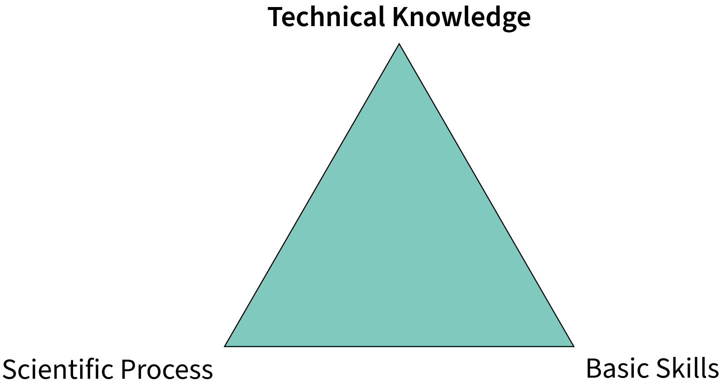
Karlsruher Institut für Technologie

Seminar Privacy and Security WS2023/24
Organisation & Topics

Patricia Guerra-Balboa

October 24, 2023

Seminar goals

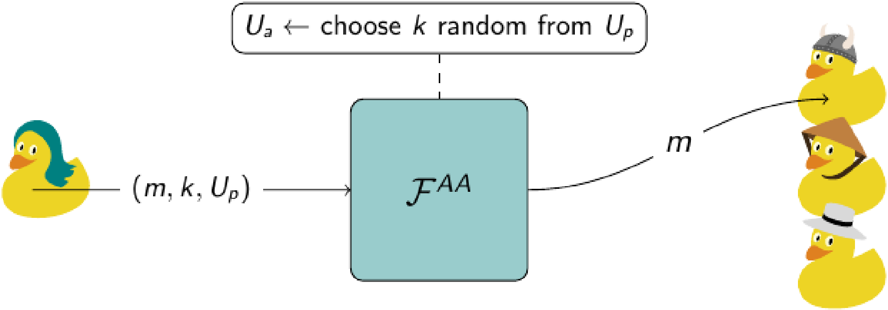


Technical Knowledge

Scientific Process

Basic Skills

Anonymous Communication



#1 Continuous Group Key Agreement (Christoph Coijanovic)

Continuous Group Key Agreement (CGKA)

CGKA lets a group of users derive a shared key that can be updated (e.g., periodically or when a new member joins). With CGKA, group chats can be *forward secret* and *post-compromise secure*.

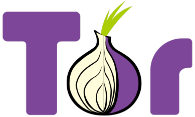
There is currently much academic interest in CGKA due to an effort by the IETF to standardize it as “IETF MLS”

Your Task

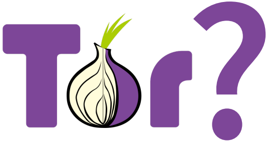
- Find state of the art in CGKA
- How compatible are different approaches with each other and MLS?

If you have any questions that Daniel cannot answer, send me an email at `christoph.coijanovic@kit.edu`

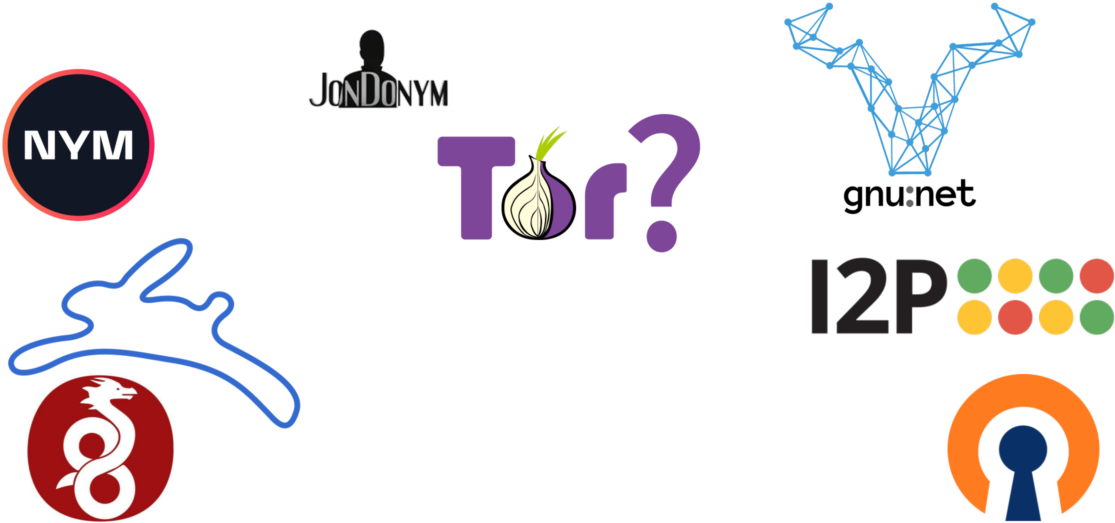
#6 Anonymous Communication in Practice (Daniel Schadt)



