



# Welcome to Cysec BSc!

*Dr.-Ing. Ben Stock*

WS24 | 2024-10-08

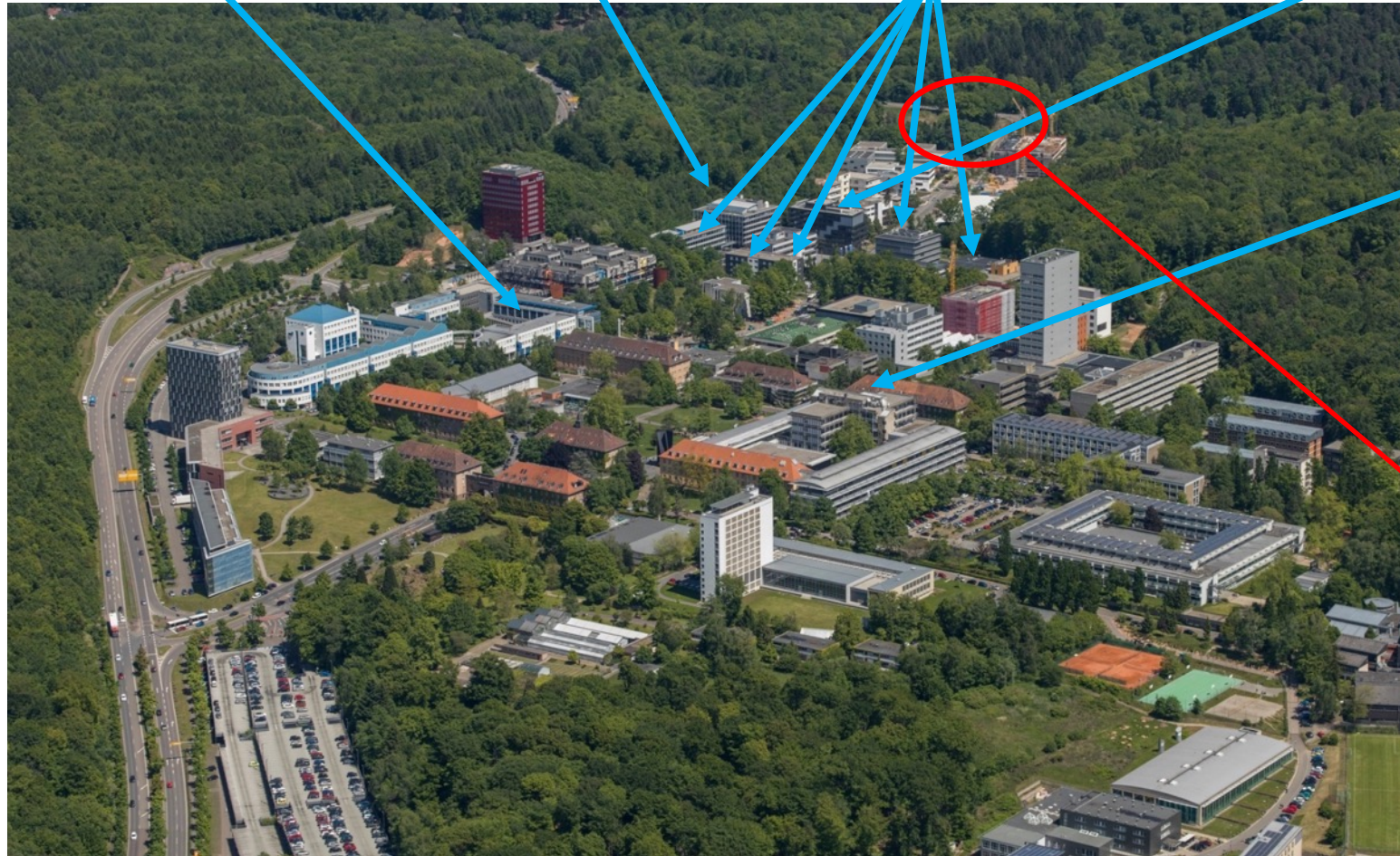


# Welcome

To your first Semester!



