

Welcome to Cysec!

Dr.-Ing. Sven Bugiel

WS23/24 | 2023-10-23

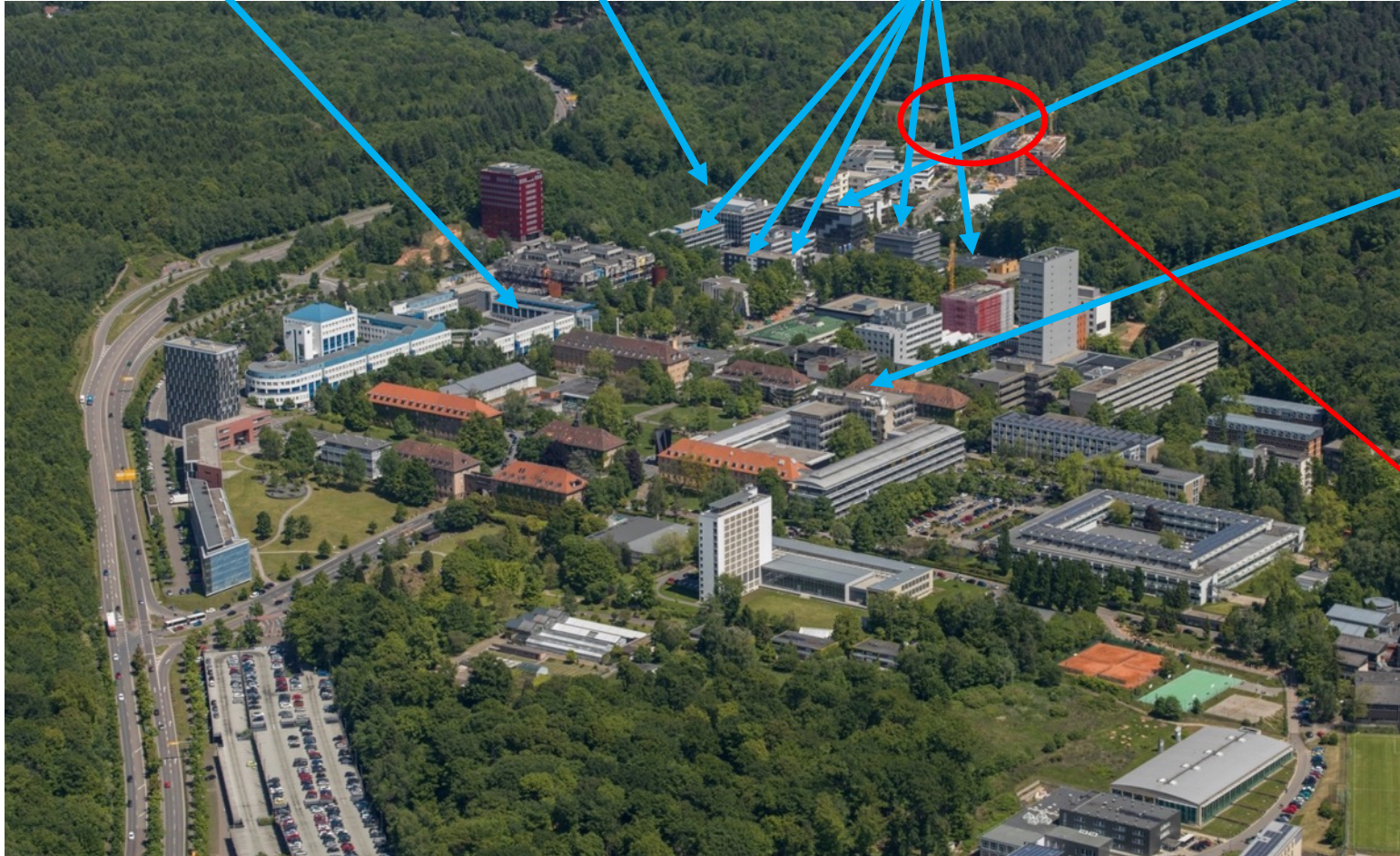


Welcome

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	Master	Staatsexamen	Doctorate
• Computer Science • Bioinformatics • Embedded Systems • Media Informatics • Cybersecurity • Cybersecurity (English), since WS 2021 • Mathematics and CS • Computational Linguistics • <i>Data Science and AI</i>	• Computer Science • Bioinformatics • Embedded Systems • Media Informatics • Visual Computing • Mathematics and CS • Language Science & Technology • <i>Data Science and AI</i> • Entrepreneurial Cybersecurity • Cybersecurity (since 2021)	• Lehramt Informatik (“Didactics of Informatics”)	• 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