#6 Anonymous Communication in Practice (Daniel Schadt)



#6 Anonymous Communication in Practice (Daniel Schadt)



#6 Anonymous Communication in Practice (Daniel Schadt)

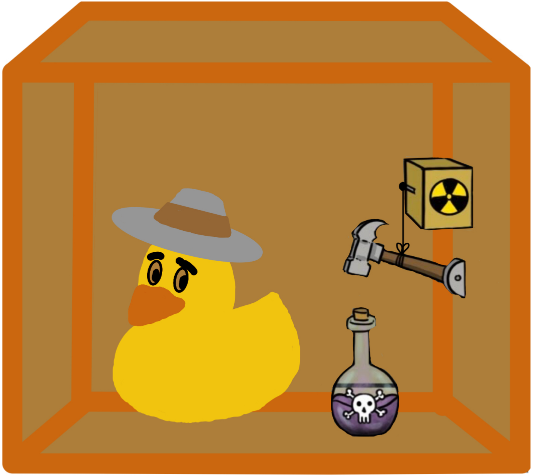
- Practical aspects
  - Active development
  - Users
  - Platforms
- Theoretical aspects
  - Threat model
  - Privacy notion

#6 Anonymous Communication in Practice (Daniel Schadt)

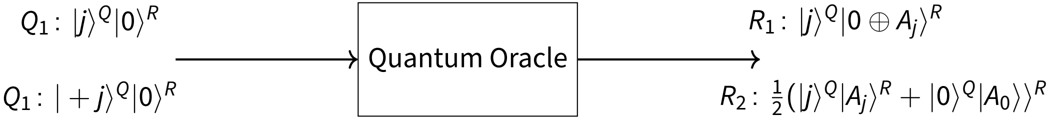
- Practical aspects
  - Active development
  - Users
  - Platforms
- Theoretical aspects
  - Threat model
  - Privacy notion

Survey the state of practical AC solutions

Quantum Privacy



#9 qRAM architecture (Shima Hassanpour)



$Q_1 : |j\rangle^Q|0\rangle^R$

$Q_1 : |+j\rangle^Q|0\rangle^R$

$R_1 : |j\rangle^Q|0 \oplus A_j\rangle^R$

$R_2 : \frac{1}{2}(|j\rangle^Q|A_j\rangle^R + |0\rangle^Q|A_0\rangle\rangle^R$

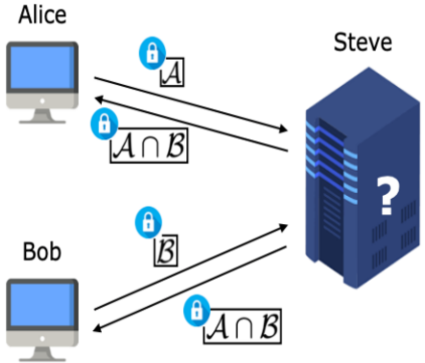
- It is a classical data lookup oracle with classical memory.

$$O_{RAM}|j\rangle|0\rangle = |j\rangle f(j)\rangle$$

- Is an interface between classical data and quantum algorithms.
- **What is the real physical implementation ideas?**

#10 Private Set Intersection (Shima Hassanpour)

- PSI is a problem within the field of secure computation
- Two-party PSI, hold a set of m items: $A = \{a_1, \ldots, a_m\}, B = \{b_1, \ldots, b_m\}$
- The goal: obtain the intersection $A \cap B$.
- MPC
- Survey quantum approaches


