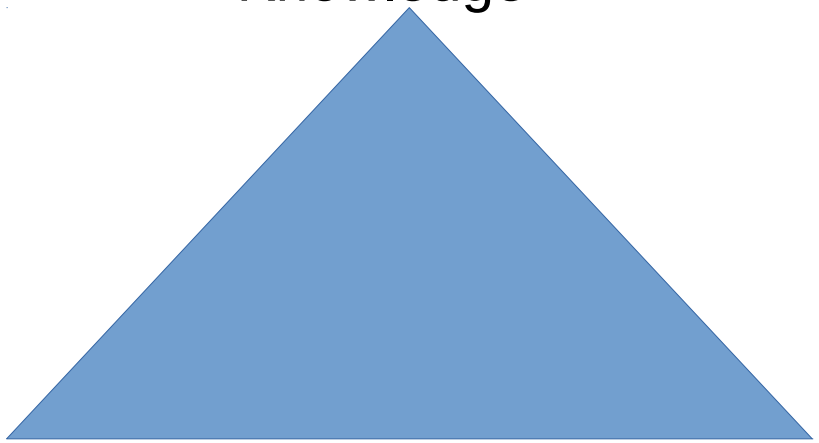
Topic Preferences

- Name:
- Email: (We'll invite you to join the program committee via this email)
- Preferred topics to work on: (let us know if your preferred topics to review differ)
  - 1: #V
  - 2: #W
  - 3: #X
  - 4: #Y
  - 5: #Z

- Send via email to christiane.kuhn@kit.edu & patricia.balboa@kit.edu
  until November 1

In two(!) weeks

Technical Knowledge



Scientific Process

Basic Skills (read, write, present)