Example Course of studies (English BSc)

1	Programming 1 (9 CP)	Mathematics for Computer Scientists 1 (9 CP)	Foundations of Cyber Security 1 (9 CP)	Mandatory elective: Intro to Python (3 CP)	30
2	Programming 2 (9 CP)	Mathematics for Computer Scientists 2 (9 CP)	Foundations of Cyber Security 2 (6 CP)	Language Courses (6 CP)	30
3	Cyber Security Lab (6 CP)	Introduction to Theoretical Computer Science (9 CP)	Fundamentals of Data Structures and Algorithms (6 CP)	Cyber Security Proseminar (5 CP)	26
4	Cryptography (9 CP)	System Architecture (9 CP)	Complementary Lecture Cyber Security (6 CP)	Statistics Lab (6 CP)	30
During the break between semesters: Software Engineering Lab (9 CP)					9
5	Advanced Lecture Cyber Security (6 CP)	Elements of Machine Learning (6 CP)	Complementary Lecture Cyber Security (6 CP)	Cyber Security Seminar (7 CP)	25
6	Advanced Lecture Cyber Security (6 CP)	Bachelor Seminar (9 CP)	Bachelor Thesis (12 CP)	Mandatory Elective: Language course (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

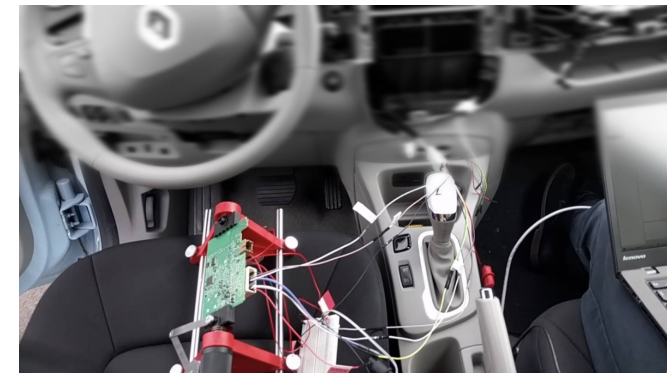
- Practical courses:
 - Web Security, Mobile Security
 - Physical-Layer Security, Side-Channel Attacks and Defenses
- Theoretical courses:
 - Privacy Enhancing Technologies
 - Verification
 - Accountability
- Complementary lectures:
 - Usable Security
 - Recht der Cybersicherheit
 - Data Analytics





Course of studies: practical focus

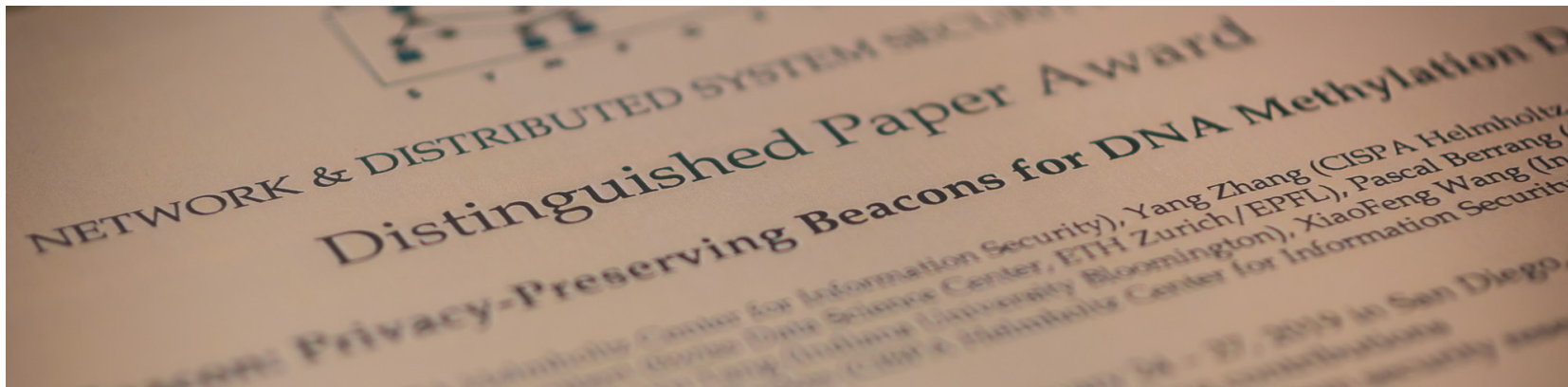
- Proseminar: Influential Papers in Web Security
- Adv. lecture 1: Physical-Layer Security
- Adv. lecture 2: Side Channels A&D
- Adv. lecture 3: Foundations of Web Security
- Seminar: Advanced Fuzzing Techniques
- Bachelor thesis: CAN-Bus Fuzzing to detect vulnerabilities or side-channels in cars?





