Karlsruhe Institute of Technology

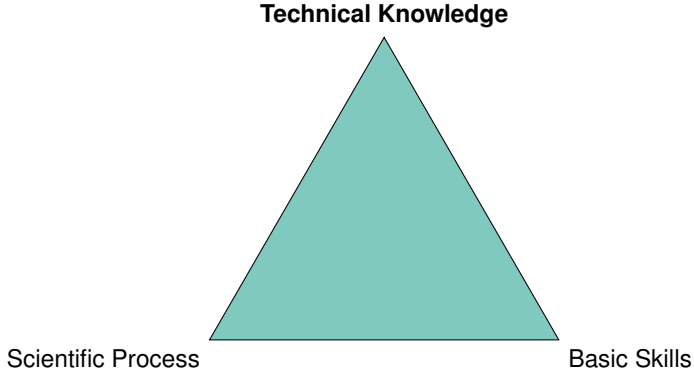
PRIVACY AND SECURITY

Seminar Privacy und Technischer Datenschutz

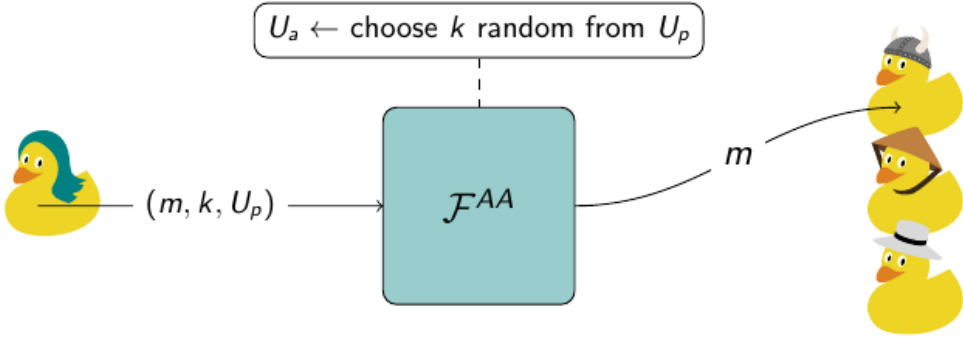
Introduction SS 2024

Patricia Guerra-Balboa | 16. April 2024

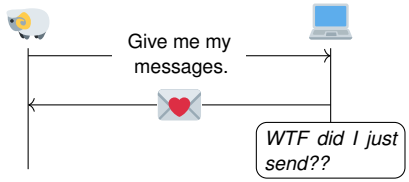
Seminar goals



Anonymous Communication



7 Oblivious Message Retrieval (Christoph Coijanovic)



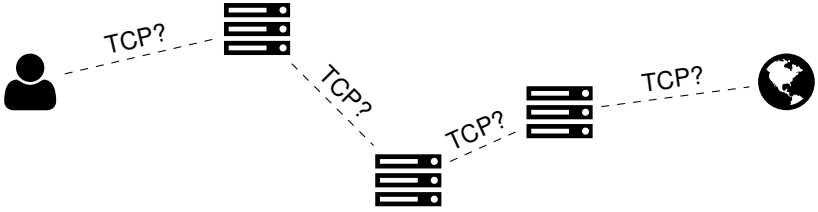
- Oblivious Message Retrieval (OMR) is the new kid on the block of anonymous communication

Your Task

Survey the existing approaches for OMR.

- How do they differ from each other?
- What are their advantages and disadvantages compared to other constructions for anonymous communication?

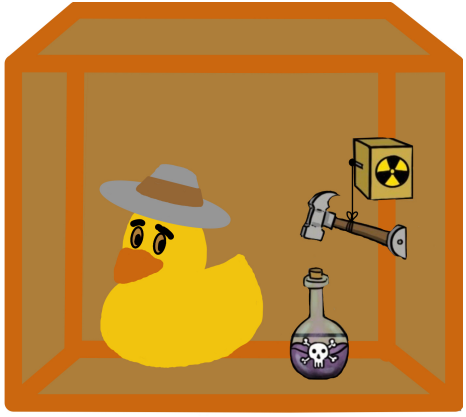
#5 Tor beyond TCP (Daniel Schadt)



- What are the problems?
- What are possible solutions?
- What are the consequences?

