**Brandenburgische Technische Universität Cottbus - Senftenberg**
**Platz der Deutschen Einheit 1, 03046 Cottbus**

Brandenburgische
Technische Universität
Cottbus - Senftenberg

# Modulhandbuch für den Studiengang Cyber Security (universitäres Profil), Master of Science, Prüfungsordnung 2017

## Inhaltsverzeichnis

# Module 11888 Master Thesis

assign to: Total Account

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11888 | Mandatory |

| | |
|---|---|
| **Modul Title** | **Master Thesis**<br>Master-Arbeit |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Panchenko, Andriy |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every semester |
| **Credits** | 30 |
| **Learning Outcome** | Students acquire the ability to solve a technical or scientific problem within a limited time budget under the guidance of a supervisor.<br>They use their acquired theoretical and practical knowledge to justify scientifically their solution of the problem as well as their improvments.<br>The development of new knowledge and techniques is a major objective.<br>They acquire the ability to present scientific facts clearly in written and oral form |
| **Contents** | The task can be of practical or theoretical nature and should correspond to challenging problems occurring in working life. To solve the task, the knowledge and methods from previous courses and the current scientific literature are to be applied and improved.<br>The technical content of the task is determined by the supervisor. It must be a related cyber security and must be confirmed by the examination board when registering. |
| **Recommended Prerequisites** | none |
| **Mandatory Prerequisites** | • At least 82 credits, including<br>• Module 11894 : Study Project<br><br>See special examination and study regulations for Cyber Security § 8. |
| **Forms of Teaching and Proportion** | Research paper/essay - 870 hours<br>Consultation - 15 hours<br>Seminar - 1 hours per week per semester |

| | |
|---|---|
| **Teaching Materials and Literature** | Literature references are provided by the supervisor at the beginning of the project.<br>The supervisor will also provide tools, equipment and documentation, depending on the topic. |
| **Module Examination** | Continuous Assessment (MCA) |
| **Assessment Mode for Module Examination** | • Master thesis, graded by at least two examinators, 75% of grade<br>The duration of the written work is limited to 5 months.<br>• Oral presentation and examination (defense), graded, 25% of grade<br><br>See examination and study regulations § 25, special examination and study regulations for Cyber Security § 8. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Cyber Security M.Sc.: Mandatory module |
| **Module Components** | • Consultations, according to agreement<br>• Intermediate presentation<br>• Final presentation (defense) |
| **Components to be offered in the Current Semester** | No assignment |

# Module 14144 Internship

assign to: Total Account

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 14144 | Mandatory |

| | |
|---|---|
| **Modul Title** | **Internship**<br>Berufspraktikum |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Panchenko, Andriy |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every semester |
| **Credits** | 10 |
| **Learning Outcome** | After successfully completing the module, students are able to understand, take on and work on a subtask of a larger project in a professional environment and document the results. They are familiar with the workflow and group organisation in professional environments. Students can apply the practical and theoretical knowledge they have acquired in the working world and assess the relevance of scientific approaches. |
| **Contents** | A time-limited task in the field of cyber security is handled in an external facility. The task is assigened by the external facility in agreement between the student's mentor and the external supervisor. |
| **Recommended Prerequisites** | The first year of study should be successfully completed. |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Practical training - 260 hours<br>Research paper/essay - 40 hours |
| **Teaching Materials and Literature** | Working materials, references, documentation will be provided by supervising facility. |
| **Module Examination** | Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | • Internship report, 3500 bis 4000 words<br>The internship report has to be delivered not later than 8 weeks after completion of the internship. It is examined by the student's mentor. |

| | |
|---|---|
| **Evaluation of Module Examination** | Study Performance – ungraded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Cyber Security M.Sc.: Mandatory module |
| **Module Components** | Internship |
| **Components to be offered in the Current Semester** | No assignment |

# Module 11859 Cryptography

assign to: Cyber Security Basics

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11859 | Mandatory |

| | |
|---|---|
| **Modul Title** | **Cryptography**<br>Kryptographie |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. habil Meer, Klaus<br>Prof. Dr. rer. nat. Averkov, Gennadiy |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every summer semester |
| **Credits** | 8 |
| **Learning Outcome** | The students should<br>• know relevant symmetric and asymmetric crypto systems<br>• understand the mathematics relevant for desgining and analyzing crypto systems<br>• be able to explain and use the most important approaches to cryptography<br>• gain the ability to understand state-of-the-art scientific work in the area of cryptography |
| **Contents** | • Mathematical Foundations relevant in the context of cryptography, including basic number theory, finite fields, polynomial rings, factorization<br>• elementary crypto systems<br>• Symmetric Cryptosystems DES and AES<br>• public key cryptography, RSA - discrete logarithm, elliptic curve systems<br>• secure signature and authentication methods<br>• security of crypto systems<br>• zero knowledge proofs<br>• complexity theoretic aspects |
| **Recommended Prerequisites** | Basic knowledge about discrete mathematics and linear algebra, for example as covered by the modules<br>• 11101: Lineare Algebra und analytische Geometrie I<br>• 11102: Lineare Algebra und analytische Geometrie II |

| | |
|---|---|
| | or<br>• 11112: Mathematik IT-1 (Diskrete Mathematik)<br>• 11113: Mathematik IT-2 (Lineare Algebra) |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 4 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 150 hours |
| **Teaching Materials and Literature** | **Books in English**<br>• G. Baumslag, B. Fine, M. Kreuzer, G. Rosenberger: A Course in Mathematical Cryptography, De Gruyter, 2015<br>• J. Hoffstein, J. Pipher, J.H. Silverman: An Introduction to Mathematical Cryptography, 2nd Edition, Springer 2014.<br>• D.R. Stinson: Cryptography: Theory and Practice, CRC, 1995<br><br>**Books in German**<br>• V. Diekert, M. Kufleitner, G. Rosenberger: Diskrete Algebraische Methoden, De Gruyter 2013 |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful completion of homework (fortnightly) and/or successful completion of tests (approx. 4 tests of 15-30 minutes each, written during the lecture period)<br><br>**Final module examination:**<br>• Written examination, 90 minutes, **OR**<br>• Oral examination, 30 - 45 minutes, (in case of a small number of participants)<br><br>In the first lecture it will be anounced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | 80 |
| **Remarks** | • Study programme Cyber Security M.Sc.: Mandatory module in complex „Cyber Security Basics“<br>• Study programme Informatik M.Sc.: Compulsory elective module in complex „Mathematik“ or in field of application „Mathematik“<br>• Study programme Artificial Intelligence M.Sc.: Compulsory elective module in complex „Advanced Methods“<br>• Study programme Angewandte Mathematik M.Sc.: Compulsory elective module in complex „Analysis / Algebra / Kombinatorik“<br>• Study programme Mathematik B.Sc.: Compulsory elective module in complex „Vertiefung“, in limited extend<br>• Study programme Wirtschaftsmathematik B.Sc.: Compulsory elective module in complex „Vertiefung“, in limited extend<br>• Study programme Physics M. Sc.: Compulsory elective module in complex „Minor Subject" |

| | |
|---|---|
| | • Study programme Mathematics M.Sc.: Compulsory elective module in complex „Analysis / Algebra / Combinatorics“<br>• Study programme Mathematical Data Science M.Sc.: Compulsory elective module in complex „Fundamentals of Data Science“ |
| **Module Components** | • Lecture: Cryptography<br>• Accompanying exercises<br>• Related examination |
| **Components to be offered in the Current Semester** | **120164** Examination<br>Cryptography (Wiederholung) |

# Module 11889 Introduction to Cyber Security

assign to: Cyber Security Basics

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11889 | Mandatory |

| | |
|---|---|
| **Modul Title** | **Introduction to Cyber Security**<br>Einführung in die IT-Sicherheit |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Panchenko, Andriy |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every winter semester |
| **Credits** | 8 |
| **Learning Outcome** | After successfully completing the module, students<br>• have basic knowledge of IT security,<br>• know the technical terms to understand current publications and relevant system solutions,<br>• are able to independently familiarise themselves with advanced IT security concepts and to acquire futher skills<br>• are able to apply the acquired knowledge to concrete problems. |
| **Contents** | **Lecture**<br>Introductory definition of technical terms; protection objectives; security risks and threats; Malware; Attack techniques; security functions and services; Access control; basic cryptographic functions: symmetric crypto systems (stream and block ciphers, DES, AES)h public key cryptography (RSA, El-Gamal, ECC), Subject and object authentication (cryptographic hash values, message authentication codes), digital signatures, key management; cryptographic protocols (Diffie-Hellmann, Kerberos, Needham-Schröder, and others); protection of IT infrastructures, firewalls, intrusion detection; honeypots;<br>**Laboratory**<br>Experiments on attacks and defence techniques |
| **Recommended Prerequisites** | none |
| **Mandatory Prerequisites** | No successful participation in module *13969 - Introduction to Cyber Security*. |
| **Forms of Teaching and Proportion** | Lecture - 4 hours per week per semester |

| | |
|---|---|
| | Practical training - 2 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 120 hours |
| **Teaching Materials and Literature** | • Stallings: Cryptography and Network Security: Principles and Practice, Pearson<br>• Paar, Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners, Springer |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful treatment of all assigned project tasks including successful presentation of the results in the laboratory course<br><br>**Final module examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30-45 min. (with small number of participants)<br><br>In the first lecture it will be anounced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Cyber Security M.Sc.: Mandatory module<br>• Study programme Informatik M.Sc.: Compulsory elective module in complex „Angewandte und technische Informatik“ (level 400) |
| **Module Components** | • Lecture: Introduction into Cyber Security<br>• Accompanying laboratory<br>• Related examination |
| **Components to be offered in the Current Semester** | **120510** Lecture<br>Introduction to Cyber Security - 4 Hours per Term<br>**120511** Exercise<br>Introduction to Cyber Security - 2 Hours per Term<br>**120514** Examination<br>Introduction to Cyber Security |