# The Saarbrücken Campus





# Saarland Informatics Campus (SIC)



- Computer Science Department of Saarland University (UdS)
- Max Planck Institute for Informatics
- Max Planck Institute for Software Systems
- German Research Center for Artificial Intelligence (DFKI)
- Centre for Bioinformatics
- Cluster of Excellence "Multimodal Computing and Interaction" (MMCI)
- Saarbrücken Graduate School of Computer Science
- International Max Planck Research School for Computer Science
- Schloß Dagstuhl (Leibniz Zentrum)
- ...

In total ca. 95 professors, research group leaders, and faculty



# Current study programs at SIC



---

## Bachelor

---

- Computer Science
- Bioinformatics
- Embedded Systems
- Media Informatics
- **Cybersecurity**
- **Cybersecurity (English), since WS 2021**
- Mathematics and CS
- Computational Linguistics
- *Data Science and AI*

---

## Master

---

- Computer Science
- Bioinformatics
- Embedded Systems
- Media Informatics
- Visual Computing
- Mathematics and CS
- Language Science & Technology
- *Data Science and AI*
- **Cybersecurity (since 2021)**

---

## Staatsexamen

---

- Lehramt Informatik (“Didactics of Informatics”)

---

## Doctorate

---

- Graduate School after completion of the Bachelor



# Example Course of studies (German BSc)

1	Programmierung 1 (9 CP)	Mathematik für Informatiker 1 (9 CP)	Foundations of Cyber Security 1 (9 CP)	FP: Ringvorlesung (2 CP)	29
2	Programmierung 2 (9 CP)	Mathematik für Informatiker 2 (9 CP)	Foundations of Cyber Security 2 (6 CP)	Statistics Lab (6 CP)	30
	In der vorlesungsfreien Zeit: Softwarepraktikum (9 CP)				9
3	Elements of Machine Learning (6 CP)	Grundzüge der theoretischen Informatik (9 CP)	Algorithmen und Datenstrukturen (6 CP)	Cyber Security Proseminar (5CP)	26
4	Cryptography (9 CP)	Systemarchitektur (9 CP)	Wahlpflicht Grundlagen der Informatik (6 CP)	FP: Tutor (4 CP)	28
5	Cyber Security Project (9 CP)	Cyber Security Seminar (7 CP)	Vertiefung I – Cyber Security (6 CP)	Vertiefung II - Cyber Security (6 CP)	28
6	Vertiefung III - Cyber Security (6 CP)	Bachelor Seminar (9 CP)	Bachelor Arbeit (12 CP)	FP: Sprachkurs (3 CP)	30



# Lecture content in the first semesters

- **Foundations of Cyber Security 1:** Cryptography, Network Security, Web Security, Privacy
- **Foundations of Cyber Security 2:** System Security, Mobile Security, Hardware Security
- **Mathematics for Computer Scientists 1:** Foundations of discrete mathematics, Analysis
- **Mathematics for Computer Scientists 2:** Algebra
- **Programming 1:** functional programming (ML), Algorithms
- **Programming 2:** object-oriented programming (Java)
  
- **All in all, there are no actual dependencies between lectures**
- **Foundations of CySec 1 and CySec 2 are in English!**



# Specialization options

- Practical courses:
  - Web Security, Mobile Security
  - Physical-Layer Security, Side-Channel Attacks and Defenses
- Theoretical courses:
  - Privacy Enhancing Technologies
  - Verification
  - Accountability
- Complementary lectures:
  - Usable Security
  - Recht der Cybersicherheit
  - Data Analytics