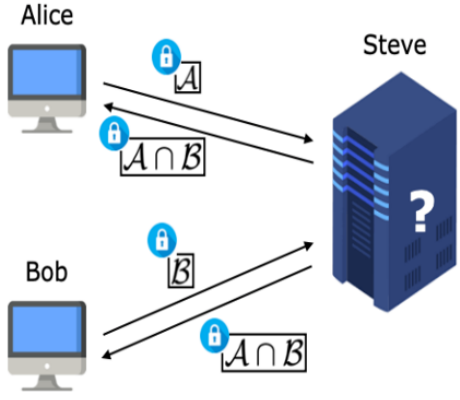
- Give a overview over the current situation
  - Explain the design choices
- Evaluate proposals
  - Efficiency, anonymity, attacks, . . .

Quantum Privacy



#14 **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

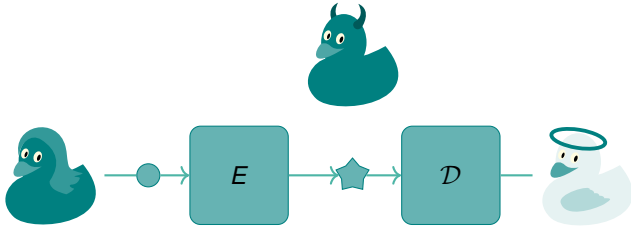


Quantum Private Query

- PIR-SPIR
- The quantum scheme for SPIR is defined as QPQ

the goal of this seminar is to review different types of QPQ and how do they work.

Cryptography

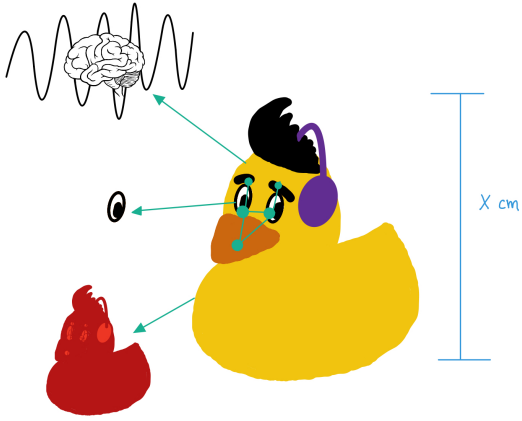


#6 **Deniability in multi-party computation** (Saskia Bayreuther)

- What is deniability in multiparty protocols?
  - Literature review
  - Definition/Formalization
- State of the art papers[1]

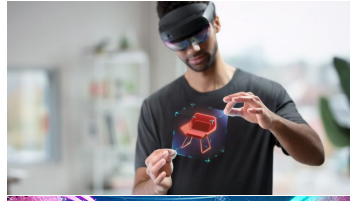
[1] Alonso Gonzalez-Ulloa und Alejandro Hevia. „Online Deniability for Multiparty Protocols with Applications to Externally Anonymous Authentication“. In: Cryptology ePrint Archive (2014)

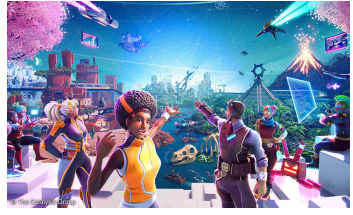
Biometrics



#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?

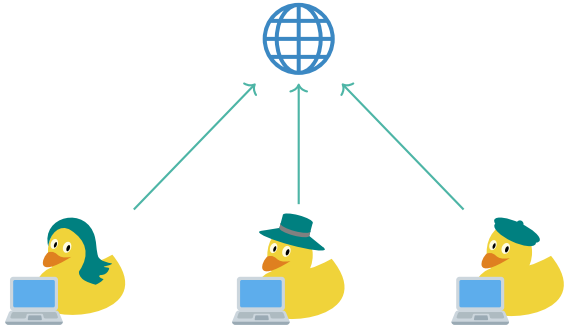




#9 **Attacks on Biometric Authentication Systems** (**Matin Fallahi**)

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

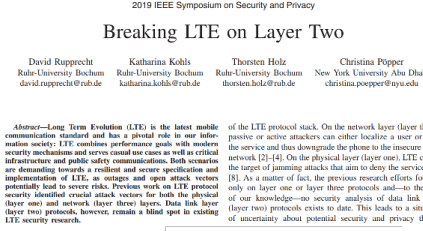
Resilient Networking



#8 **Survey on Vulnerabilities in 5G network Layer 2**

(Kamyar Abedi)