# Module 11891 IT Security Law

assign to: Cyber Security Basics

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11891 | Mandatory |

| | |
|---|---|
| **Modul Title** | **IT Security Law**<br>IT-Sicherheitsrecht |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Panchenko, Andriy |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every winter semester |
| **Credits** | 6 |
| **Learning Outcome** | The student acquire basic knowledge in data protection law with references to data security, in order to carry out appropriate IT tasks in a company and communicate with data protection officers and legal department, or to audit and consult companies. They also acquire comprehension of basic principles of the IT security law, in order to be able to communicate with the Federal Office for Information Security. Furthermore they get to know principles of the EU Directive on security of network and information systems (NIS Directive) and the Federal NIS Directive Implementation Act, likewise principles of the criminal offenses related to IT security, in order to recognize in practice whether the legal department should be informed in the event of an incident. |
| **Contents** | • Basic concepts and principles of data protection law - EU General Data Protection Regulation and German Accompanying Law<br>• Legal requirements for technical and organizational measures for data protection<br>• Oblication to report unlawful acsess to data<br>• Legal challenge in third country transfer of personal data<br>• Data processing and technical / organizational measures for data security<br>• Impact assessment<br>• Legal requirement for IT security management<br>• Data protection by design and by default<br>• IT Security Law and the KRITIS Regulation<br>• EU Directive on Network and Information Security (NIS Directive)<br>• NIS Directive Implementation act |

| | |
|---|---|
| | • Law on computer crime: computer sabotage, § 303b Criminal Code (StGB), preparation, conduct of the spying out and interception of electronic data, § 202a StGB; Computer fraud, § 263a StGB, Data modification, § 303a StGB |
| **Recommended Prerequisites** | none |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 4 hours per week per semester<br>Self organised studies - 120 hours |
| **Teaching Materials and Literature** | Will be provided at the beginning of the course. |
| **Module Examination** | Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | • Written examination, 90 min. **OR**<br>• Oral examination, 30-45 min. (with small number of participants)<br>In the first lecture it will be anounced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Cyber Security M.Sc.: Mandatory module |
| **Module Components** | • Lecture: IT Law<br>• Related examination |
| **Components to be offered in the Current Semester** | **120030** Lecture<br>IT Security Law - 4 Hours per Term<br>**120031** Examination<br>IT Security Law |

# Module 11894 Study Project

assign to: Specialised Modules

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11894 | Mandatory |

| | |
|---|---|
| **Modul Title** | **Study Project**<br>Studienprojekt |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Panchenko, Andriy |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every winter semester |
| **Credits** | 8 |
| **Learning Outcome** | Acquisition of practical skills and deepening of knowledge in a field of cyber security, in particular:<br>• Deep insight of the state of the art on the area defined by the project task<br>• Ability to acquaint autonomously new knowledge in the field of IT security<br>• Ability to apply existing and new knowledge to solve the project task<br>• Ability to carry out projects (project planning, time management, communication, ...)<br>• Ability to cooperate with other developers<br>• Ability to work on a specific task within a given deadline, independently and successfully |
| **Contents** | In the study project, the participants will acquire practical skills in the application of machine learning (ML) techniques in the area of IT security in adversarial settings. The field of ML is playing an ever increasing role in computer science in general and IT security in particular. The idea of the study project is to mount different attacks and/or implement and evaluate defenses against them.<br>The students will develop scripts to automate the process of executing the attacks and/or defenses. By doing so, they will collect datasets / artifacts that will be used for further analysis, feature engineering and extraction, training and testing of different machine learning techniques. Finally, the students will analyze the results in the form of different quality metrics, and will present the results and write a report. |

| | |
|---|---|
| | In the form of a self organized study project, the students get familiar and/or deepen their knowledge in machine learning and their applications to cyber security. The participants get deep insights in the state-of-the-art research in ML for cyber security and apply the existing knowledge to build, test, and evaluate their own attacks and defenses. For each project the following work steps have to be accomplished:<br>• Getting acquainted with the state of the art<br>• Acquisition of new knowledge in self-study<br>• Project planning<br>• Selection of the methods to be used<br>• Elaboration of a solution approach<br>• Implementation of the solution approach as a prototype<br>• Testing / evaluating the prototype<br>• Documentation<br>• Final colloquium<br><br>The module is carried out as a project study in groups of 2 students. |
| **Recommended Prerequisites** | • Solid knowledge in the field of the project.<br>• Knowledge of at least one programming language and one scripting language. At the beginning of the course this knowledge is gonna be assessed. |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Consultation - 1 hours per week per semester<br>Study project - 165 hours<br>Self organised studies - 60 hours |
| **Teaching Materials and Literature** | Depending on the project the relevant information will be provided at the beginning of the module. |
| **Module Examination** | Continuous Assessment (MCA) |
| **Assessment Mode for Module Examination** | • Executable and tested prototype (50% of total marks)<br>• Complete documentation (20% of total marks)<br>• Successful intermediate presentation of results (10% of total marks)<br>• Successful final presentation of results (20% of total marks)<br><br>Task-oriented scope of each performance. 75% of the total marks are needed to pass the module. |
| **Evaluation of Module Examination** | Study Performance – ungraded |
| **Limited Number of Participants** | 30 |
| **Remarks** | • Study programme Cyber Security M.Sc.: Mandatory module<br>• Study programme Informatik M.Sc.: Compulsory elective module in complex „Seminare oder Praktika“ (level 400)<br><br>For repeaters, the module is also offered occasionally in the summer semester. |
| **Module Components** | none |

| | |
|---|---|
| **Components to be offered in the Current Semester** | **120520** Study project<br>Study Project Adversarial Machine Learning |

# Module 11862 Pervasive System Security

assign to: Cyber Security Methods

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11862 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Pervasive System Security**<br>Sicherheit in Pervasiven Systemen |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. Langendörfer, Peter |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every winter semester |
| **Credits** | 6 |
| **Learning Outcome** | Upon completion of the module, students will know the basics of security in pervasive systems. They will know the different fields of work in which the systems are used, such as telemedicine and homeland security. They are able to identify security requirements and threats to privacy. They understand how the means presented are used to ensure security requirements. They are able to apply different algorithms in the field. They will be able to analyze security protocols and analyze their weaknesses. |
| **Contents** | This lecture introduces different kinds of pervasive systems considering diverse application areas such as telemedicine and homeland security. These examples are used to elaborate security and privacy requirements as well as threats against these goals. Then means ensuring the security goals will be introduced, here a clear focus is on cryptographic systems as the means of implementing security goals. Selected security protocols e.g. for key exchange, digital signature generation/verification, etc. will be discussed taking into account their limitations and means to successfully attack those protocols.<br>Topics covered include in particular:<br>• Topology, functionality and limitations of pervasive systems in different application areas.<br>• Symmetric and asymmetric cryptosystems<br>• Security protocols for key exchange<br>• Generation and verification of digital signatures<br>• Security aspects in the algorithms and their implementations<br>• Security vulnerabilities of the protocols and possible attack targets<br>• Privacy protection issues |

- Physical attacks and their classification
- Side channel attacks (SCA) on encryption means and appropriate countermeasures
- Physical processes exploited for SCA; basics of measurement
- Fault injection (FI) attacks, physical basics and suitable countermeasures

**Recommended Prerequisites**

Knowledge of the content of the modules
- 11454: Grundlagen der Rechnernetze
- 11864: Wireless Sensor Networks: Concepts, Protocols and Applications
- 11859: Cryptography

as well as basics in mathematics and physics.

**Mandatory Prerequisites**

none

**Forms of Teaching and Proportion**

Lecture - 2 hours per week per semester
Exercise - 1 hours per week per semester
Self organised studies - 135 hours

**Teaching Materials and Literature**

- Paar, C., Pelzl, J. (2010): Understanding Cryptography - A Textbook for Students and Practitioners, Springer
- Schneier, Bruce (1996): Applied Cryptography : Protocols, Algorithms, and Source Code in C, Wiley
- F. Koeune, F. Standaert (2005): A Tutorial on Physical Security and Side-Channel Attacks, Springer
- Ross Anderson (2020): Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition, Wiley

**Module Examination**

Prerequisite + Final Module Examination (MAP)

**Assessment Mode for Module Examination**

**Prerequisite:**
- Successful completion of homework **OR** successful completion of two intermediate written examinations in the course (at least 50% per submission)

**Final module examination:**
- Written examination, 90 min. **OR**
- Oral examination, 30 min. (with small number of participants)

In the first lecture it will be anounced, which type of prerequisite must be fulfilled and if the examination will be offered in written or oral form.

**Evaluation of Module Examination**

Performance Verification – graded

**Limited Number of Participants**

none

**Remarks**

- Study programme Informatik M.Sc.: Compulsory elective module in "Angewandte und technische Informatik" (level 400)
- Study programme Cyber Security M.Sc.: Compulsory elective module in complex "Cyber Security Methods"
- Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Software-basierte Systeme“

| | |
|---|---|
| **Module Components** | • Lecture: Pervasive System Security<br>• Accompanying exercises<br>• Related examination |
| **Components to be offered in the Current Semester** | **122250** Lecture/Exercise<br>Pervasive System Security - 3 Hours per Term<br>**122251** Examination<br>Pervasive System Security |

# Module 11863 Hands on Knowledge for Side Channel Attacks

assign to: Cyber Security Methods

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11863 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Hands on Knowledge for Side Channel Attacks**<br>Praxis der Seitenkanal-Angriffe |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. Langendörfer, Peter |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every summer semester |
| **Credits** | 6 |
| **Learning Outcome** | This module aims at providing basic knowledge – theoretical and practical – for successfully conducting side channel attacks. |
| **Contents** | Even for successfully applying basic side channel attacks such as „Simple Power Analysis“ or „Simple Electromagnetic Analysis“ knowledge in different areas is essential:<br>• Thorough understanding of cryptographic algorithms<br>• Good knowledge about measurement and<br>• Analysis and evaluation tools<br><br>In this mdule the necessary skills will be taught theoretically first. Afterwards they are applied by the students in the crypto hardware laboratory of IHP (Innovations for High Performance Microelectronics). The devices used for practical training have been designed and manufactured at IHP. So there are AES and ECC implementations available for experiments. The power analysis will be based on pre-recorded simulation and measurement results. |
| **Recommended Prerequisites** | Firm knowledge of module<br>• 11862 Pervasive System Security |
| **Mandatory Prerequisites** | • Successful participation in module *11862 - Pervasive System Security*.<br>• No successful participation in module *14478 - Praxis der Seitenkanal-Angriffe*. |
| **Forms of Teaching and Proportion** | Lecture - 1 hours per week per semester |

| | |
|---|---|
| | Consultation - 1 hours per week per semester<br>Practical training - 2 hours per week per semester<br>Self organised studies - 120 hours |
| **Teaching Materials and Literature** | Are handed out at the beginning of the module |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful implementation of the experiments in the lab, analysis of the traces<br><br>**Final module examination:**<br>• Final presentation of the experimental results including a short oral examination, 45-60 min. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Cyber Security M.Sc.: Compulsory elective module in complex "Cyber Security Methods"<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Software-baierte Systeme“<br><br>Due to the limited space available in the laboratory rooms of the IHP the module responsible should be contacted at an early stage. |
| **Module Components** | • Lecture/Practical training: Hands on Knowledge for Side Channel Attacks including consultations<br>• Subsequent block laboratory in the laboratory rooms of the IHP during the lecture free period.<br>• Examination: Hands on Knowledge for Side Channel Attacks |
| **Components to be offered in the Current Semester** | **122290** Examination<br>Hands on Knowledge for Side Channel Attacks (Re-examination) |