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	Math 1	Prog 1	Math 1		
12-14	Sport	Reading	Food	Food	Sport		
14-16	Ring lect.	Prog 1	Sleeping	CySec 1	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			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							
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	Statistics Lab	Statistics Lab			Programmierung 2
-9					
-10					
-11					
-12					
-13					
-14		Programmierung 2		Foundations of Cyber Security 2 (Grundlagen der Cybersicherheit 2)	
-15					
-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

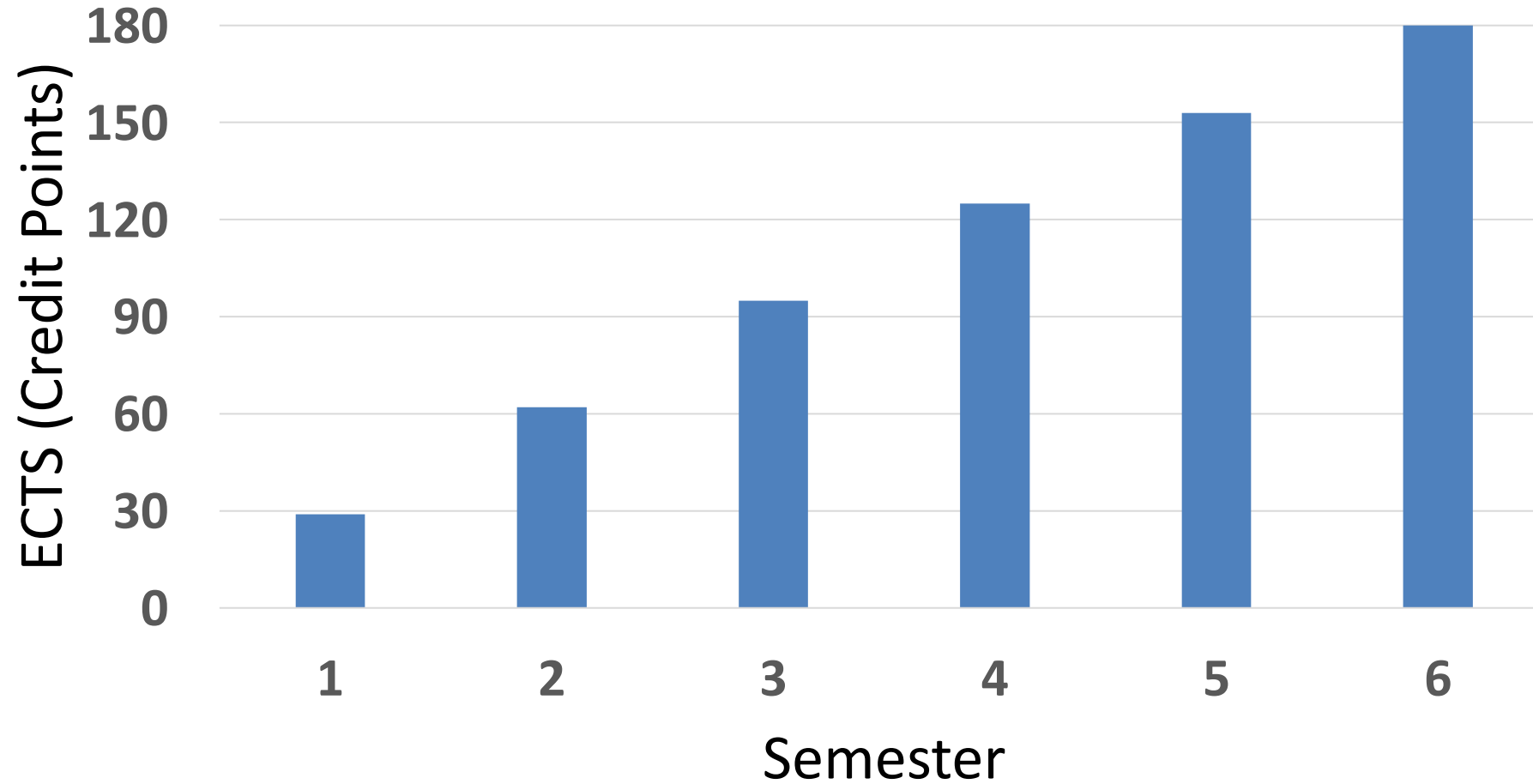
9 ECTS

Softwarepraktikum

Sven Apel - [LSF](#)