Karlsruhe Institute of Technology



2019 IEEE Symposium on Security and Privacy

Breaking LTE on Layer Two

David Rupprecht
Ruhr-University Bochum
david.rupprecht@rub.de

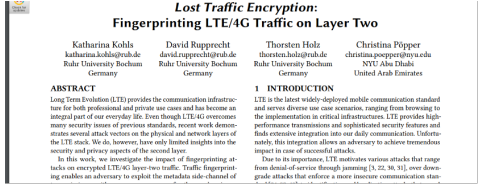
Katharina Kohls
Ruhr-University Bochum
katharina.kohls@rub.de

Thorsten Holz
Ruhr-University Bochum
thorsten.holz@rub.de

Christina Pöpper
New York University Abu Dhabi
christina.poepper@nyu.edu

Abstract—**Long Term Evolution (LTE) is the latest mobile communication standard and has a pivotal role in our information society: LTE combines performance goals with modern security mechanisms and serves causal use cases as well as critical infrastructure and public safety communications. Both scenarios are demanding towards a resilient and secure specification and implementation of LTE, as outages and open attack vectors potentially lead to severe risks. Previous work on LTE protocol security identified crucial attack vectors for both the physical (layer one) and network (layer three) layers. Data link layer (layer two) protocols, however, remain a blind spot in existing LTE security research.**

of the LTE protocol stack. On the network layer (layer three), passive or active attackers can either localize a user or deny the service and thus downgrade the phone to the insecure GSM network [2]–[4]. On the physical layer (layer one), LTE can be the target of jamming attacks that aim to deny the service [5]–[8]. As a matter of fact, the previous research efforts focused only on layer one or layer three protocols and—to the best of our knowledge—no security analysis of data link layer (layer two) protocols exists to date. This leads to a situation of uncertainty about potential security and privacy threats



Lost Traffic Encryption: Fingerprinting LTE/4G Traffic on Layer Two

Katharina Kohls
katharina.kohls@rub.de
Ruhr University Bochum
Germany

David Rupprecht
david.rupprecht@rub.de
Ruhr University Bochum
Germany

Thorsten Holz
thorsten.holz@rub.de
Ruhr University Bochum
Germany

Christina Pöpper
christina.poepper@nyu.edu
NYU Abu Dhabi
United Arab Emirates

ABSTRACT

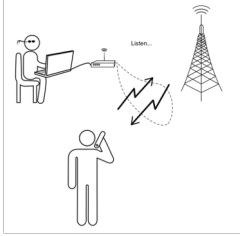
Long Term Evolution (LTE) provides the communication infrastructure for both professional and private use cases and has become an integral part of our everyday life. Even though LTE/4G overcomes many security issues of previous standards, recent work demonstrates several attack vectors on the physical and network layers of the LTE stack. We do, however, have only limited insights into the security and privacy aspects of the second layer.

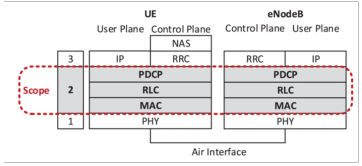
In this work, we investigate the impact of fingerprinting attacks on encrypted LTE/4G layer-two traffic. Traffic fingerprinting enables an adversary to exploit the metadata side-channel of

1 INTRODUCTION

LTE is the latest widely-deployed mobile communication standard and serves diverse use case scenarios, ranging from browsing to the implementation in critical infrastructures. LTE provides high-performance transmissions and sophisticated security features and finds extensive integration into our daily communication. Unfortunately, this integration allows an adversary to achieve tremendous impact in case of successful attacks.