# Module 11892 Software Security

assign to: Cyber Security Methods

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11892 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Software Security**<br>Softwaresicherheit |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. Lambers, Leen |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | On special announcement |
| **Credits** | 6 |
| **Learning Outcome** | After successfully completing the module, students have acquired knowledge of methods and tools for the design and analysis of secure software systems. They are able to apply and evaluate methods and tools to design and analyze secure software systems. They are able to independently develop and present specialized knowledge in the field of software security. |
| **Contents** | • Methods and tools for the design and analysis of secure software systems<br>• Ethical and social aspects related to software security. |
| **Recommended Prerequisites** | Knowledge of:<br>• basics of software engineering<br>• basics in mathematics (logic, algebra, number theory) |
| **Mandatory Prerequisites** | No successful participation in module *11478 - Softwaresicherheit*. |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 120 hours |
| **Teaching Materials and Literature** | • Gary McGraw, Software Security: Building Security In. Addison Wesley, 2006<br>• Ross Anderson: Security Engineering, Wiley, 2001<br>• Jan Jürjens: Secure Systems Development with UML, Springer, 2010<br>• Eduardo Fernandez-Buglioni: Security Patterns in Practice: Designing Secure Architectures Using Software Patterns, Wiley, 2013 |

| | |
|---|---|
| | • Software Security: Principles, Policies, and Protection, HexHive Books, http://nebelwelt.net/SS3P/, Mathias Payer, 2021 |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful treatment of exercise tasks including successful presentation of results in the exercise courses (75% must be reached)<br><br>**Final Module Examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30-45 min. (with small number of participants)<br><br>In the first lecture it will be anounced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Computer Science M.Sc.: Compulsory elective module in complex „Practical Computer Science“ (level 400)<br>• Study programme eBusiness M.Sc.: Compulsory elective module in complex „Development and Deployment of eBusiness Systems“<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Cyber Security Methods“<br>• Study programme Applied Mathematics M.Sc.: Compulsory elective module in complex „Applications“, field „Computer Science“<br><br>If there is no need that the module is taught in English, alternatively the german version 11478 „Softwaresicherheit“ may be offered instead. |
| **Module Components** | • Lecture: Software Security<br>• Accompanying exercise<br>• Related examination |
| **Components to be offered in the Current Semester** | **120650** Examination<br>Software Security (Wiederholungsprüfung) |

# Module 11897 Security of Resource-constraint Systems

assign to: Cyber Security Methods

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11897 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Security of Resource-constraint Systems**<br>Sicherheit von Resourcen-beschränkten Systemen |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. Langendörfer, Peter |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Each winter semester even year |
| **Credits** | 6 |
| **Learning Outcome** | The Students know potential security issues of embedded systems. They can analyse embedded systems and identify security issues. They know standard approaches that can help to solve security issues and can develop security concepts for embedded systems. |
| **Contents** | • Potential attacks and attacker models<br>• Micro controller architectures<br>• Memory management<br>• Operating systems<br>• Micro Kernels<br>• Hypervisor<br>• Security protocols |
| **Recommended Prerequisites** | Knowledge of the content of the modules<br>• 12204 : Operating Systems I<br>• 12339 : Operating Systems II (Multi-Level Memory Management) |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 120 hours |
| **Teaching Materials and Literature** | Information about current literature will be provided at the beginning of the course. |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |

| | |
|---|---|
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful completion of homework **OR** successful completion of two intermediate written examinations in the course<br><br>**Final module examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30 min. (with small number of participants)<br><br>In the first lecture it will be anounced, which type of prerequisite must be fulfilled and if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | 40 |
| **Remarks** | • Study programme Computer Science M.Sc.: Compulsory elective module in "Applied and Technical Computer Science" (level 400)<br>• Study programme Information and Media Technology M.Sc.: Compulsory elective module in "Dependable HW/SW-Systems"<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex "Cyber Security Methods" |
| **Module Components** | • Lecture: Security of Resource-constraint Systems (HW/SW)<br>• Accompanying exercise<br>• Related examination |
| **Components to be offered in the Current Semester** | **122210** Lecture/Exercise<br>Security of Resource-constraint Systems - 4 Hours per Term<br>**122211** Examination<br>Security of Resource-constraint Systems |

# Module 11898 Cyber Security Lab

assign to: Cyber Security Methods

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11898 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Cyber Security Lab**<br>Praktikum IT-Sicherheit |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Panchenko, Andriy |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | On special announcement |
| **Credits** | 6 |
| **Learning Outcome** | The students should<br>• acquire basic knowledge of security vulnerabilities in IT systems,<br>• understand basic attack techniques,<br>• acquire practical skills for detecting and defending attacks. |
| **Contents** | The laboratory is conducted in groups of two.<br>The following work steps are performed for each project task:<br>• getting acquainted eith the current state of knowledge related to the project task,<br>• elaboration of a solution approach,<br>• implementing the solution approach in a prototypical operating or computer network environment,<br>• documentation,<br>• final colloquium. |
| **Recommended Prerequisites** | Solid knowledge about computer networks, operating systems (Unix) and system programming as well as topics of module<br>• 11889: Introduction into Cyber Security |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Consultation - 1 hours per week per semester<br>Study project - 105 hours<br>Self organised studies - 60 hours |
| **Teaching Materials and Literature** | Depending on the project the relevant information will be provided at the beginning of the laboratory. |

| | |
|---|---|
| **Module Examination** | Continuous Assessment (MCA) |
| **Assessment Mode for Module Examination** | • Successful completion of the practical tasks including documentation (70% of total score)<br>• Final colloquium, 15 minutes (30% of total score)<br><br>Task-oriented scope of each performance. 90% of the total score are required to pass the module. |
| **Evaluation of Module Examination** | Study Performance – ungraded |
| **Limited Number of Participants** | 25 |
| **Remarks** | • Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Cyber Security Methods“<br>• Study programme Informatik M.Sc.: Compulsory elective module in complex „Seminare oder Praktika“ (level 400) |
| **Module Components** | • Laboratory:  Cyber Security Lab<br><br>At the beginning there is an introductory meeting in which the project tasks, the boundary conditions for the tasks as well as operating or computer network environment are presented. |
| **Components to be offered in the Current Semester** | No assignment |

# Module 11899 Cyber Security Application Areas

assign to: Cyber Security Methods

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11899 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Cyber Security Application Areas**<br>IT Sicherheit in ausgewählten Anwendungsfeldern |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. Langendörfer, Peter |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | On special announcement |
| **Credits** | 6 |
| **Learning Outcome** | The students should<br>• learn about security incidents,<br>• be able to assess the complexity of the attacks,<br>• be aware of the interrelationships of different security/safety issues,<br>• be able to determine basic countermeasure for selected attacks. |
| **Contents** | In this module security issues of different application areas will be introduced. The application fields investigated are automotive, automation industry, critical infrastructures e.g. drinking/waste water systems or public transport, but also financial systems. The core of the lecture are security incidents reported in the past. These incidents will be examined and the reasons why they were successful will be explained. |
| **Recommended Prerequisites** | Basic knowledge in computer networks and programming. |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 120 hours |
| **Teaching Materials and Literature** | Will be delivered at the beginning of the course. |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:** |

| | |
|---|---|
| | • Successful completion of homework **OR** successful completion of two intermediate written examinations in the course<br><br>**Final module examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30 min. (with small number of participants)<br><br>In the first lecture it will be anounced, which type of prerequisite must be fulfilled and if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Cyber Security M.Sc.: Compulsory elective module in complex "Cyber Security Methods"<br>• Study programme Computer Science M.Sc.: Compulsory elective module in "Applied and Technical Computer Science" (level 400) |
| **Module Components** | • Lecture: Cyber Security Application Areas<br>• Accompanying exercise<br>• Related examination |
| **Components to be offered in the Current Semester** | **122220** Lecture/Exercise<br>Cyber Security Application Areas - 4 Hours per Term<br>**122221** Examination<br>Cyber Security Application Areas |

# Module 12790 Seminar Advanced Topics in Network and System Security

assign to: Cyber Security Methods

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 12790 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Seminar Advanced Topics in Network and System Security**<br>Seminar Fortgeschrittene Themen in Netzwerk- und Systemsicherheit |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Panchenko, Andriy |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | On special announcement |
| **Credits** | 6 |
| **Learning Outcome** | Students have a deeper understanding of distributed vs. centralized communication, security and privacy paradigms and their application in collaborative environments. They are capable to establish links between the basic concepts and applied scenarios, with reference to ongoing research activities within the research group IT Security.<br>Students are prepared for the Master's thesis. |
| **Contents** | Concrete topics and application scenarios are adapted to the focus of the discussed methods. Typical topics are network and system security, anonymity, privacy enhancing technologies, digital forensics, computer networks, distributed systems, mobile security, web security, applied cryptography, etc.<br>Master students will get assigned a topic that is based on recent publications in one of the top conferences in the field (e.g., IEEE S&P, ACM CCS, NDSS, USENIX Security, PETS) and have to prepare a paper on the state of the art on their topic. In this time, we will have presentations on ongoing research of our group members as well as streaming of presentations from top conferences in the field with the follow-up internal discussion. Depending on the format, it is also possible that in the second phase, students will be asked to write a conference-style review for a few papers of the others. These reviews will be presented and publicly discussed. Next, based on the reviews, students will have the possibility to improve their paper and have to prepare a presentation on their topic. Before publicly presenting it to the class, they have to make a test presentation by their supervisor. Finally, there will be a presentation and discussion within the class. |

| | |
|---|---|
| **Recommended Prerequisites** | Solid knowledge in the field of the seminar |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Seminar - 2 hours per week per semester<br>Research paper/essay - 60 hours<br>Self organised studies - 60 hours |
| **Teaching Materials and Literature** | Literature references for individual retrieval will be provided at the beginning of the seminar. |
| **Module Examination** | Continuous Assessment (MCA) |
| **Assessment Mode for Module Examination** | • Successful oral presentation, 30-45 minutes depending on topic (50% of total marks)<br>• Written report, 10-15 pages depending on topic (30% of total marks)<br>• Active participation in courses (20% of total marks)<br><br>75% of the total marks are needed to pass the module. |
| **Evaluation of Module Examination** | Study Performance – ungraded |
| **Limited Number of Participants** | 15 |
| **Remarks** | • Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Cyber Security Methods“<br>• Study programme Informatik M.Sc.: Compulsory elective module in complex „Seminare oder Praktika“ (level 400)<br>• Study programme eBusiness M.Sc.: Compulsory elective module in main focus: „Development and Deployment of eBusiness Systems“<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Seminare oder Praktika“<br>• Study programme Mathematical Data Science M.Sc.: Compulsory elective module in complex „Data Science Applications“ |
| **Module Components** | Seminar Advanced Topics in Network and System Security |
| **Components to be offered in the Current Semester** | **120530** Seminar<br>Research Seminar "Advanced Topics in Network and System Security" - 2 Hours per Term |