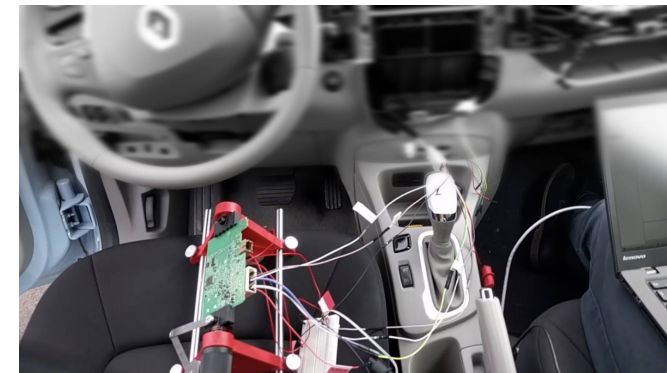
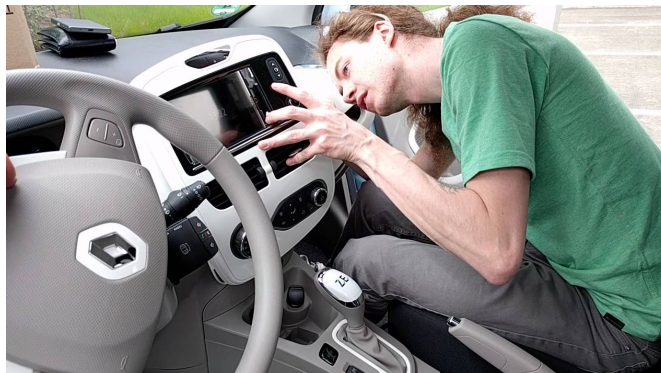






# Course of studies: practical focus

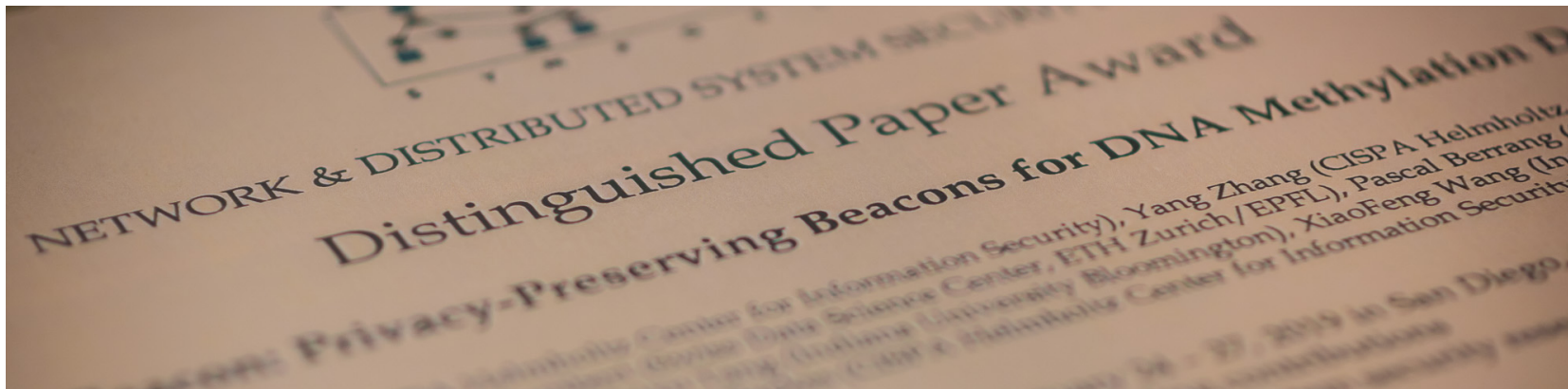
- Proseminar: Influential Papers in Web Security
- Adv. lecture 1: Physical-Layer Security
- Adv. lecture 2: Side Channels A&D
- Adv. lecture 3: Foundations of Web Security
- Seminar: Advanced Fuzzing Techniques
- Bachelor thesis: CAN-Bus Fuzzing to detect vulnerabilities or side-channels in cars?





# Course of studies: theoretical focus

- Proseminar: Medical Privacy
- Adv. lecture 1: Privacy Enhancing Technologies
- Adv. lecture 2: Machine Learning in Cybersecurity
- Adv. lecture 3: Advanced Public Key Encryption
- Seminar: Data Privacy
- Bachelor thesis: Develop novel methods for securely analyzing medical data





# Your first semester: Example schedule

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
8-10							
10-12			Math 1	Prog 1	Math 1		
12-14							
14-16	Ring lect.	Prog 1		CySec 1			
16-18							
18-20							
20-22							