Due to its importance, LTE motivates various attacks that range from denial-of-service through jamming [3, 22, 30, 31], over downgrade attacks that enforce a more insecure communication stan-





#3 Network slicing in software-defined networks

(Fritz Windisch)

Karlsruhe Institute of Technology

Network Slicing

- Partitioning a network into multiple isolated segments
- Improves security through isolation, encryption on the network stack, and more
- Can provide resource guarantees
- Applications: from mobile standards to remote surgeries

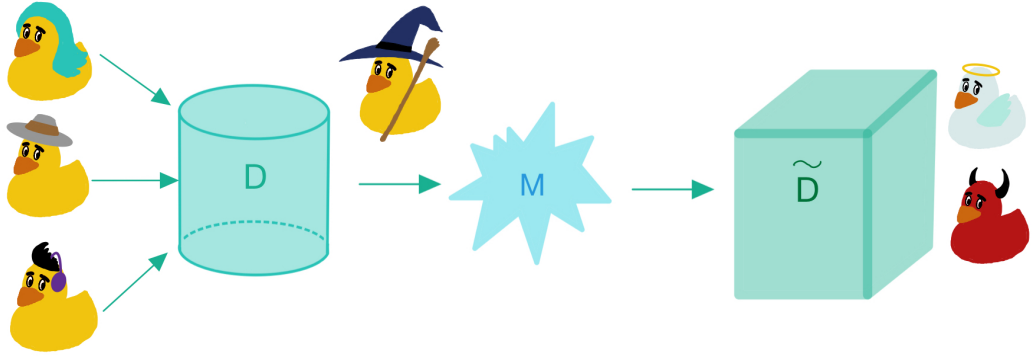
Software-defined networks (SDN)

Separates the network stack into two planes: Control plane and data plane

Topic

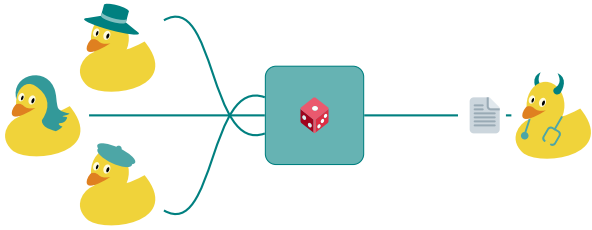
Collect an overview of the state-of-the-art in network slicing, alongside their security claims and limitations

Statistical Disclosure Control



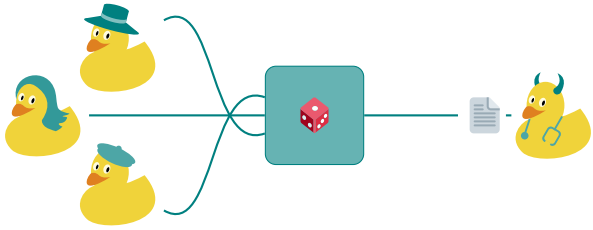
#4 Choosing things privately with Differential Privacy

(Patricia Guerra-Balboa)

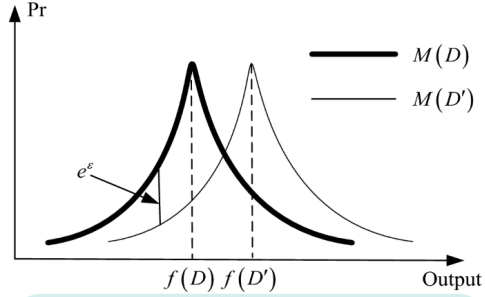


#4 Choosing things privately with Differential Privacy

(Patricia Guerra-Balboa)



#10 The Choice of ε in DP (Àlex Miranda-Pascual)



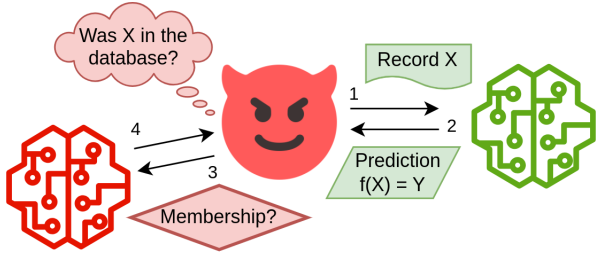
What are good values of ε?

0.1? 2? 50?

#13 Out of the Lab: Privacy Threats of Machine Learning

(Felix Morsbach)

- ML models are vulnerable to attacks that infer information about the training data
  - → possibly causing privacy violations
- Whether this is an actual privacy risk is debatable
  - Information gained is probabilistic!
- Determining privacy risks is difficult
  - **What about privacy harm?**



Objective

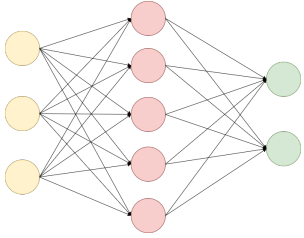
For a use case of your choice:
Research and discuss possible privacy harms of inference attacks on machine learning models.