# Module 12973 Network and System Security

assign to: Cyber Security Methods

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 12973 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Network and System Security**<br>Netzwerk- und Systemsicherheit |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Panchenko, Andriy |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every summer semester |
| **Credits** | 6 |
| **Learning Outcome** | Students will get familiar with challenges in securing computer systems and networks. They will get acquainted with fundamental security and privacy concepts that will be used as building blocks for later specialization. |
| **Contents** | In the scope of this module, we explore, among others, the following topics:<br>• Anonymity and Privacy (mixes, onion routing, Tor<br>• Firewalls<br>• Malware, Botnets, and Intrusion Detection<br>• Exploits<br>• Wireless Security<br>• Physical Security<br>• Biometrics<br>• Access Control<br>• Electronic Payments<br>• E-voting<br>• Digital Rights Management |
| **Recommended Prerequisites** | Knowledge of the contents of modules<br>• 11859 *Kryptographie*<br>• 11889 *Einführung in die IT-Sicherheit* |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 2 hours per week per semester |

| | |
|---|---|
| | Self organised studies - 120 hours |
| **Teaching Materials and Literature** | Provided on the homepage of the chair. |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful treatment of all assigned project tasks including successful presentation of the results<br><br>**Final module examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30-45 min. (with small number of participants)<br><br>In the first lecture it will be anounced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Cyber Security Methods“<br>• Study programme Informatik M.Sc.: Compulsory elective module in complex „Angewandte und technische Informatik“ (level 400)<br>• Study programme eBusiness M.Sc.: Compulsory elective module in complex „Entwicklung und Aufbau von eBusiness-Systemen“<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Hardware-basierte Systeme: Elektrotechnik, Informationstechnik und Sensorik“<br>• Study programme Mathematical Data Science M.Sc.: Compulsory elective module in complex „Data Science Applications“ |
| **Module Components** | • Lecture: Network and System Security<br>• Accompanying exercises<br>• Related examination |
| **Components to be offered in the Current Semester** | **120580** Examination<br>Network and System Security (Wiederholung) |

# Module 12979 Internet Measurements and Forensics

assign to: Cyber Security Methods

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 12979 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Internet Measurements and Forensics**<br>Internet-Messungen und Forensik |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. Hohlfeld, Oliver |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every summer semester |
| **Credits** | 6 |
| **Learning Outcome** | This course will give a detailed introduction on how to empirically measure large communication systems on the example of the Internet as the largest communication network. The focus in on the explanation of methods for conducting such large-scale assessments to i) understand complex systems and ii) assesses their security properties. The course aims at familiarizing students with key aspects of Internet traffic, Internet protocol use and security, and methods to conduct large-scale studies for security. It will also discuss how to use measurement data for network forensics. |
| **Contents** | • Analyzing Internet naming: The domain name system and its security<br>• Internet traffic characteristics and measurement approaches (e.g., sampling, aggregation)<br>• Internet control plane analysis and robustness<br>• Internet-wide probing for liveness / security<br>• Strategies for sound measurements<br>• Internet application security measurement strategies<br>• Internet security infrastructures and network forensics<br><br>How does Internet traffic look like? Are there some characteristic properties? How and where is it possible to improve the Internet, and how can those improvements be tested? How can the previous questions be addressed, and what technical challenges does one face while monitoring? How can data privacy be ensured? Is there something to bear in mind when analyzing such measurements in a statistical manner? Is it possible to generate realistic traffic based on statistical characteristics? |

| | |
|---|---|
| **Recommended Prerequisites** | Knowledge about foundational aspects of computer networks (e.g., basic protocols such as IP, TCP, HTTP) as thought in introductory courses on computer networks is expected. |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 1 hours per week per semester<br>Self organised studies - 135 hours |
| **Teaching Materials and Literature** | • Kurose, J. F.; Ross, K. W.: Computer Networking: A Top Down Approach<br>• Crovella, M; Krishnamurthy, B; Internet Measurement: Infrastructure, Traffic and Applications |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful completion of exercise sheets<br><br>**Final module examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30-45 min. (with small number of participants)<br><br>In the first lecture it will be announced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Informatik M.Sc.: Compulsory elective module in complex „Angewandte und technische Informatik“ (level 400)<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Computer Science“ and in complex „Cyber Security Methods“<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Hardware-basierte Systeme: Elektrotechnik, Informationstechnik und Sensorik“<br>• Study programme Physics M.Sc.: Compulsory elective module in complex „Minor Subject“ |
| **Module Components** | • Lecture: Internet Measurements and Forensics<br>• Accompanying exercise<br>• Related examination |
| **Components to be offered in the Current Semester** | No assignment |

# Module 13490 Secure Cyber-Physical Systems

assign to: Cyber Security Methods

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 13490 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Secure Cyber-Physical Systems**<br>Sichere Cyber-Physische Systeme |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Panchenko, Andriy |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every summer semester |
| **Credits** | 6 |
| **Learning Outcome** | After successfully completing the module, students can assess and master the challenges in securing cyber-physical systems and industrial control networks. They have deepened their knowledge of the module “Introduction to Cybersecurity“. They understand the principles of system and network security with a special focus on cyber-physical systems. They know the security and privacy concepts as building blocks for the later specialization. |
| **Contents** | Cyber-physical systems (CPS) are closely connected to their environment via sensors and actuators. It is "the fusion of reality with the network". They comprise of a A/D and D/A converters to sense and interact, to influence the physical environment in a coordinated way. The spectrum of CPS ranges from medical devices (e.g., pace makers), smart vehicles up to countrywide industrial control networks (e.g., energy networks, smart grids). Functioning of our society depends on the cyber-physical systems.<br>This course is the continuation of the Introduction into Cyber Security and covers principles of system and network security with a special focus on cyber-physical systems. It introduces security and privacy concepts as building blocks for later specialization.<br>In the scope of this module, we explore, among others, the following topics:<br>• Introduction and General Security Concepts<br>• The World of Cyber-Physical Systems<br>• Industrial Protocols<br>• Definitions, Security Goals, Attacker Models<br>• Physical Security |

| | |
|---|---|
| | • Access Control<br>• Isolation Mechanisms<br>• Firewalls<br>• Anomaly and Intrusion Detection<br>• Honeypots<br>• Fingerprinting Techniques<br>• Security Protocols<br>• Malware |
| **Recommended Prerequisites** | Knowledge of the material of the modules<br>• 11889 *Einführung in die IT-Sicherheit*<br>• 12973 *Netzwerk- und Systemsicherheit* (can be taken in parallel) |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 120 hours |
| **Teaching Materials and Literature** | • Gollmann: Computer Security, Wiley & Sons<br>• William Stallings, Lawrie Brown: Computer Security: Principles and Practice, Pearson<br>• Du: Computer & Internet Security: A Hands-on Approach<br><br>Additional information will be provided at the begin of the module. |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful treatment of all assigned project tasks (usually about 3-5 tasks) including successful presentation of the results in the laboratory course (approx. 15 minutes per task)<br><br>**Final module examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30-45 min. (with small number of participants)<br><br>In the first lecture it will be anounced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Cyber Security Methods“<br>• Study programme Informatik M.Sc.: Compulsory elective module in complex „Angewandte und technische Informatik“ (level 400)<br>• Study programme eBusiness M. Sc.: Compulsory elective module in complex „Entwicklung und Aufbau von eBusiness-Systemen“<br>• Study programme Artificial Intelligence M.Sc.: Compulsory elective module in complex „Advanded Methods“<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Software-basierte Systeme“ |

| | |
|---|---|
| **Module Components** | • Lecture: Secure Cyber-Physical Systems<br>• Accompanying exercise<br>• Related examination |
| **Components to be offered in the Current Semester** | **120582** Examination<br>Secure Cyber-Physical Systems (Wiederholung) |

# Module 13800 Engineering of Trustworthy Systems

assign to: Cyber Security Methods

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 13800 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Engineering of Trustworthy Systems**<br>Entwicklung vertrauenswürdiger Systeme |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. Langendörfer, Peter |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every summer semester |
| **Credits** | 8 |
| **Learning Outcome** | After successfully completing the module, students are familiar with the central aspects of systems engineering, in particular the development, construction and operation of hybrid platforms. They are able to implement the guarantee of reliability, security and protection of complex modules. In addition to functional requirements, students are also able to consider economic and organizational aspects such as cost efficiency and the management of human resources. |
| **Contents** | This class both delivers theoretical foundations and methodological approaches and an oppotunity for students to work in teams of two to four to independently develop parts of a complex system.<br>Theoretical background<br>Systems engineering concepts and approaches that will be illustrated by examples:<br>• System Design and Project Management: Design of a development project, project management, processes and tools, risk management, supply management<br>• Development Process: Market trends of selected application area, Requirement engineering, SE models such as V-model, waterfall model etc.<br>• Security Engineering approaches such as BSI Grundschutz, NIST Special Publication 800-82, Attack Trees, Penetration tools, etc.<br>• Architecture development process, HW/SW architecture, networks, bus systems (e.g. CAN, Modbus), processor families, standard SW modules, boundary conditions for the design of architectures (size, costs, assembly, wiring) |

| | |
|---|---|
| | Hands-On-Experience<br>Small teams of students will get the chance to develop selected parts of a complex system. Their tasks will be:<br>• Leading a development team (role will change over time)<br>• Designing a sub-system adhering to predefined interfaces<br>• Implementing the system<br>• Testing the newly developed sub-system Integrating the newly developed subsystems into the complete system<br>• Testing the complete system including attacks such as buffer overflows, replay attacks, DoS Attacks etc. |
| **Recommended Prerequisites** | Firm knowledge of module<br>• 11889 Introduction to Cyber Security<br>• 11897 Security of Resource-constraint Systems |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 3 hours per week per semester<br>Exercise - 1 hours per week per semester<br>Study project - 30 hours<br>Self organised studies - 150 hours |
| **Teaching Materials and Literature** | Will be announced in the first lecture. |
| **Module Examination** | Continuous Assessment (MCA) |
| **Assessment Mode for Module Examination** | • Successful completion of homework, 5-7 series (50% of total marks)<br>• Successful development of selected parts of a complex system (50% of total marks)<br><br>75% of the total marks are needed to pass the module |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | 20 |
| **Remarks** | • Study programme Informatik M.Sc.: Compulsory elective module in complex „Angewandte und technische Informatik" (Niveaustufe 400)<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Cyber Security Methods“ |
| **Module Components** | • Lecture with integrated exercise: Engineering of Trustworthy Systems |
| **Components to be offered in the Current Semester** | No assignment |