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

Biometrics

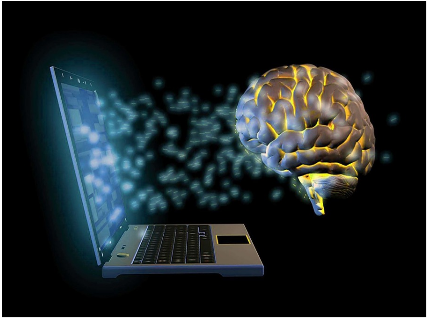
#2 Privacy Protections for Mixed Reality (Simon Hanisch)

- Mixed reality, including virtual reality and augmented reality, offers new possibilities but also introduces new threats to the privacy of its users
- How can the privacy of users be protected in mixed reality?
- Goal: Perform a survey of existing privacy-protecting techniques for mixed reality
- Compare the found solution to existing privacy threats, are they already all addressed?

© The Octalysis Group

#7 Neural Mechanisms of Speech Processing (Matin Fallahi)

- What can brainwaves reveal about language tasks?
- How are these information extracted?
- How does state-of-the-art perform?

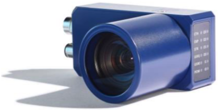


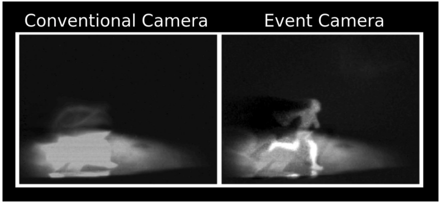
#8 Attacks on Biometric Authentication Systems (Matin Fallahi)

- What attacks compromise biometrics?
- How to mitigate them?
- How do they differ from traditional methods?

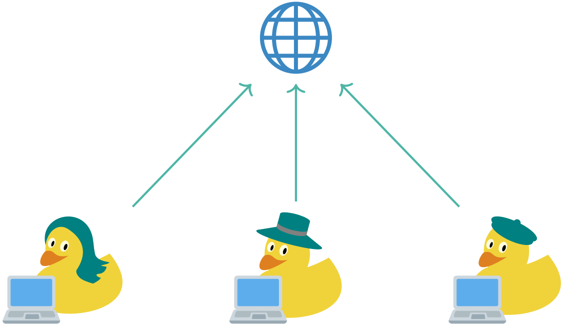
#9 A Literature-based Privacy Analysis of Event Cameras (Julian Todt)

- Event cameras are getting more common
- Privacy implications are unknown
  - Some claim higher privacy, others show identification potential
- Goal: Literature Review that leads to privacy analysis and comparison to traditional cameras





Resilient Networking



#12 Zero-trust: Verification first (Fritz Windisch)

- ► New threats on networks due to new technologies like IoT
- ► Attacks can come from any angle – no one can be trusted

⇒ Design of networks following a zero-trust approach

Topic:

- ► Collect an overview over zero-trust
- ► Research current approaches and compare them
- ► Identify current gaps in research/future directions

#13 Network slicing: Isolation of network devices in software-defined networks (Fritz Windisch)

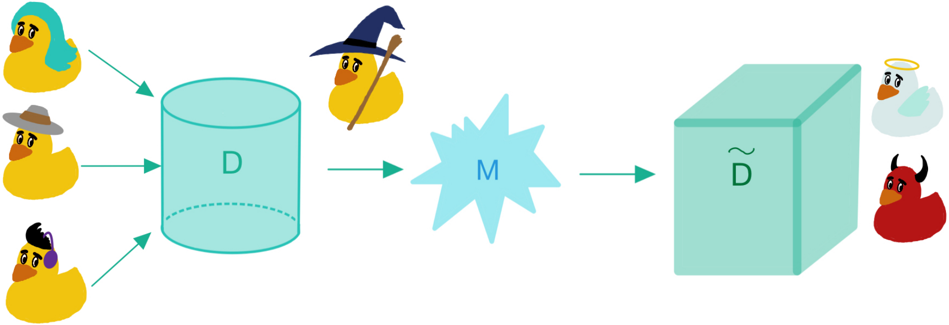
- Network slicing has become more attention following the 5G standards
- Network slicing isolates devices in groups to
  - Limit attack surface
  - Provide QoS guarantees