#12 Privacy-Preserving Machine Learning Frameworks

(Felix Morsbach)

Karlsruhe Institute of Technology

- Multiple defenses to address privacy and confidentiality threats of machine learning models exist (e.g. differentially private or federated learning)
- A **lot** of them are implemented and available as off-the-shelve solutions
  - For example Tensorflow Privacy (Google), Opacus (Facebook), ...
- For practitioners it is often unclear which libraries are suitable for which use cases, how to compare them, what protection guarantees they provide, or simply what their protection goals are?



Objective

Summarize and categorize currently available privacy-preserving machine learning libraries.

#11 **Conceptualizing Model** & **Hyperparameter Comprehension for PPML**

(Felix Morsbach)

Karlsruhe Institute of Technology

- Hyperparameter optimization and model selection are key steps during machine learning development
- Especially in PPML, this is prohibitively expensive in terms of computing resources
- Model and hyperparameter comprehension of ML practitioners is crucial
- Knowledge is often tacit and intractable → difficult to explicate
- **It is unclear what model and hyperparameter comprehension is** (and how to explicate it)

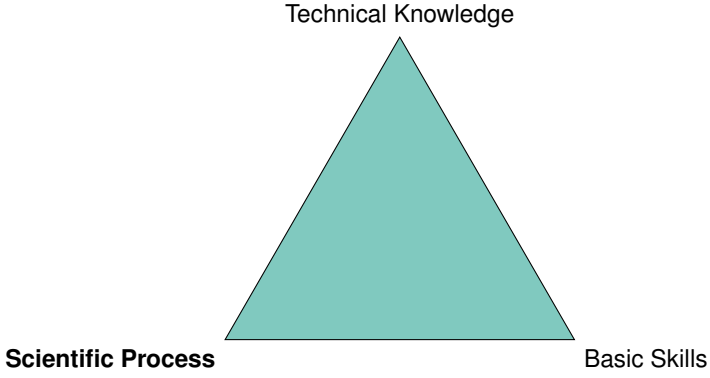
Objective

Conceptualize model and hyperparameter comprehension of practitioners by reviewing recent literature.

Topic Preferences list

- Send me your TOP 5 ordered list by mail
- Deadline: April 23, 2024, 24:59
- Mail: patricia.balboa@kit.edu

Seminar goals

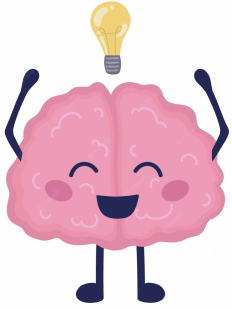


About scientific conferences

1. Pick topic

About scientific conferences

1. Pick topic
2. Make a contribution



About scientific conferences

1. Pick topic
2. Make a contribution
3. Write and submit a paper

About scientific conferences

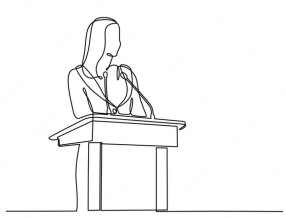
1. Pick topic
2. Make a contribution
3. Write and submit a paper
4. Get reviews from peers

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)

About scientific conferences

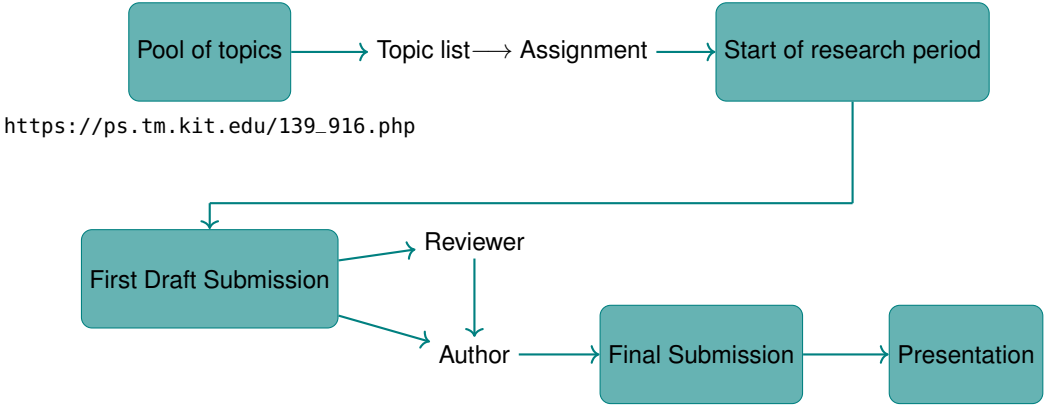
1. Pick topic
2. Make a contribution
3. Write and submit a paper
4. Get reviews from peers
5. Revise paper (and get accepted)
6. Present contribution at the conference