# Module 14035 Application of Side-Channel Analysis Methods in the Earlier Design Phase of Cryptographic Implementations

assign to: Cyber Security Methods

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 14035 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Application of Side-Channel Analysis Methods in the Earlier Design Phase of Cryptographic Implementations**<br>Anwendung von Seitenkanalanalyse-Methoden in der frühen Entwurfsphase kryptographischer Designs |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Hon.Prof. Dr.-Ing. Dyka, Zoya |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every winter semester |
| **Credits** | 6 |
| **Learning Outcome** | Upon completion of the module, students will be familiar with various statistical, machine learning, and clustering methods for analyzing side-channel leakage sources. They are able to apply these methods and evaluate and comparatively discuss their effectiveness in extracting secret data.They will be able to use, understand, and describe selected methods for analyzing a given set of traces. They understand the applicability of the analysis methods as a means to determine the vulnerability of cryptographic designs in their early design phase, using the example of a hardware accelerator of elliptic curve point multiplication for an elliptic curve cryptosystem. |
| **Contents** | This course covers both theoretical and practical aspects of applying statistical and machine learning methods as a means of extracting secret data for side-channel attacks. Selected statistical as well as clustering methods will be presented and described. The suitability of the methods for determining side-channel leakage sources in attacked designs is discussed. Furthermore, selected countermeasures against physical attacks are presented and their effectiveness is discussed.<br><br>Main topics covered are:<br>• Evaluation of algorithmic countermeasures such as elliptic curve point blinding, scalar randomization, and scalar splitting on the resistance of cryptographic accelerators for elliptic curve cryptosystems against horizontal side-channel attacks |

| | |
|---|---|
| | • Importance of analytics in identifying side-channel leakage sources in the early design phase of cryptographic designs |
| **Recommended Prerequisites** | none |
| **Mandatory Prerequisites** | Passed exam of module:<br>• 11863 *Hands on Knowledge for Side Channel Attacks* |
| **Forms of Teaching and Proportion** | Seminar - 2 hours per week per semester<br>Study project - 60 hours<br>Research paper/essay - 30 hours<br>Self organised studies - 60 hours |
| **Teaching Materials and Literature** | • Kabin, Ievgen & Kreiser, Dan & Dyka, Zoya & Langendoerfer, Peter. (2018). FPGA Implementation of ECC: Low-Cost Countermeasure against Horizontal Bus and Address-Bit SCA. 1-7. 10.1109/RECONFIG.2018.8641732<br>• Kabin, I., Dyka, Z., Klann, D. et al. Resistance of the Montgomery Ladder Against Simple SCA: Theory and Practice. J Electron Test 37, 289–303 (2021). https://doi.org/10.1007/s10836-021-05951-3 |
| **Module Examination** | Continuous Assessment (MCA) |
| **Assessment Mode for Module Examination** | • presentation: 5-10 minutes (10%);<br>• written report: 5-10 pages (50%),<br>• implementation: proven correct functionality (40%) |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | 10 |
| **Remarks** | • Study programme Cyber Security M.Sc.: Compulsory elective module in complex "Cyber Security Methods"<br>• Study programme Informatik M.Sc.: Compulsory elective module in complex „Praktische Informatik" (level 400) |
| **Module Components** | • Seminar Application of Side-Channel Analysis Methods in the Earlier Design Phase of Cryptographic Implementations |
| **Components to be offered in the Current Semester** | **122260** Seminar<br>Application of side-channel analysis methods in the earlier design phase of cryptographic implementations - 2 Hours per Term |

# Module 11847 Neural Networks and Learning Theory

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11847 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Neural Networks and Learning Theory**<br>Neuronale Netze und Lerntheorie |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. habil Meer, Klaus |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Each summer semester even year |
| **Credits** | 8 |
| **Learning Outcome** | Students will get insight into different network architectures and their principles of operation. Notions like artificial intelligence and automatic learning will be made precise during the course. A central issue is the understanding of mathematical ideas underlying different network learning algorithms. This includes both positive solutions of problems and knowledge about limits of the approaches studied. |
| **Contents** | Some central network architectures are treated. These architectures differ in the way they manipulate input data, the way they perform learning tasks and the analysis of corresponding algorithms by mathematical means. More precisely, the following types of networks are covered:<br>• General aspects of architecures, in particular feedforward nets, recurrent nets<br>• Perceptron network, perceptron learning algorithm<br>• Backpropagation algorithm<br>• Radial basis function networks<br>• Support Vector Machines<br>• Learning theory and Vapnik-Chervonenkis dimension<br>• Self-organizing networks<br>• Hopfield networks<br><br>Special emphasis will be given to the mathematical analysis of algorithms. This will make it necessary to study some basic facts of optimization and probability theory. |

| | |
|---|---|
| **Recommended Prerequisites** | Basic knowledge both concerning optimality criteria in differentiable optimization and probability theory are advisable, but will be treated briefly in the course.<br>Solid knowledge of the content of module<br>• 11213: Mathematik IT -3 (Analysis) |
| **Mandatory Prerequisites** | No successful participation in associated phase-out module 12450 *Neuronale Netze und Lerntheorie*. |
| **Forms of Teaching and Proportion** | Lecture - 4 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 150 hours |
| **Teaching Materials and Literature** | • E. Alpaydin: Maschinelles Lernen, Oldenbourg Verlag München, 2008<br>• M. Anthony, N.Biggs: Computational Learning Theory, Cambridge University Press 1997<br>• N. Christiani, J. Shawe-Taylor: An Introduction to Support Vector Machines and kernel-based Learning Methods, Cambridge Univ. Press, 2003<br>• A.C.C Coolen, R. Kühn, P. Sollich: Theory of Neural Information Processing Systems, Oxford University Press 2005<br>• P. Fischer: Algorithmisches Lernen, Teubner 1999<br>• P. Flach: Machine Learning: The Art and Science of Algorithms that Make Sense of Data, Cambridge University Press 2012<br>• F. M. Ham, I. Kostanic: Principles of Neurocomputing for Science & Engineering, McGraw Hill 2001<br>• S. Haykin: Neural Networks, Prentice Hall, 1999<br>• R. Rojas: Theorie der neuronalen Netze, Springer 1996<br>• S. Shalev-Shwartz, S. Ben-David: Understanding Machine Learning, Cambridge University Press 2014. |
| **Module Examination** | Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | • Written examination, 90 min. **OR**<br>• Oral examination, 30-45 min. (with small number of participants)<br><br>In the first lecture it will be announced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | 100 |
| **Remarks** | • Study programme Informatik M.Sc.: Compulsory elective module in complex „Grundlagen der Informatik" (level 400)<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Computer Science"<br>• Study programme Artificial Intelligence M.Sc.: Compulsory elective module in complex „Learning and Reasoning“<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Kognitions- und Neurowissenschaft“ |

| | |
|---|---|
| | • Study programme Angewandte Mathematik M.Sc.: Compulsory elective module in complex „Analysis / Algebra / Kombinatorik“<br>• Study programme Mathematik B.Sc.: Compulsory elective module in complex „Vertiefung“, in limited extend<br>• Study programme Wirtschaftsmathematik B.Sc.: Compulsory elective module in complex „Vertiefung“, in limited extend<br>• Study programme Physics M.Sc.: Compulsory elective module in complex „Minor Subject“<br>• Study programme Mathematical Data Science M.Sc.: Compulsory elective module in complex „Advanced Mathematical Methods in Data Science“ |
| **Module Components** | • Lecture: Neural Networks and Learning Theory<br>• Accompanying exercise<br>• Related examination |
| **Components to be offered in the Current Semester** | **120162** Examination<br>Neural Networks and Learning Theory (Wiederholung) |

# Module 11860 Distributed and Parallel Systems II (Concurrency, Replication and Consistency)

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11860 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Distributed and Parallel Systems II (Concurrency, Replication and Consistency)**<br>Verteilte und Parallele Systeme II (Nebenläufigkeit, Replikation, Konsistenz) |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Nolte, Jörg |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Each summer semester even year |
| **Credits** | 6 |
| **Learning Outcome** | The students get to know coordination techniques for parallel activities in distributed systems, they understand and are able to implement/use them. Also, different models of consistency and ways to evaluate them are taught. Teamwork is further improved. |
| **Contents** | Distributed and Parallel Systems 2 is centered on aspects of synchronization and concistency in distributed systems. Models and pradigms for parallel processing (task -vs. data perallelism, collective operations, tuple spaces and data flow models, lazy and greedy synchronization) are key to the lecture. Furthermore, active and passive methods of replication and their corresponding models of consistency (weak vs. strong) are also taught.<br>The lecture is accompanied by a hand-on assignment on the PC-cluster. |
| **Recommended Prerequisites** | Knowledge of the content of the modules<br>• 12204: Operating Systems I<br>• 12341: Distributed and Parallel Systems I (Basic Principles) |
| **Mandatory Prerequisites** | No successful participation in module *12432 - Verteilte und Parallele Systeme II (Nebenläufigkeit, Replikation, Konsistenz)*. |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 120 hours |

| | |
|---|---|
| **Teaching Materials and Literature** | none |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Implementation of a prototype<br><br>**Final module examination:**<br>• Oral examination, 30-45 min. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Computer Science M.Sc.: Compulsory elective module in complex „Applied and Technical Computer Science“ (level 400)<br>• Study programme Information and Media Technology M.Sc.: Compulsory elective module in „Dependable HW/SW-Systems“<br>• Study programme eBusiness M.Sc.: Compulsory elective module in main focus „Development and Deployment of eBusiness Systems“<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Computer Science“<br>• Study programme Artificial Intelligence Engineering M.Sc.: Compulsory elective module in complex „Software-based Systems“<br><br>If there is no need that the module is taught in English, alternatively the german version 12432 "Verteilte und Parallele Systeme II (Nebenläufigkeit, Replikation, Konsistenz)" may be offered instead.<br><br>Modules 11860 "Distributed and Parallel Systems II (Concurrency, Replication and Consistency)" and 12432 "Verteilte und Parallele Systeme II (Nebenläufigkeit, Replikation, Konsistenz)" can not be combined. |
| **Module Components** | Lecture: Distributed and Parallel Systems II (Concurrency, Replication and Consistency)<br>Accompanying exercises |
| **Components to be offered in the Current Semester** | No assignment |