# Your first semester: Example schedule

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
8-10	Sleeping	Sleeping	Sleeping	Hangover	Sleeping		
10-12	Sleeping	Sleeping	<b>Math 1</b>	<b>Prog 1</b>	<b>Math 1</b>		
12-14	Sport	Reading	Food	Food	Sport		
14-16	<b>Ring lect.</b>	<b>Prog 1</b>	Sleeping	<b>CySec 1</b>	Job		
16-18	Gaming	Job	Beering	Netflix	Job		
18-20	Gaming	Job	Beering	Netflix	Job		
20-22	Beering	Job	More beering	Netflix	Cinema		



# Your first semester: Example schedule

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
8-10							
10-12			<b>Math 1</b>	<b>Prog 1</b>	<b>Math 1</b>		
12-14							
14-16	<b>Ring lect.</b>	<b>Prog 1</b>		<b>CySec 1</b>			
16-18							
18-20							
20-22							



# Your first semester: Example schedule

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
8-10							
10-12	CySec I Exercise		Math 1	Prog 1	Math 1		
12-14							
14-16	Ring lect.	Prog 1	Prog 1 Exercise	CySec 1			
16-18	CySec I Project				Math 1 Exercise		
18-20	CySec I Project						
20-22							



# Your first semester: Example schedule

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
8-10							
10-12	CySec I Exercise	Exercise prep.	Math 1	Prog 1	Math 1		
12-14	Exercise prep.	Exercise prep.	Study Math 1	Study Prog 1			
14-16	Ring lect.	Prog 1	Prog 1 Exercise	CySec 1	Study Math 1		
16-18	CySec I Project	Study Prog 1	Exercise prep.	Study CySec 1	Math 1 Exercise		
18-20	CySec I Project						
20-22							



# Online tool of SIC

STUDIENGANG: Cybersicherheit - IM SEMESTER: 2 - [Ändern](#)

	Montag	Dienstag	Mittwoch	Donnerstag	Freitag
-8					
-9	Statistics Lab	Statistics Lab			
-10					Programmierung 2
-11					
-12					
-13					
-14					
-15		Programmierung 2		Foundations of Cyber Security 2 (Grundlagen der Cybersicherheit 2)	
-16					
-17					

Prog2 Mfi2 CySec2 StatLab SoPra 39 / 39 (empfohlen) ECTS ausgewählt

- Anmerkungen? Schreib uns!
- Kalender exportieren
- PDF drucken

- Hilfreiche Links:
- [Studiengangsseite](#)
  - [Studienordnung](#)
  - [Beispielstudienplan](#)

+ Weitere Vorlesung hinzufügen

Feste Vorlesung 9 ECTS

Programmierung 2  
Sebastian Hack - [LSF](#)

Feste Vorlesung 9 ECTS

Mathematik für Informatiker 2  
Bisher unbekannt / To be determined

Feste Vorlesung 6 ECTS

Foundations of Cyber Security 2 (Grundlagen der Cybersicherheit 2)  
Michael Schwarz - [LSF](#)

Feste Vorlesung 6 ECTS

Statistics Lab  
Verena Wolf - [LSF](#)