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



Your Paper

- English
- ACM/AMS/IEEE or other official template
- No required number of pages (typically something arround 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

Abbildung: 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://ps.tm.kit.edu/139_916.php`
- Review (PC member role): Access to papers via EasyChair.
- Submitting reviews via EasyChair ("Reviews"→ "My papers"→ “Add review”)

Giving & Receiving Feedback

Giving:

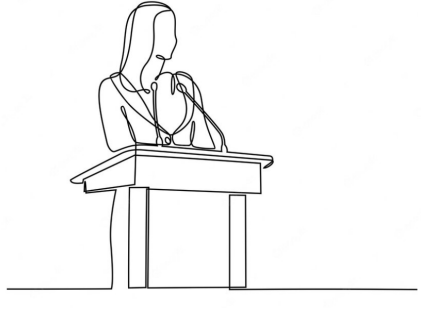
You will review 2 papers

Receiving

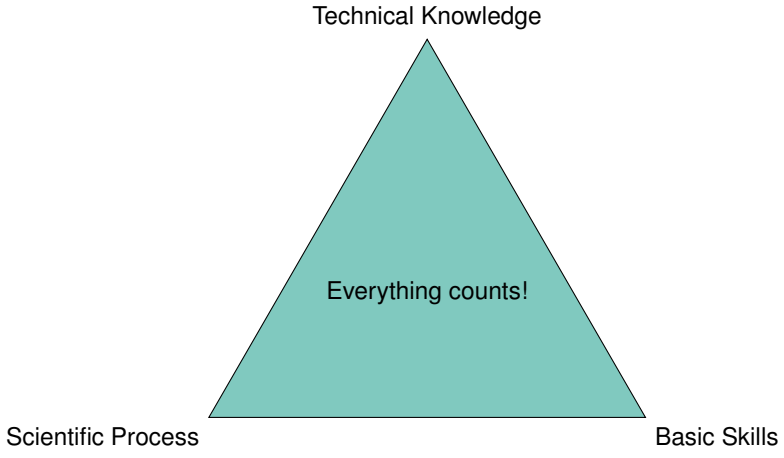
You will receive 3 reviews

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

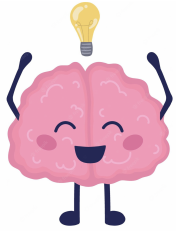


Evaluation & Grades

X_1 = written paper

X_2 = Reviews

X_3 = Presentation



X_4 = Participation in the Q&A

Final Grade:

$$0.45 * X_1 + 0.3 * X_3 + 0.2 * X_2 + 0.05 * X_4$$

You need a minimum both in the written and presentation grade to pass!!!

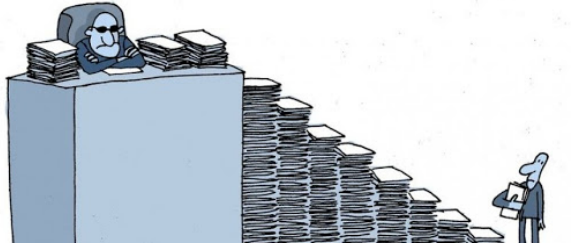
Timeplan

Date	Milestone
16.04.2024 10:00–10:45	Topic presentation
23.04.2024 10:00–11:00	Basic Skills
23.04.2024	Topic preferences due
24.04.2024	Topic assignment (contact your mentor!)
30.06.2024	Paper submission deadline
07.07.2024	Reviews deadline
14.07.2024	Revised paper deadline
∼23.07.2024	Presentation at our conference

Tabelle: Timeplan updates in our webpage `https://ps.tm.kit.edu/139_916.php`

Bureaucracy

- Always inform if you decide to drop out!
- The deadline for abandoning the seminar is 30.06.2024. 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/139_916.php`
  - Email to potential supervisors: `https://ps.tm.kit.edu/english/21.php`

Seminar Goals