# Module 11861 Operating Systems II (Multi-Level Memory Management)

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11861 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Operating Systems II (Multi-Level Memory Management)**<br>Betriebssysteme II (Speicherverwaltung: Mechanismen und Strategien) |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Nolte, Jörg |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Each winter semester odd year |
| **Credits** | 6 |
| **Learning Outcome** | Students get to know and understand complex memory management and input/output strategies. They are able to implement those strategies and integrate them into bigger systems. Teamwork abilities are improved. |
| **Contents** | Operating Systems II is based on Operating Systems I. The lecture is focused on processes, protection mechanisms used in operating systems, concepts for address spaces, memory management units, methods and techniques for memory management on operating system and runtime environment level, integration and interaction between memory management, I/O systems and networks. In the on-hands assignments the students incrementally implement a virtual memory management system in user mode. |
| **Recommended Prerequisites** | Knowledge of the content of the module<br>• 12204: Operating Systems I |
| **Mandatory Prerequisites** | No successful participation in module *12339 - Betriebssysteme II (Speicherverwaltung: Mechanismen und Strategien)*. |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 120 hours |
| **Teaching Materials and Literature** | • Lecture Slides.<br>• Information about current literature is provided on the lecture home page. |

| | |
|---|---|
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite**:<br>• Implementation of a prototype<br><br>**Final module examination:**<br>• Oral examination, 30-45 min. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Informatik B.Sc.: Compulsory elective module in complex „Angewandte und technische Informatik“ (level 300).<br>• Study programme Informations- und Medientechnik B.Sc.: Compulsory elective module for main focus 1: „Praktische Informatik“<br>• Study programme Künstliche Intelligenz Technologie B.Sc.: Compulsory elective module in complex „Software-basierte Systeme“<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Software-basierte Systeme“<br>• Study programme eBusiness M.Sc.: Main focus „Entwicklung und Aufbau von eBusiness-Systemen“<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in main focus „Computer Science“<br><br>If there is no need that the module is taught in English, alternatively the german version 12339 „Betriebssysteme II (Speicherverwaltung: Mechanismen und Strategien)“ may be chosen instead.<br><br>Modules 11861 „Operating Systems II (Multi-Level Memory Management)“ and 12339 „Betriebssysteme II (Speicherverwaltung: Mechanismen und Strategien)“ can not be combined. |
| **Module Components** | • Lecture Operating Systems II (Multi-Level Memory Management)<br>• Accompanying exercises<br>• Related Examination |
| **Components to be offered in the Current Semester** | **121010** Lecture<br>Operating Systems II (Multi-Level Memory Management) - 2 Hours per Term<br>**121011** Exercise<br>Operating Systems II (Multi-Level Memory Management) - 2 Hours per Term<br>**121013** Examination<br>Operating Systems II (Multi-Level Memory Management) |

# Module 11864 Wireless Sensor Networks: Concepts, Protocols and Applications

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11864 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Wireless Sensor Networks: Concepts, Protocols and Applications**<br>Drahtlose Sensornetze: Konzepte, Protokolle und Anwendungen |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Piotrowski, Krzysztof |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every winter semester |
| **Credits** | 6 |
| **Learning Outcome** | Participants know the architecture of wireless sensor networks. They can select and classify protocols for different applications. Participants can design and understand complex protocols. They understand the connection between physical impacts on communication and necessary technical means to keep the network alive. They can design own networks and argue about the design decisions. They can judge about future developments. |
| **Contents** | Architecture of sensor networks, node-architectures, MAC protocols, addressing, routing, synchronisation, operating systems, topology management, applications, security and key-exchange protocols. |
| **Recommended Prerequisites** | Basic knowledge of technical computer science concepts and communication systems. |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 120 hours |
| **Teaching Materials and Literature** | Are available on Moodle, starting from the first week of lectures. |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful completion of exercise assignments |

| | |
|---|---|
| | **Final module examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30 min. (with small number of participants)<br><br>In the first lecture it will be anounced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Informatik B.Sc.: Compulsory elective module in complex "Angewandte und Technische Informatik" (level 300)<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex "Computer Science"<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Software-basierte Systeme“<br>• Study programme Physics M.Sc.: Compulsory elective module in complex „Minor Subject“<br>• Study programme Micro- and Nanoelectronics M.Sc.: Compulsory elective module in complex „Applications“ |
| **Module Components** | • Lecture/Exercise: Wireless Sensornetworks: Concepts, Protocolls and Applications<br>• Related examination |
| **Components to be offered in the Current Semester** | **122130** Lecture/Exercise<br>Wireless Sensor Networks: Concepts, Protocolls and Applications - 4 Hours per Term<br>**122131** Examination<br>Wireless Sensor Networks: Concepts, Protocolls and Applications |

# Module 11881 Foundations of Data Mining

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11881 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Foundations of Data Mining**<br>Grundlagen des Data Mining |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. habil. Schmitt, Ingo |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every winter semester |
| **Credits** | 6 |
| **Learning Outcome** | Acquaintance with the statistical and learning-theoretical foundations of knowledge extraction from large data sets; knowledge of specific notions and of mathematical background in order to understand current publications and software concerning the field; ability of transfer to concrete problems; knowledge of algorithms and their usage. |
| **Contents** | • Foundation of statistics<br>• Clustering (partition-based, density-based, hierarchical, ...)<br>• Classification (decision trees, support vector machines, deep learning on convolution neural networks, ...)<br>• Association rules (frequent itemsets)<br>• further data mining approaches<br><br>Acquired knowledge will be applied within a project. |
| **Recommended Prerequisites** | The module cannot be successfully completed without knowledge of the content of<br>• 11112 *Mathematik IT-1 (Diskrete Mathematik)*<br>• 11113 *Mathematik IT-2 (Lineare Algebra)* |
| **Mandatory Prerequisites** | • No successful participation in module 12351 *Grundlagen des Data Mining*. |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 1 hours per week per semester<br>Practical training - 1 hours per week per semester<br>Self organised studies - 120 hours |

| | |
|---|---|
| **Teaching Materials and Literature** | • James, Gareth; Witten, Daniela; Hastie, Trevor; Tibshirani, Robert: An Introduction to Statistical Learning with Applications in R. Springer, New York 2013.<br>• Aloaydin, Ethem: Machine Learning. The MIT Press, Massachusetts Institute of Technology, 2004.<br>• Mitchell, Tom M.: Machine Learning. McGraw-Hill, 1997. |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful completion of practical training tasks and exercises tasks<br><br>**Final module examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30-45 min. (with small number of participants)<br><br>In the first lecture it will be annunced, if the examination will offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | 80 |
| **Remarks** | • Study programme Informatik B.Sc.: Compulsory elective module in complex „Grundlagen der Informatik“ (level 300)<br>• Study programme eBusiness M.Sc.: Compulsory elective module in main focus „Entwicklung und Aufbau von eBusiness-Systemen"<br>• Study programme Artificial Intelligence M.Sc.: Compulsory elective module in complex „Knowledge Acquisition, Representation, and Processing“<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Computer Science“<br>• Study programme Mathematik B.Sc.: Compulsory elective module in complex „Anwendungen“, field „Informatik“<br>• Study programme Wirtschaftsmathematik B.Sc.: Compulsory elective module in complex „Anwendungen“, field „Informatik“<br>• Study programme Mathematical Data Science M.Sc.: Compulsory elective module in complex „Fundamentals of Data Science“<br><br>If there is no need that the module is taught in English, alternatively the german version 12351 „Grundlagen des Data Mining“ may be offered instead.<br>Module 11881 „Foundations of Data Mining“ and 12351 „Grundlagen des Data Mining“ can not be combined. |
| **Module Components** | • Lecture Foundations of Data Mining<br>• Accompanying exercise with laboratory<br>• Related examination |
| **Components to be offered in the Current Semester** | **120230** Lecture<br>Grundlagen des Data Mining / Foundations of Data Mining - 2 Hours per Term<br>**120231** Exercise |

Grundlagen des Data Mining / Foundations of Data Mining - 2 Hours per Term
**120234** Examination
Grundlagen des Data Mining / Foundations of Data Mining

# Module 11886 Dependability and Fault Tolerance

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 11886 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Dependability and Fault Tolerance**<br>Zuverlässigkeit und Fehlertoleranz |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Dr.-Ing. habil. Herglotz, Christian Josef |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every winter semester |
| **Credits** | 6 |
| **Learning Outcome** | Students learn to regard and to analyze digital circuits and systems with respect to their reliability and dependability. They also learn how to implement mechanism for a fault tolerant behaviour into digital circuits and systems. |
| **Contents** | Introduction: Problems of system reliability and dependability.<br>Chapter 1: Faults and fault mechanisms in digital circuits and systems.<br>Chapter 2: Technologies for IC production testing.<br>Chapter 3: Methods for built-in self test (off-line).<br>Chapter 4: Methods and Architectures for on-line fault detection and compensation.<br>Chapter 5: Basic architectures for reconfigurable and self-repairing circuits and systems<br>Chapter 6: Challenges in AI Hardware Systems |
| **Recommended Prerequisites** | Basic knowledge in digital design, electrical engineering and integrated electronics. |
| **Mandatory Prerequisites** | No successful participation in module<br>• 12476 *Zuverlässigkeit und Fehlertoleranz*. |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Laboratory training - 2 hours per week per semester<br>Self organised studies - 120 hours |

| | |
|---|---|
| **Teaching Materials and Literature** | Script and presentations available for downloading. List of references is presented at the beginning of the course. Problems for exercises and instructions for lab experiments can be downloaded. |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful completion of exercises and presentation of results in course<br><br>**Final module examination:**<br>• Oral examination, 30-45 min. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Informatik M.Sc.: Compulsory elective module in complex "Angewandte und Technische Informatik" (level 400)<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex "Computer Science"<br>• Study programme Artificial Intelligence M.Sc.: Compulsory elective module in complex „Advanded Methods“<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Hardware-basierte Systeme: Elektrotechnik, Informationstechnik und Sensorik“ |
| **Module Components** | • Lecture: Dependability and Fault Tolerance<br>• Accompanying laboratory<br>• Related examination |
| **Components to be offered in the Current Semester** | **120440** Lecture<br>Dependability and Fault Tolerance - 2 Hours per Term<br>**120441** Practical training<br>Dependability and Fault Tolerance - 2 Hours per Term<br>**120443** Examination<br>Dependability and Fault Tolerance |

# Module 12882 Embedded Real-Time Systems

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 12882 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Embedded Real-Time Systems**<br>Eingebettete Echtzeitsysteme |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Dr.-Ing. Karnapke, Reinhardt |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | On special announcement |
| **Credits** | 6 |
| **Learning Outcome** | Students know and understand complex relationships in real-time (operating-) systems. They are able apply and develop them. They recognize the practical relevance of the acquired knowledge.<br>They deepen their ability to collaborate with other developers. |
| **Contents** | The module „Embedded Real-Time Systems“ is based on the module „Operating Systems I“. The module focuses on the special challenges of both embedded systems and real-time systems.<br>In the practical exercises students will program different embedded systems and control them simultaneously in real time. |
| **Recommended Prerequisites** | • Solid programming skills in C / C++<br>• Knowledge of the functionality of operating systems, such as knowledge of the content of module 12204 "Operating Systems I" |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 120 hours |
| **Teaching Materials and Literature** | • Slides of the lecture<br>• Current references will be presented on the web page of the module. |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Incremental implementation of a prototype |

| | |
|---|---|
| | **Final module examination:**<br>• Oral examination, 30-45 min. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Informatik B.Sc.: Compulsory elective module in complex „Angewandte und technische Informatik“ (level 300)<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Informatik“<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Software-basierte Systeme“ |
| **Module Components** | • Lecture: Eingebettete Echtzeitsysteme<br>• Accompanying exercise<br>• Related examination |
| **Components to be offered in the Current Semester** | **121040** Lecture<br>Embedded Real-Time Systems - 2 Hours per Term<br>**121041** Exercise<br>Embedded Real-Time Systems - 2 Hours per Term<br>**121042** Examination<br>Embedded Real-Time Systems |