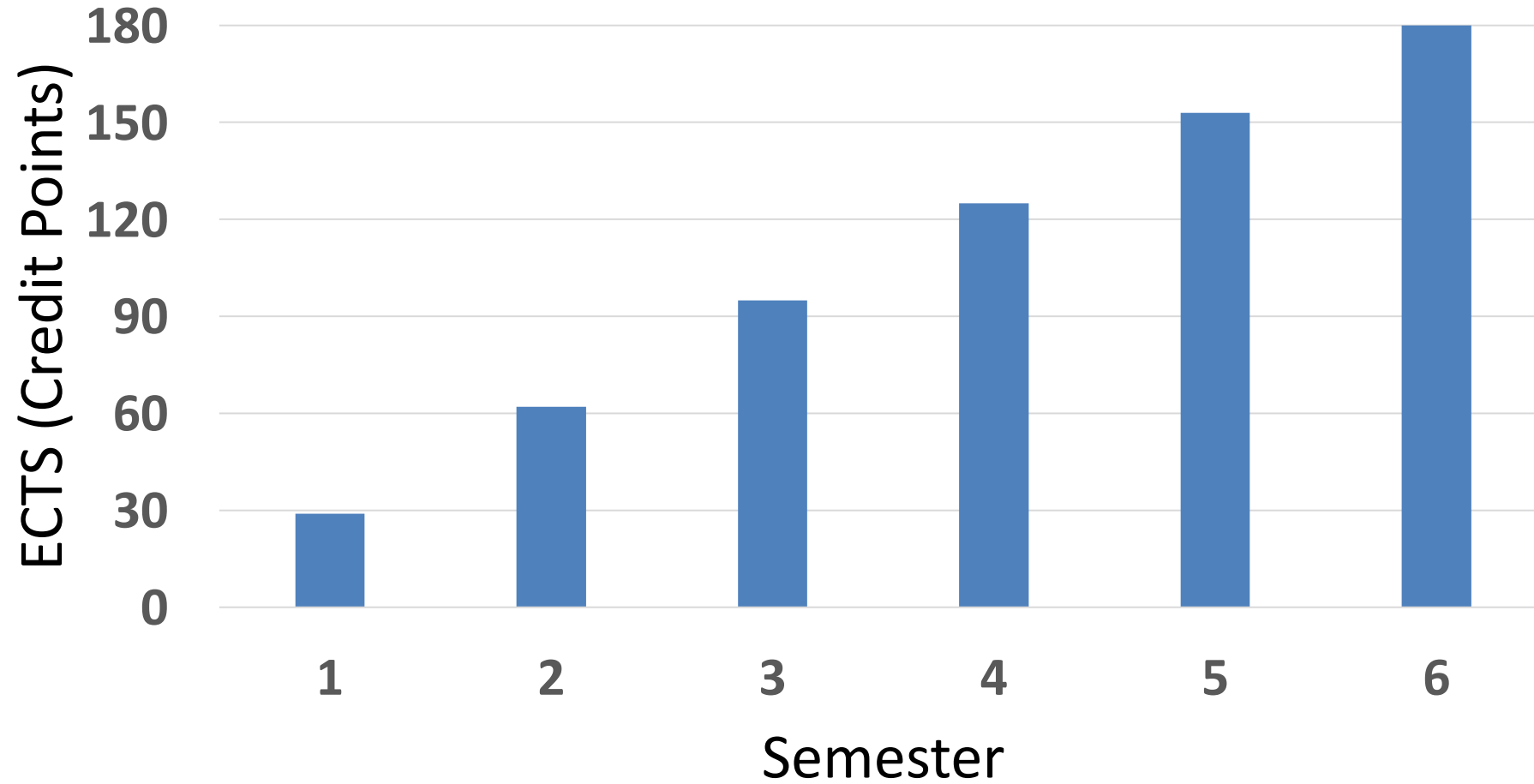
Feste Vorlesung 9 ECTS

Softwarepraktikum  
Sven Apel - [LSF](#)



