# Security and Privacy of Information Systems

**Rafael Schaefer**

Technische Universität Berlin
Information Theory and Applications Chair

# 0. Course Information

# General Information

| | |
|---|---|
| **Instructor:** | Rafael Schaefer |
| **Contact:** | HFT 6 |
| | 030 - 314 26 632 (Voice) |
| | 030 - 314 28 320 (Fax) |
| | `rafael.schaefer@tu-berlin.de` |
| | (include “Security and Privacy 2019” in subject) |
| **Office Hours:** | Room HFT-TA 611A, by appointment (send email) |
| | |
| **Administrative Assistant:** | Ms. Jana Hantke |
| **Contact:** | HFT 6 |
| | `jana.hantke@tu-berlin.de` |
| | |
| **Lectures:** | Monday 10:15 – 11:45, room HFT-TA 131 |
| **Exercise:** | Monday 12:15 – 13:45, room HFT-TA 131 |
| | |
| **Course Documents:** | use the ISIS system |
| | `https://isis.tu-berlin.de/` |

# Background

- **Advised pre-requisites (background):**
  - VL Information Theory (0432 L 654)
    *Winter semester*

    or equivalent background.
  - Probability theory.
  - Calculus and elementary functional analysis.
  - Notions of convex optimization.

# Exam

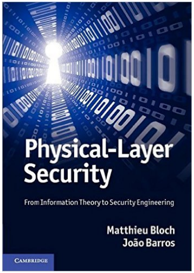
- **Exams, grading policy and homework:**
  - **Exam:** the course is passed by a combination of a project presentation and an oral examination.
  - The project is assigned approximately in the middle of the semester, and consists of reading an assigned paper in the area of information theoretic security and privacy, preparing a 30min **detailed** presentation followed by oral questions specifically on the paper and in general, on the course topics.
  - This course contributes for:
    1. 100/100 pts for the Module 40885 *Security and Privacy of Information Systems*.
  - The course has no formal graded homework. Problems and projects are posted and solutions are given and discussed, in order to help student's preparation for the final test.

# Additional Reading

- M. Bloch and J. Barros
  *Physical-Layer Security: From Information Theory to Security Engineering*
  Cambridge University Press, Cambridge UK, 2011.

- Y. Liang, H. V. Poor, and S. Shamai (Shitz)
  *Information Theoretic Security*
  Foundations and Trends in Communications and Information Theory, now publishers, 2008, `http://dx.doi.org/10.1561/0100000036`.

  IMPORTANT: You can access an electronic version of this book from TUB machines.



Information Theoretic Security
Yingbin Liang, H. Vincent Poor, and Shlomo Shamai (Shitz)
now

# Additional Reading

- Introductory textbook to information theory (good starting point; basic concepts of information theory; focuses on single-user/point-to-point channel)

  T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley & Sons, 2006

- Further topics on information theory (further topics on information theory; multi-user/network settings; one chapter on information theoretic secrecy)

  A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011

- Advanced reference on information theory (advanced book; one chapter on information theoretic secrecy)

  I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge University Press, 2011

- Advanced reference on information theoretic security and privacy (advanced book; collection of different topics)

  R. F. Schaefer, H. Boche, A. Khisti, and H. V. Poor, Eds., *Information Theoretic Security and Privacy of Information Systems*. Cambridge, UK: Cambridge University Press, 2017

- *Further reading will be pointed out for each chapter individually*

# Tentative Course Schedule

| Week | Topic |
|---|---|
| 1 (8.4) | Organization and Motivation |
| 2 (15.4) | Review: Information Theory |
| 3 (22.4) | *Easter Monday (Ostermontag)* |
| 4 (29.4) | Information Theoretic Security |
| 5 (6.5) | Wiretap Channel |
| 6 (13.5) | Secret Key Generation |
| 7 (20.5) | Biometric Authentication |
| 8 (27.5) | Information Theoretic Privacy |
| 9 (3.6) | Private Information Retrieval |
| 10 (10.6) | *Whit Monday (Pfingstmontag)* |
| 11 (17.6) | Differential Privacy |
| 12 (24.6) | *Project Assignment* |
| 13 (1.7) | |
| 14 (8.7) | *Project Presentation* |