# Module 12975 Internet - Functionality, Protocols, Applications

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 12975 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Internet - Functionality, Protocols, Applications**<br>Internet - Funktionsweise, Protokolle, Anwendungen |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. Hohlfeld, Oliver |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every summer semester |
| **Credits** | 6 |
| **Learning Outcome** | Students understand the functioning of the Internet, in particular the most important Internet protocols and principles of application design, including the underlying basics and techniques (e.g. the internet protocol stack), as well as the basics of multimedia communication. They are familiar with modern developments in the Internet and advanced topics from practice and research (e.g. quality of qervice, peer-to-peer, cloud computing, internet of things). They are enabeled to specialize in these topics. |
| **Contents** | • History, structure, and organization of the Internet<br>• Internet economics<br>• Internet protocol stack (IPv4, CIDR, IPv6, DHCP, BGP, TCP, UDP, DNS, HTTP)<br>• Quality of Service (types, mechanisms, Intserv, Diffserv)<br>• Fundamentals of multimedia communication<br>• Data center networking<br>• Content distribution networks |
| **Recommended Prerequisites** | Knowledge of the content of module:<br>• 11454 *Grundlagen der Rechnernetze* |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 3 hours per week per semester<br>Exercise - 1 hours per week per semester<br>Self organised studies - 120 hours |

| | |
|---|---|
| **Teaching Materials and Literature** | • Tanenbaum, A. S., Wetherall, D. J: Computer Networks (5th Edition), Prentice Hall, Pearson Studium, 2011<br>• Stallings, W.: Data and Computer Communications (8th ed.), Prentice Hall, 2008.<br>• Kurose, J. F.; Ross, K. W.: Computernetzwerke (5. Aufl.), Pearson Studium, 2012.<br>• Steinmetz, R.; Nahrstedt, C.: Multimedia Systems. Springer, 2010 |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful completion of exercise sheets<br><br>**Final module examination:**<br>• Written examination,90 min. **OR**<br>• Oral examination, 30-45 min. (with small number of participants)<br><br>In the first lecture it will be announced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Informatik M.Sc.: Compulsory elective module in complex „AAngewandte und technische Informatik“ (level 400)<br>• Study programme eBusiness M.Sc.: Compulsory elective module in complex „Entwicklung und Aufbau von eBusiness-Systemen“<br>• Study programme Physics M.Sc.: Compulsory elective module in subsidiary subject „Computer Science“<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Computer Science“<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Software-basierte Systeme“ |
| **Module Components** | • Lecture: Internet - Functionality, Protocols, Applications<br>• Accompanying exercise<br>• Related examination |
| **Components to be offered in the Current Semester** | No assignment |

# Module 12976 Processor Architecture

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 12976 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Processor Architecture**<br>Prozessor-Architektur |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Dr.-Ing. habil. Herglotz, Christian Josef |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every winter semester |
| **Credits** | 8 |
| **Learning Outcome** | Students learn about architectures and functional concepts of processors. They can select processors for specific tasks and optimise their operation. They also know to design processor components and they become familiar with processor synthesis systems. |
| **Contents** | Students understand architectures and functional concepts of processors. They can select processors for specific tasks and optimise their operation. They also know to design processor components and are familiar with processor synthesis systems. |
| **Recommended Prerequisites** | Basic knowledge in digital design and computer architecture. |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 4 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 150 hours |
| **Teaching Materials and Literature** | Script and presentations available for downloading. List of references is presented at the beginning of the course. Problems for exercises and instructions for lab experiments can be downloaded. |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful completion of exercises and presentation of results in course |

| | |
|---|---|
| | **Final module examination:**<br>• Oral examination, 30-45 min. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Informatik M.Sc.: Compulsory elective module in complex „Angewandte und Technische Informatik“ (level 400)<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Computer Science"<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex “Hardware-basierte Systeme: Elektrotechnik, Informationstechnik und Sensorik“ |
| **Module Components** | • Lecture: Processor-Architecture<br>• Accompanying exercise<br>• Related examination |
| **Components to be offered in the Current Semester** | **120430** Lecture<br>Processor Architecture - 4 Hours per Term<br>**120431** Exercise<br>Processor Architecture - 2 Hours per Term<br>**120433** Examination<br>Processor Architecture |

# Module 12979 Internet Measurements and Forensics

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 12979 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Internet Measurements and Forensics**<br>Internet-Messungen und Forensik |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. Hohlfeld, Oliver |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every summer semester |
| **Credits** | 6 |
| **Learning Outcome** | This course will give a detailed introduction on how to empirically measure large communication systems on the example of the Internet as the largest communication network. The focus in on the explanation of methods for conducting such large-scale assessments to i) understand complex systems and ii) assesses their security properties. The course aims at familiarizing students with key aspects of Internet traffic, Internet protocol use and security, and methods to conduct large-scale studies for security. It will also discuss how to use measurement data for network forensics. |
| **Contents** | • Analyzing Internet naming: The domain name system and its security<br>• Internet traffic characteristics and measurement approaches (e.g., sampling, aggregation)<br>• Internet control plane analysis and robustness<br>• Internet-wide probing for liveness / security<br>• Strategies for sound measurements<br>• Internet application security measurement strategies<br>• Internet security infrastructures and network forensics<br><br>How does Internet traffic look like? Are there some characteristic properties? How and where is it possible to improve the Internet, and how can those improvements be tested? How can the previous questions be addressed, and what technical challenges does one face while monitoring? How can data privacy be ensured? Is there something to bear in mind when analyzing such measurements in a statistical manner? Is it possible to generate realistic traffic based on statistical characteristics? |

| | |
|---|---|
| **Recommended Prerequisites** | Knowledge about foundational aspects of computer networks (e.g., basic protocols such as IP, TCP, HTTP) as thought in introductory courses on computer networks is expected. |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 1 hours per week per semester<br>Self organised studies - 135 hours |
| **Teaching Materials and Literature** | • Kurose, J. F.; Ross, K. W.: Computer Networking: A Top Down Approach<br>• Crovella, M; Krishnamurthy, B; Internet Measurement: Infrastructure, Traffic and Applications |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful completion of exercise sheets<br><br>**Final module examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30-45 min. (with small number of participants)<br><br>In the first lecture it will be announced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Informatik M.Sc.: Compulsory elective module in complex „Angewandte und technische Informatik“ (level 400)<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Computer Science“ and in complex „Cyber Security Methods“<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Hardware-basierte Systeme: Elektrotechnik, Informationstechnik und Sensorik“<br>• Study programme Physics M.Sc.: Compulsory elective module in complex „Minor Subject“ |
| **Module Components** | • Lecture: Internet Measurements and Forensics<br>• Accompanying exercise<br>• Related examination |
| **Components to be offered in the Current Semester** | No assignment |

# Module 13513 Communication Networks / Security Research Class

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 13513 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Communication Networks / Security Research Class**<br>Forschungsmodul zu Kommunikationsnetzen / -Sicherheit |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. Hohlfeld, Oliver |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | On special announcement |
| **Credits** | 6 |
| **Learning Outcome** | After successfully completing the module, students posess the following knowlege and skills:<br>• Detailed knowledge of current research topics in the field of Communication Networks / Network Security<br>• In-depth knowledge and understanding of a selected current topic<br>• Knowledge of scientific methods for the development of own results<br>• Ability to work independently on a research topic |
| **Contents** | This module targets students who are interested in acquiring an in-depth understanding of current research topics in communication networks / network security / network data science. Each course / semester will focus on a selected research area announced in the beginning of the course. The module begins with a set of lectures to provide the foundations on the selected research area. Students will then work on exploring their individually assigned research topics, both in theory and in practice. Results of this research work are presented and discussed within the class.<br>Discussed research areas can fall within:<br>- Network security<br>- Network architecture<br>- Network measurements / performance evaluation / simulation<br>- Networked systems (e.g., social networks)<br>- Quality of experience of networked systems |
| **Recommended Prerequisites** | Knowledge about foundational aspects of computer networks (e.g., basic protocols such as Ethernet, IP, TCP, HTTP, routing) as thought in introductory courses on computer networks is expecte, e.g.: |

| | |
|---|---|
| | • 11454 Grundlagen der Rechnernetze |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Seminar - 2 hours per week per semester<br>Practical training - 2 hours per week per semester<br>Study project - 60 hours<br>Self organised studies - 30 hours |
| **Teaching Materials and Literature** | • Depending on the topic the relevant information will be provided at the beginning of the module. |
| **Module Examination** | Continuous Assessment (MCA) |
| **Assessment Mode for Module Examination** | The assessment consists of equal parts:<br>• one scientific presentation (45 minutes) of the assigned research topic followed by a discussion (project assignment)<br>• one oral (15 minutes) or written examination (60 minutes) on the content of the lecture part<br>• one theoretical or practical paper on the individual research topic (project assignment)<br><br>In the first lecture it will be announced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Informatik M.Sc.: Compulsory elective module in complex „Angewandte und technische Informatik“ (level 400)<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Computer Science“ |
| **Module Components** | • Lecture „Communication Networks / Security Research Class“<br>• Subsequent seminar<br>• Subsequent laboratory<br><br>The module starts with a lecture part. Afterwards the different topics are presented in a seminar part. In the laboratory part, a problem is then implemented in detail. |
| **Components to be offered in the Current Semester** | No assignment |