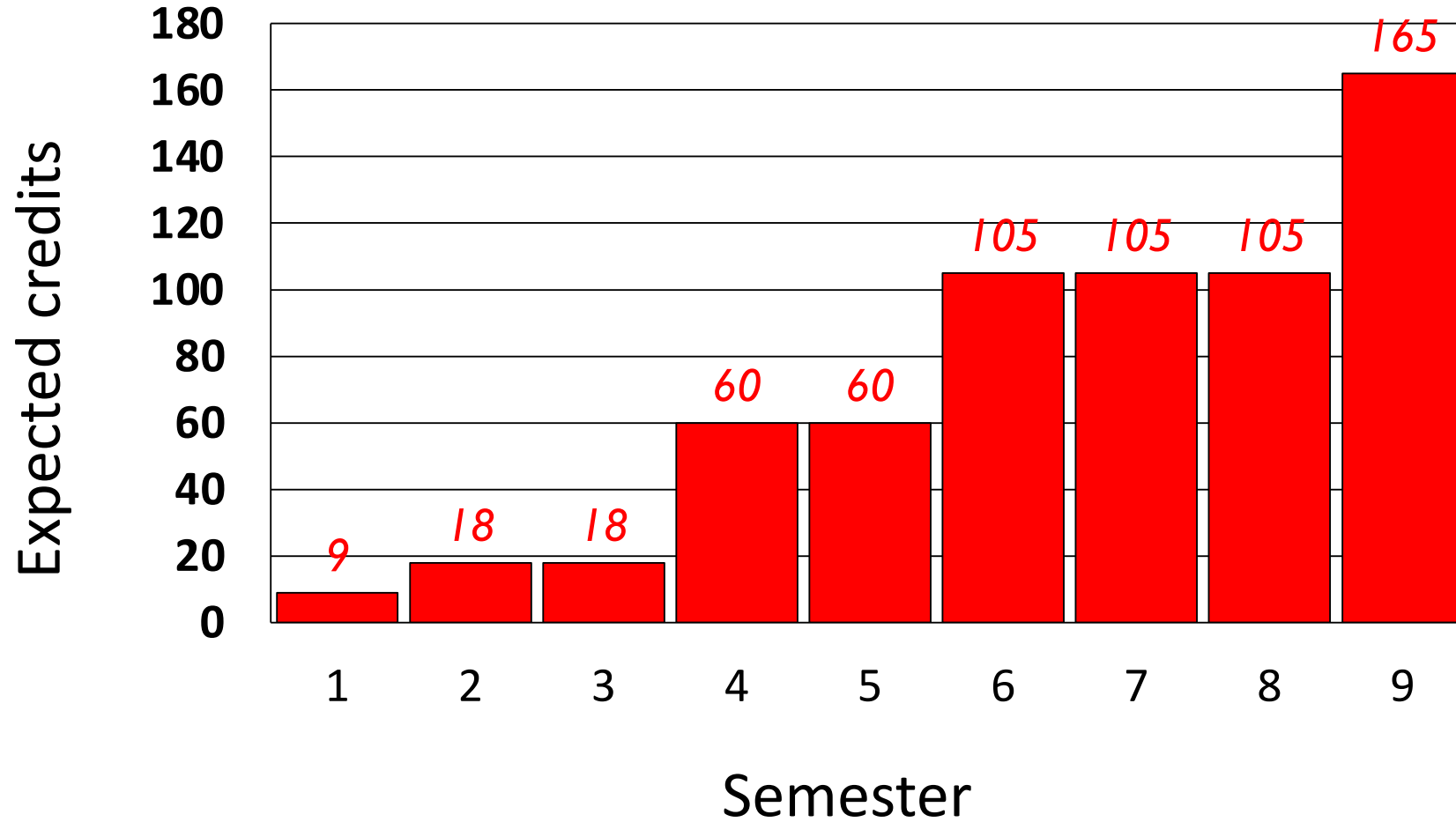


# Progress in regular study time





# Progress control





# Exam registration in Computer Science

- The main exam and the backup exam **each represent one examination attempt**, for which you must register separately. **There are three examination attempts per module!**
- For all **introductory lectures**, you will receive a free attempt if you pass the examination (written exam) within the standard study period at the first possible examination date (registration for the 4<sup>th</sup> attempt in the study coordination or examination office).  
Attention: Cryptography is not an introductory lecture.
- **Registration** for exams in HISPOS at the **latest one week before the exam (after that, even with the consent of the lecturer, registration is no longer possible!!!)**.
- **Deregistration** at the **latest one week** before the exam (after that, a doctor's certificate is required)
- Shortened deregistration period for proseminars, seminars, and ring lecture perspectives in computer science (**up to three weeks after topic assignment**)



## Vorlesungsverzeichnis (SoSe 2024)

Seitenansicht wählen: → kur.

- ① Vorlesungsverzeichnis
  - ① MI Fakultät für Mathematik und Informatik
    - ① Informatik
      - ① Studiengänge Cybersicherheit / Entrepreneurial Cybersecurity
        - ① Bachelor Cybersicherheit, StO 2020
          - ① Vertiefungsvorlesungen

