

Privacy Enhancing Technologies (BSc)

Lecture I: Introduction

Univ.-Prof. Dr. Dominique Schröder

October 07, 2024



PRIVACY
ENHANCING
TECHNOLOGIES

Agenda

- Team
- Motivation
- Lecture Concept
- Contents
- Exercises
- Exams

Team

Univ.Prof.

Dr. Dominique Schröder

`dominique.schroeder@tuwien.ac.at`



Dominique

Paul Gerhart

`paul.gerhart@tuwien.ac.at`



Paul

Contact

You can contact us

- via the forums on TUWEL
- via email: teaching-pets@list.tuwien.ac.at

 Exercises

 General Questions and Announcements

 Lecture

 Communication for Students

Motivation



Source:<https://www.wikipedia.org>

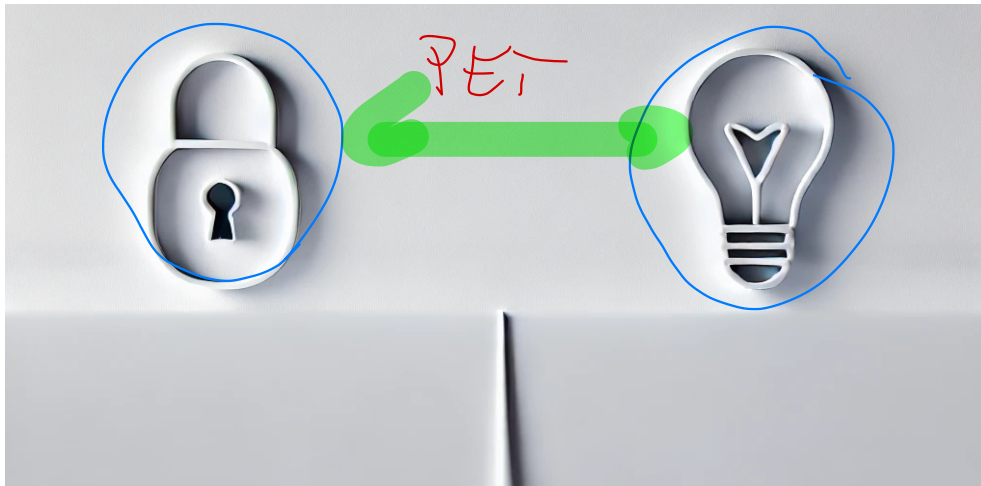
"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say".

— Edward Snowden

Privacy Areas (Not Exhaustive)

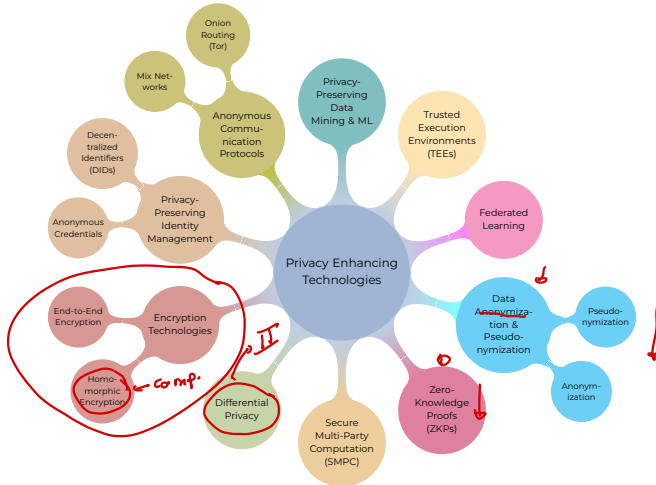


Privacy vs. Innovation



Source: <https://www.openAI.org>

Privacy-Enhancing Technologies



Limitations of PETs



Source https://youtu.be/F4WZ_k0vUDM?si=hzp3b7VPqKcuSN7F

Organizational

Lecture Concept

- Classical lecture
- Lecture is taking place **in person** on **Monday from 9:15 to 11:00** in FAV Hörsaal 1 - Inf (106)
- No streaming nor recording → topic was date...
- Three exercise sessions
- Midterm and final exam

Content & Procedure

KW	Type	Lectures <i>(many changes) → forum</i>
42	Lecture	Internet and Privacy in the Web
43	Lecture	Fingerprinting & Censorship
44	Exercise	Introduction to Rust
45	Lecture	Cryptographic Preliminaries
46	Lecture	DDH Key Exchange, Security Reductions
47	Exercise	Proofs and Theoretical Deepening
48	Lecture	TLS
49	Exam	Midterm Exam
50	Exercise	Rust Key Exchange
51	Lecture	Messaging I
3	Lecture	Messaging II (Forward Security, Post Compromise Security)
4	Lecture	Onion <i>→ Routing</i>
5	Lecture	Q & A
6	Exam	Final Exam
9	Exam	Reexam (Both for Midterm and Final)

Exercises

- You will find Information in TUWEL
- Exercise: KW 44 "Introduction to Rust"
- Exercise: KW 47 "Proofs and Theoretical Deepening"
- Exercise: KW 50 "Rust Key Exchange"

Exams

Midterm Exam:

2nd December, FAV Hörsaal 1 - Inf (106), 9.00 - 11.00

Final Exam:

27th January, FAV Hörsaal 1 - Inf (106), 9.00 - 11.00

Retake Midterm Exam:

24th February, Room TBA, 10.00 - 12.00

Retake Final Exam:

24th February, Room TBA, 12.00 - 14.00