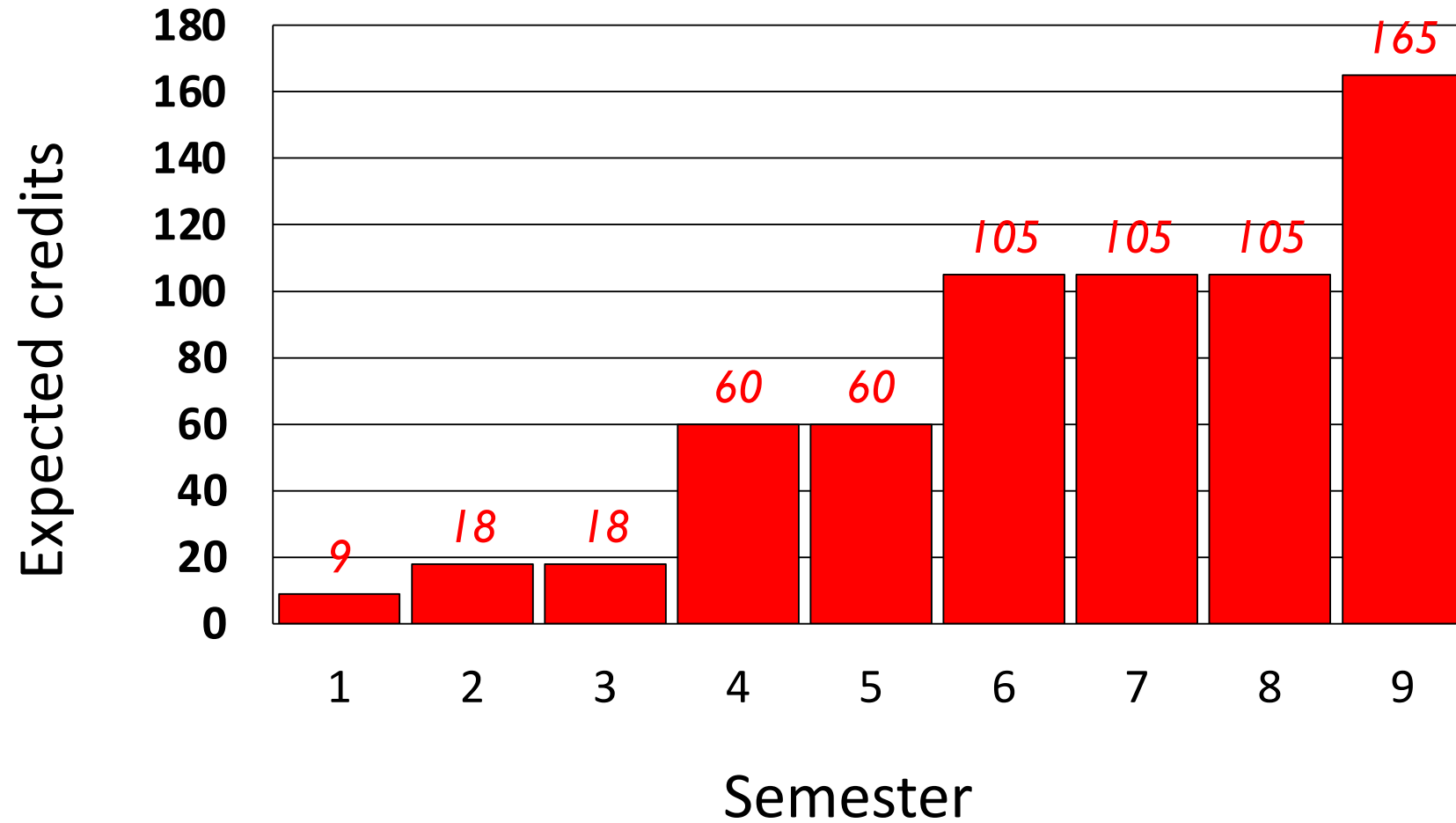


Progress in regular study time





Progress control





Prüfungsanmeldung in der Informatik

- Haupt- und Nachklausur stellen **jeweils einen Prüfungsversuch** dar, zu dem man sich separat anmelden muss. **Pro Modul gibt es drei Prüfungsversuche!**
- Für alle **Grundvorlesungen** erhalten Sie einen Freiversuch, wenn Sie die Prüfungsleistung (Klausur) in Regelstudienzeit beim erstmöglichen Prüfungstermin ablegen (Anmeldung zum 4. Versuch in Studienkoordination oder Prüfungssekretariat); Achtung: Cryptography ist keine GrdVL
- **Anmeldung zu Prüfungen** in HISPOS bis **spätestens eine Woche (danach ist selbst mit Zustimmung des Dozenten keine Anmeldung mehr möglich!!!)** vor der Klausur
- **Abmeldung** bis spätestens **eine Woche** vor der Klausur (danach Attest erford.)
- Verkürzte Rücktrittsfrist für Proseminare, Seminare und Perspektiven der Informatik (**bis drei Wochen nach Themenvergabe**)



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 4th 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**)



Course Overview (WiSe 2023/24)

View: → short →

① Vorlesungsverzeichnis

→ ① Mathematics and Computer Science

→ ① Computer Science

→ ① Courses on Cybersecurity / Entrepreneurial Cybersecurity

→ ① Bachelor Cybersicherheit, StO 2020

→ ① Vertiefungsvorlesungen

Lect.-No.	Lecture	Type	Activity
146217	Mobile Security - Bugiel	Advanced lecture	
147087	Robustness in Machine Learning - Zhang	Advanced lecture	
147094	Side-Chanel Attacks and Defenses - Schwarz	Advanced lecture	
147108	Games in Machine Learning - Stich	Advanced lecture	