Vst.-Nr.	Veranstaltung	Vst.-Art	Aktion
149440	<a href="#">Topics in Algorithmic Data Analysis</a> - Vreeken	Weiterführende Vorlesung	
150328	<a href="#">Privacy-Enhancing Technologies</a> - Lueks	Weiterführende Vorlesung	
150329	<a href="#">Foundations of Web Security</a> - Stock	Weiterführende Vorlesung	
150330	<a href="#">Attacks Against Machine Learning Models</a> - Zhang	Weiterführende Vorlesung	
150331	<a href="#">Distributed Graph Algorithms</a> - Brandt	Weiterführende Vorlesung	
150332	<a href="#">Parameterized Verification</a> - Jacobs	Weiterführende Vorlesung	
150333	<a href="#">Optimization for Machine Learning</a> - Stich	Weiterführende Vorlesung	
150334	<a href="#">Reactive Synthesis</a> - Dimitrova	Blockvorlesung	
150335	<a href="#">Physical-Layer Security</a> - Tippenhauer	Weiterführende Vorlesung	
150392	<a href="#">Recht der Cybersicherheit - Datenschutzrechtliche Aspekte</a> - Sorge	Weiterführende Vorlesung	
150739	<a href="#">Trustworthy Machine Learning</a> - Fritz , Boenisch , Dziedzic	Weiterführende Vorlesung	
151269	<a href="#">Usable Security</a> - Krombholz , Fassl	Blockvorlesung	

<https://www.lsf.uni-saarland.de/>



# Course Management System (CMS)



- [cms.cispa.saarland](https://cms.cispa.saarland)
- [cms.sic.saarland](https://cms.sic.saarland)

## Winter term 2023/2024

### Games in Machine Learning

Advanced Lecture - Tatjana Chavdarova, Sebastian Stich

### Machine Learning in Cybersecurity

Advanced Lecture - Mario Fritz

### Mobile Security

Advanced Lecture - Sven Bugiel

### Robustness in Machine Learning

Advanced Lecture - Xiao Zhang

### Security Testing

Advanced Lecture - Andreas Zeller

### Side-Channel Attacks and Defenses

Advanced Lecture - Michael Schwarz

### Systems Security

Advanced Lecture - Ali Abbasi, Thorsten Holz

### Elements of Machine Learning

Basic and Advanced Lecture - Krikamol Muandet and Jilles Vreeken

### Foundations of Cybersecurity

Basic Lecture - Ben Stock

### Security (WS 2023/2024)

Core Lecture - Thorsten Holz

### Verification

Core Lecture - Bernd Finkbeiner

### Perspectives of Entrepreneurial Cybersecurity

Lecture Series - Sven Bugiel, Giancarlo Pellegrino

### Cybersecurity Lab

Practical Training - Ben Stock

### CySec Project Winter Term '23/24

Project - CISPA

### Decision Procedures for Verification and Synthesis

Proseminar - Rayna Dimitrova

### Usable Security Research to Enhance Online Child Protection

Proseminar - Carolyn Guthoff, Katharina Krombholz

### Wireless and Mobile Security

Proseminar - Mridula Singh

### Advanced Theory of Secure Messaging

Seminar - Cas Cremers

### An Extravaganza of Algorithmic Models

Seminar - Sebastian Brandt, Alexandre Nolin

### Complexity of Games

Seminar - Dániel Marx, Tim Hartmann

### Machine Learning Security Reproducibility

Seminar - Lea Schönherr

### Mining Input Structures

Seminar - Rafael Dutra + Andreas Zeller

### New Developments in PETS

Seminar - Wouter Lueks

### Privacy of Machine Learning

Seminar - Yang Zhang

### Pruning deep neural networks for lottery tickets

Seminar - Rebekka Burkholz

### Static Program Analysis Lab

Seminar - Jordan Samhi + Andreas Zeller

### The Web Security Seminar

Seminar - Aurore Fass, Giancarlo Pellegrino, Cristian-Alexandru Staicu, Ben Stock



# Central registration for (Pro)Seminars

- All seminars and proseminars are assigned centrally.
  - Resolve problems from the past:  
Waiting lists, overbooked seminars, no places for some students
- <https://seminars.cs.uni-saarland.de>

SIC Seminars

**SIC** Saarland Informatics  
Campus

## Seminar Assignment

### Winter Term 2023

Proseminar Assignment Winter 2023/2024

Seminar Assignment Winter 2023/2024



# Stay abroad (“Auslandsaufenthalt”)











- Within Europe: ERASMUS
  - Numerous partner universities of the UdS computer science department
  - Contact person (current list of collaborations and implementation): **Study Coordination**
  - Studies for 1-2 semesters or internship
  - Request by **March 1** (for winter semester) or **September 1** (for summer semester)
- Non-European countries:
  - Coordinated by the International Office, Campus Center
  - Contact person USA: **Mr. Heintz**