⇒ Will play a key role in applications like remote surgery and more

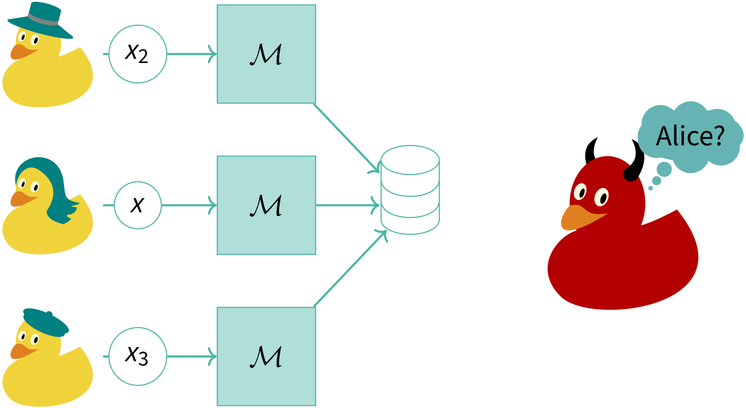
Topic:

- Give an overview over network slicing
- Research current solutions (single- and multi-domain)
- Compare the solutions found (concerning features, security and limitations)
- Identify current gaps in research/future directions

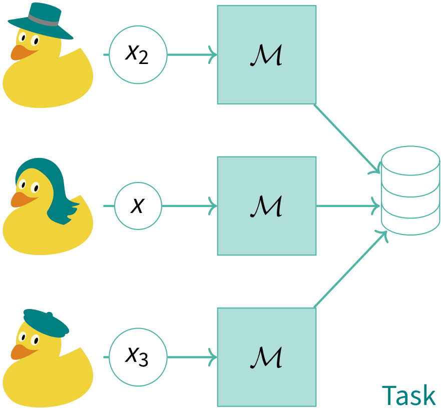
Statistical Disclosure Control



#3 Attack Resilience of DP (Patricia Guerra-Balboa)



#3 Attack Resilience of DP (Patricia Guerra-Balboa)

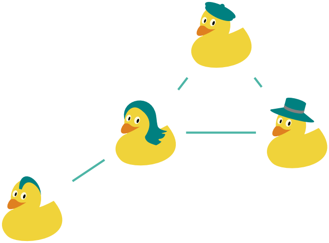


Task 1: Survey Existing Attacks

Task 2: Find Theoretical Adversarial Bounds

Optional Task: Design New Attacks

#4 Correlation-based attacks against DP (Patricia Guerra-Balboa)



Moltkestraße
Schlossgarten
Schlossgartenbahn
Jahnstraße
Bismarckstraße
Südliche Hildapromenade
Hoffstraße
Stabelstraße
Schlossbezirk
Schlossplatz
K 9656
Zirkel
Kaiserallee
Weststadt
Kaiserstraße
Kaiserstraße
Parkstraße
Oststa
Essenw
Scheffelstraße
Schillerstraße
Moningerstraße
Lessingstraße
Hirschstraße
Waldstraße
L 605
Gottesauer Straße
Esplanade
B 10

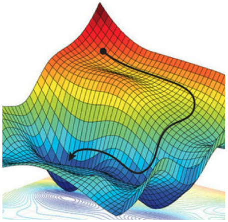
Task 1: Survey Existing Empirical Attacks

Task 2: Find Theoretical Adversarial Bounds

Optional Task: Focus on Trajectory data

#14 An Introduction to DP Stochastic Gradient Descent (Felix Morsbach)

- Stochastic gradient descent (SGD) is an iterative optimization algorithm for finding the parameters that provide the best fit between predicted and actual outputs, widely used in machine learning
- To prevent information leakage from trained models, differentially private versions of SGD exist
- However, there have been a multitude of approaches being proposed on how to make SGD differentially private

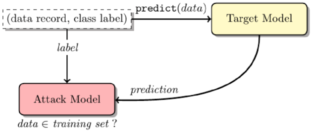


🎯 Develop a tutorial covering DP-SGD for machine learning. Explain how optimization algorithms can be made differentially private, especially how different DP composition theorems can be applied.