147110	Security Testing - Zeller	Advanced lecture	
147126	Systems Security - Holz , Abbasi	Advanced lecture	
147458	Formal Methods in Security - Künnemann , Nemati , Patrignani , Cremers	Advanced lecture	
147460	Machine Learning in Cybersecurity - Fritz	Advanced lecture	

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



Course Management System (CMS)



- cms.cispa.saarland
- 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



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)
 - CISPA got its first own building end of 2015 (east entrance UdS)
 - 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



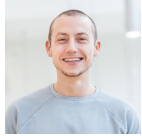
Introducing CISPA (2/2)



Brandt



Döttling



Hanzlik



Joux



Loss



Lenzen



Marx

**RA1: Algorithmic
Foundations
& Cryptography**



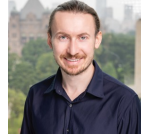
Backes



Boenisch



Burkholz



Dziedzic



Fritz



Lueks



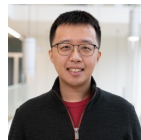
Muandet



Stich



Vreeken



X. Zhang



Y. Zhang

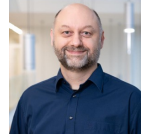
**RA2: Trustworthy
Information Processing**



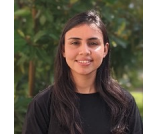
Cremers



Dimitrova



Finkbeiner



Golia



Jacobs

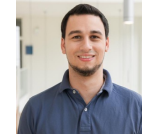
**RA3: Reliable Security
Guarantees**



Holz



Schönherr



Schwarz



Zeller

**RA4: Threat Detections &
Defenses**



Abbasi



Bugiel



Rossow

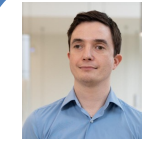


Singh



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
- 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!

bugiel@cispa.de & stock@cispa.de



https://www.reddit.com/r/cysec_memes/
https://www.reddit.com/r/sic_memes/