# Introducing CISPA (1/2)

- CISPA – Helmholtz Center for Information Security
  - Member of the Helmholtz Association since 01/2019 (≈50M Euro funding / year)
  - New campus in St. Ingbert by 2027
- Currently, about 400 employees
  - 40+ Faculty and Senior Researchers, 200+ PhD students and postdocs, 60+ Hiwis
  - 120+ Administration / Scientific Services
- CISPA is among the world's elite in cybersecurity research
  - According to csrankings.org, currently the leading institution in the field of IT security world-wide



#	Institution	Count	Faculty
1	▶ CISPA Helmholtz Center  	74.3	23
2	▶ Georgia Institute of Technology  	53.9	26
3	▶ Purdue University  	37.5	20
4	▶ ETH Zurich  	37.2	17
5	▶ Carnegie Mellon University  	31.4	22





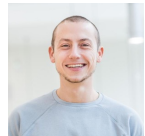
# Introducing CISPA (2/2)



Brandt



Döttling



Hanzlik



Joux



Loss



Lenzen



Marx



Sasy

**RA1: Algorithmic  
Foundations  
& Cryptography**



Backes



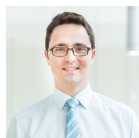
Boenisch



Burkholz



Dziejic



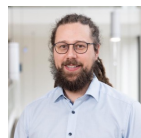
Fritz



Lueks



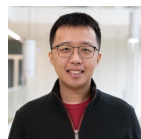
Muandet



Stich



Vreeken



X. Zhang



Y. Zhang

**RA2: Trustworthy  
Information Processing**



Cremers



Dimitrova



Finkbeiner



Jacobs

**RA3: Reliable Security  
Guarantees**



Holz



Schönherr



Schwarz



Zeller

**RA4: Threat Detections &  
Defenses**



Abbasi



Bugiel



Rossow



Singh



Tippenhauer

**RA5: Secure Connected  
and Mobile Systems**



Fahl



Fass



Golla



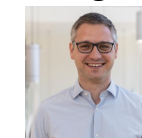
Krombholz



Pellegrino



Staicu



Stock

**RA6: Empirical and  
Behavioral Security**



# Career path for students at CISPA



- Outstanding students from courses can work as Hiwi (student assistant)
  - First, familiarization with the topic, then assignment to research projects
- As a student assistant, it is much easier to start with the bachelor's thesis
  - The goal is already the first proper publication
- Afterwards, Grad School for the doctorate
  - Various topics in IT security are possible
  - Top infrastructure at CISPA
- Future at CISPA Helmholtz Center for Information Security
- Or: Create a startup with the help of CISPA



# Points of contact

- **Always the first point of contact:** Fachschaft (Students Council)
  - E1 3, Room 109, <https://cs.fs.uni-saarland.de/>
- For examination matters: **Prüfungssekretariat** (Examination Office)
  - Responsible: Ellen Wintringer (cybersicherheit@ps-mint.uni-saarland.de)  
<https://www.ps-mint.uni-saarland.de/>
- **Studienkoordinatorin** (Study Coordinator): : E1 3, Room 209, via email:  
[studium@cs.uni-saarland.de](mailto:studium@cs.uni-saarland.de)
- Possibly further step:
  - **Dr. Ben Stock** (general contact person for the study program)  
Kaiserstraße 21, St. Ingbert - Appointment by agreement
  - **Prof. Christian Rossow** (examination matters)  
Appointment by agreement

# Viel Erfolg! Good Luck!

– Do you have criticism or suggestions for improvement? –  
Please feel free to contact us!

[stock@cispa.de](mailto:stock@cispa.de)



[https://www.reddit.com/r/cysec\\_memes/](https://www.reddit.com/r/cysec_memes/)  
[https://www.reddit.com/r/sic\\_memes/](https://www.reddit.com/r/sic_memes/)