#15 Out of the Lab:

What Can Membership Inference Attacks Actually Do? (Felix Morsbach)

- Membership inference attacks are able to infer information about the data used for training machine learning models
- Much research focused on this topic and many demonstrations of this vulnerability exist, usually they are based academic or non-sensitive datasets
- Whether (and how) these attacks in their current form actually pose privacy risks is debatable



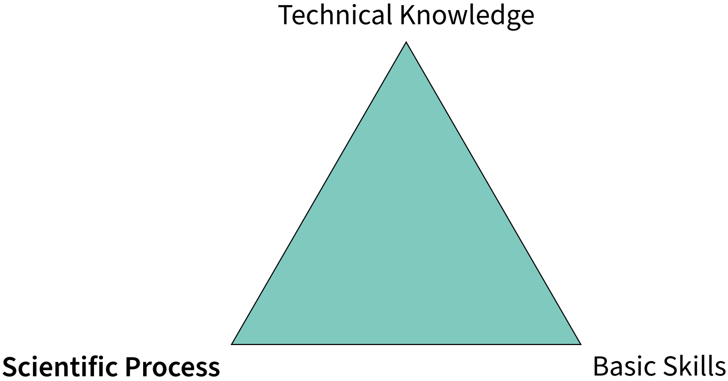
Investigate the privacy implications a membership inference attack could have and assess whether current state-of-the-art membership inference attacks actually would be capable to cause such harm

Topic Preferences list

- Complete the formular: `https://portal.wiwi.kit.edu/ys/7695`
- Deadline: 30.10.2023 23:55
- You need to rank all the topics
- You need to rank at least one topic with 1,2,3,4 and 5 starts.

Figure 1: QR code to the formular `https://ps.tm.kit.edu/english/139_887.php`

Seminar goals



Technical Knowledge

Scientific Process

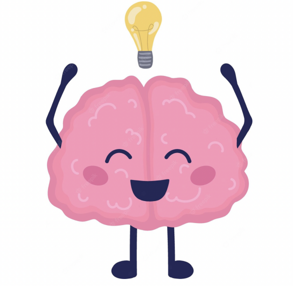
Basic Skills

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

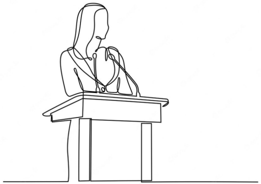
1. Pick topic
2. Make a contribution
3. Write and submit a paper
4. Get reviews from peers
5. Revise paper (and get accepted)
6. Present contribution at the conference

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

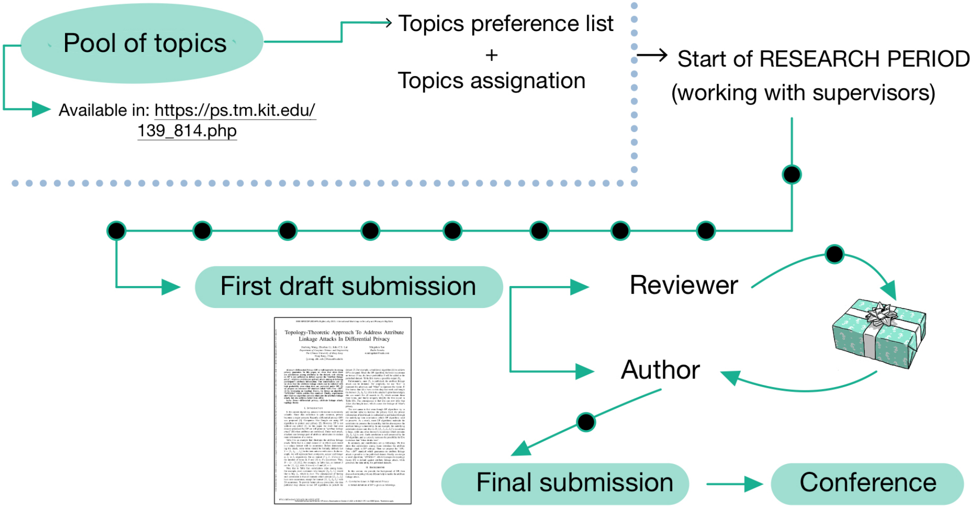
1. Pick topic
2. Make a contribution
3. Write and submit a paper
4. Get reviews from peers
5. Revise paper (and get accepted)
6. Present contribution at the conference



Our scientific conference

1. Pick topic (Choose from our selection)
2. Make a contribution: Find and read literature on your topic. Understand, compare, 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

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 2: 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=sp2324`
- Review (PC member role): Access to papers via EasyChair.
- Submitting reviews via EasyChair ("Reviews" → "My papers" → “Add review”)

Giving & Receiving Feedback

Giving:

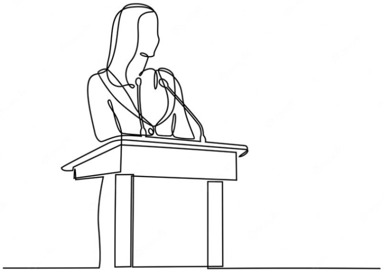
You will review 2 papers

Receiving

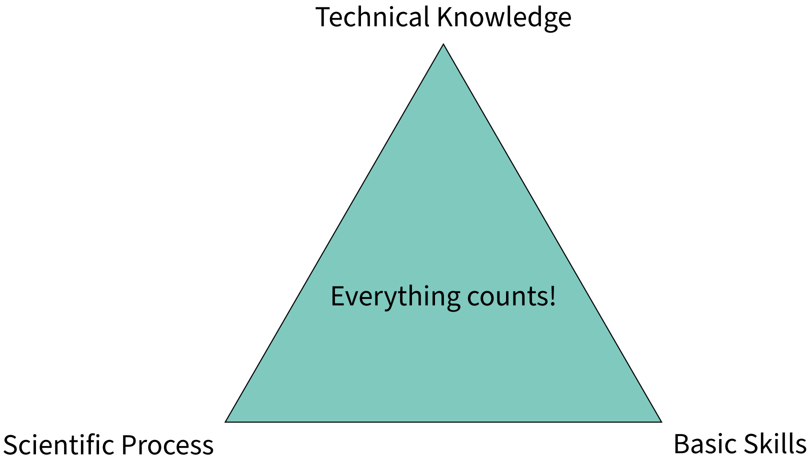
You will receive 3 reviews

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!

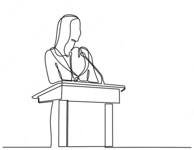
Scientific Process

Basic Skills

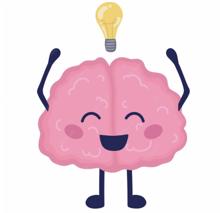
Evaluation & Grades

X_1 = written paper

X_2 = Reviews



X_3 = Presentation



X_4 = Participation in the Q&A

Final Grade:

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

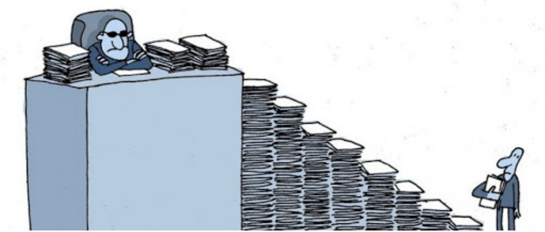
Timeplan

Date	Milestone
24.10.2023	Topic presentation
02.11.2023 9:45 – 11:15	Basic Skills
30.10.2023	Topic preferences due
30.10.2023	Topic assignment (contact your mentor!)
28.01.2024	Paper submission deadline
04.02.2024	Reviews deadline
11.02.2024	Revised paper deadline
∼20.02.2024	Presentation at our conference

Table 1: Timeplan updates in our webpage `https://ps.tm.kit.edu/139_887.php`

Bureaucracy

- Always inform if you decide to drop out!
- The deadline for abandoning the seminar is 28.01.2024. 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



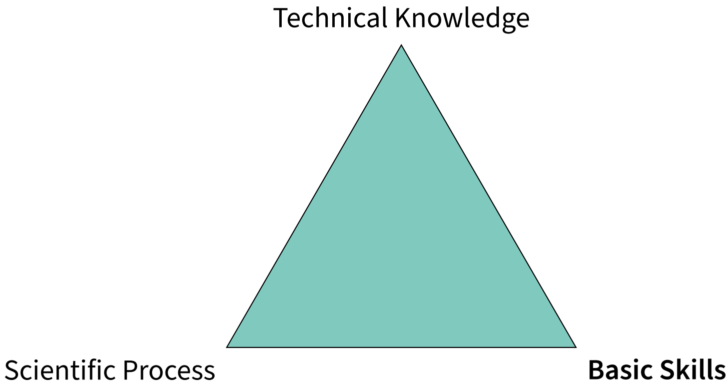
Getting information

- **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/english/139_887.php`
  - Email to potential supervisors: `https://ps.tm.kit.edu/english/21.php`

Seminar Goals



Technical Knowledge

Scientific Process

Basic Skills