# Module 13690 Hands on Wireless Sensor Network Applications

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 13690 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Hands on Wireless Sensor Network Applications**<br>Praktische Anwendungen von drahtlosen Sensornetzwerken |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr.-Ing. Piotrowski, Krzysztof |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every summer semester |
| **Credits** | 6 |
| **Learning Outcome** | After successfully completing the module, students are acquainted with the practical approach for implementing a wireless sensor network application. They know the technical foundations as well as the security and data protection aspects.<br>They are able to recognise the different aspects of the application and determine the partly conflicting requirements from this. They can make the necessary decisions to determine the final application and its features. In the case of several solutions, possibly with several parameters, they are able to find an optimal solution. |
| **Contents** | • Architecture of wireless sensor node<br>• Mechanisms to save energy<br>• Communication protocols and data processing<br>• Security and privacy aspects<br><br>These topics are prototypically implemented in the exercises using example problems. |
| **Recommended Prerequisites** | • Sound knowledge of the programming language C<br>• Basic knowledge of technical computer science |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Exercise - 2 hours per week per semester<br>Self organised studies - 120 hours |

| | |
|---|---|
| **Teaching Materials and Literature** | • Holger Karl, Andreas Willig, Protocols and Architectures for Wireless Sensor Networks, John Wiley & Sons, 2007<br>• Jochen H. Schiller, Mobile Communications, Second Edition, Addison-Wesley, 2003<br><br>More might be announced during the first class meeting. |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful completion of exercise assignments<br><br>**Final module examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30 min. (with small number of participants)<br><br>In the first lecture it will be anounced, if the examination will be offered in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Computer Science“<br>• Study programme Informatik M.Sc.: Compulsory elective module in complex „Angewandte und Technische Informatik“ (level 400) |
| **Module Components** | • Lecture/Exercise: Hands on Wireless Sensor Network Applications<br>• Related examination |
| **Components to be offered in the Current Semester** | **122140** Examination<br>Hands on Wireless Sensor Network Applications<br>(Wiederholungsprüfung) |

# Module 13911 Algebra: Structures and Algorithms

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 13911 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Algebra: Structures and Algorithms**<br>Algebra: Strukturen und Algorithmen |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. Averkov, Gennadiy |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | On special announcement |
| **Credits** | 6 |
| **Learning Outcome** | After successfully completing the module, students are able to work with basic algebraic concepts and know basic algebraic facts and constructions. They are able to use this knowledge to solve algebraic problems, with our without the assistance of computer-algebra systems. Students understand the basic algebraic algorithmic machinery of computational algebra. |
| **Contents** | • Commutative rings and ideals<br>• Affine varieties<br>• Groebner basis and the Hilbert basis theorem<br>• Elimination of variables with Groebner bases and resultsants<br>• Hilbert's Nullstellensatz<br>• Selected applications (e.g. global optimization, solution of kinematic problems, automated theory proving) |
| **Recommended Prerequisites** | Knowledge of the content of the modules<br>• 11101: *Lineare Algebra und analytische Geometrie I*<br><br>or<br>• 11112: *Mathematik IT-1 (Diskrete Mathematik)*, and<br>• 11113: *Mathematik IT-2 (Lineare Algebra)* |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 3 hours per week per semester<br>Exercise - 1 hours per week per semester<br>Self organised studies - 120 hours |

| | |
|---|---|
| **Teaching Materials and Literature** | • D. Cox, J. Little, and D. O'Shea: Ideals, Varieties, and Algorithms–An Introduction to Computational Algebraic Geometry and Commutative Algebra, Springer Publishing Company, 2010<br>• D. Cox, J. Little, and D. O'Shea: Using Algebraic Geometry, Springer Publishing Company, 2005<br>• S. Lang: Algebra, Springer Publishing Company, 2002 |
| **Module Examination** | Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Final module examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30 - 45 min. (with small number of participants)<br><br>In the first lecture it will introduced, if the examination will organized in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Angewandte Mathematik M.Sc.: Compulsory elective module in complex „Analysis / Algebra / Kombinatorik“<br>• Studiengang Mathematics M.Sc.: Wahlpflichtmodul im Komplex „Analysis / Algebra / Combinatorics“<br>• Studiengang Mathematical Data Science M.Sc.: Wahlpflichtmodul im Komplex „Advanced Mathematical Methods in Data Science“<br>• Study programme Mathematik B.Sc.: Compulsory elective module in complex „Vertiefung“, in limited extend<br>• Study programme Wirtschaftsmathematik B.Sc.: Compulsory elective module in complex „Vertiefung“, in limited extend<br>• Study programme Artificial Intelligence M.Sc.: Compulsory elective module in complex „Advanded Methods“<br>• Study programme Informatik B.Sc.: Compulsory elective module in „Praktische Mathematik" or in field of application „Mathematics"<br>• Study programme Informatik M.Sc.: Compulsory elective module in „Mathematik" or in field of application „Mathematik"<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Computer Science“ |
| **Module Components** | • Lecture *Algebra: Structures and Algorithms*, with integrated exercise<br>• Related examination |
| **Components to be offered in the Current Semester** | **130220** Lecture/Exercise<br>Algebra: Structures and Algorithms - 4 Hours per Term<br>**130222** Examination<br>Algebra: Structures and Algorithms |

# Module 13912 Coding Theory

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 13912 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Coding Theory**<br>Datenkodierung |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. nat. Averkov, Gennadiy |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | On special announcement |
| **Credits** | 6 |
| **Learning Outcome** | After successfully completing the module, students will know and understand the problems and basics of data coding. They can transfer known facts and procedures of linear algebra to this application field and have learned further concepts of algebra. They know linear codes and understand the meaning of the parameters. They know simple decoding algorithms, can apply them and show their correctness. |
| **Contents** | • Basics of coding theory<br>• Theory of linear codes<br>• Examples of linear codes, in particular, Reed-Solomon codes<br>• General and specific decoding algorithms<br>• Simple Goppa codes |
| **Recommended Prerequisites** | Knowledge of the content of the modules<br>• 11101: *Lineare Algebra und analytische Geometrie I*<br><br>or<br>• 11112: *Mathematik IT-1 (Diskrete Mathematik)*, and<br>• 11113: *Mathematik IT-2 (Lineare Algebra)* |
| **Mandatory Prerequisites** | none |
| **Forms of Teaching and Proportion** | Lecture - 3 hours per week per semester<br>Exercise - 1 hours per week per semester<br>Self organised studies - 120 hours |
| **Teaching Materials and Literature** | • van Lint, J., van der Geer, G., Introduction to Coding Theory and Algebraic Geometry |

| | |
|---|---|
| | • J.I. Hall, Notes on Coding Theory<br>• Willems, Wolfgang, Codierungstheorie und Kryptographie |
| **Module Examination** | Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Final module examination:**<br>• Written examination, 90 min. **OR**<br>• Oral examination, 30 - 45 min. (with small number of participants)<br><br>In the first lecture it will introduced, if the examination will organized in written or oral form. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Angewandte Mathematik M.Sc.: Compulsory elective module in complex „Analysis / Algebra / Kombinatorik“<br>• Study programme Mathematik B.Sc.: Compulsory elective module in complex „Vertiefung“, in limited extend<br>• Study programme Wirtschaftsmathematik B.Sc.: Compulsory elective module in complex „Vertiefung“, in limited extend<br>• Study programme Artificial Intelligence M.Sc.: Compulsory elective module in complex „Knowledge Acquisition, Representation, and Processing“<br>• Study programme Informatik B.Sc.: Compulsory elective module in „Praktische Mathematik" or in field of application „Mathematics"<br>• Study programme Informatik M.Sc.: Compulsory elective module in „Mathematik" or in field of application „Mathematik"<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Computer Science“<br>• Study programme Mathematics M.Sc.: Compulsory elective module in complex „Analysis / Algebra / Combinatorics“<br>• Study programme Mathematical Data Science M.Sc.: Compulsory elective module in complex „Advanced Mathematical Methods in Data Science“ |
| **Module Components** | • Lecture *Coding Theory*, with integrated exercise<br>• Related examination |
| **Components to be offered in the Current Semester** | **130251** Examination<br>Coding Theory (Wiederholung) |

# Module 14021 Explainable Machine Learning

assign to: Computer Science

## Study programme Cyber Security

| Degree | Module Number | Module Form |
|---|---|---|
| Master of Science | 14021 | Compulsory elective |

| | |
|---|---|
| **Modul Title** | **Explainable Machine Learning**<br>Erklärbares Maschinelles Lernen |
| **Department** | Faculty 1 - Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology |
| **Responsible Staff Member** | Prof. Dr. rer. biol. hum. Schneider, Erich |
| **Language of Teaching / Examination** | English |
| **Duration** | 1 semester |
| **Frequency of Offer** | Every winter semester |
| **Credits** | 6 |
| **Learning Outcome** | Students understand the interpretability and explainability of machine learning systems. They master methods of interpretability and can optimise systems for interpretability. They are able to implement interpretability and explainability mechanisms for machine learning systems. |
| **Contents** | The most significant disadvantage of machine learning and deep learning algorithms today: the interpretability of models. To trust predictions of real-life applications of AI it is important to understand how (Explainability) and why (Interpretability) a prediction is made.<br>• Key Concepts of Interpretability and Explainability Challenges<br>• Fundamentals of Feature Importance and Impact<br>• Global and Local Model-Agnostic Explainability Methods<br>• Anchor and Counterfactual Explanations<br>• Visualizing Convolutional Neural Networks<br>• Interpretation Methods for multivariate Forecasting and Sensitivity Analysis<br>• Tuning for Explainability |
| **Recommended Prerequisites** | Basic knowledge of programming and machine learning |
| **Mandatory Prerequisites** | Knowledge of the content of module<br>• 11881: Foundations of Data Mining<br><br>or<br>• 12351: Grundlagen des Data Mining |

| | |
|---|---|
| **Forms of Teaching and Proportion** | Lecture - 2 hours per week per semester<br>Laboratory training - 2 hours per week per semester<br>Self organised studies - 120 hours |
| **Teaching Materials and Literature** | • Script and presentations are available for download in Moodle at the beginning of the semester and on an ongoing basis. Problems for exercises and instructions for lab experiments can be downloaded.<br><br>• Serg Masis, Interpretable Machine Learning with Python: Learn to build interpretable high-performance models with hands-on real-world examples, Packt 2021<br>• Ajay Thampi, Interpretable Ai: Building Explainable Machine Learning Systems, Manning 2022<br>• Christoph Molnar, Interpretable Machine Learning: A Guide For Making Black Box Models Explainable, 2022<br>• Uday Kamath; John Liu, Explainable Artificial Intelligence: An Introductionto Interpretable Machine Learning, Springer 2021 |
| **Module Examination** | Prerequisite + Final Module Examination (MAP) |
| **Assessment Mode for Module Examination** | **Prerequisite:**<br>• Successful completion of exercises and presentation of results in course<br><br>**Final module examination:**<br>• Written examination, 120 min. |
| **Evaluation of Module Examination** | Performance Verification – graded |
| **Limited Number of Participants** | none |
| **Remarks** | • Study programme Informatik M.Sc.: Compulsory elective module in complex „Angewandte und Technische Informatik" (level 400)<br>• Study programme Artificial Intelligence M.Sc.: Compulsory elective module in complex „Learning and Reasoning“<br>• Study programme Künstliche Intelligenz Technologie M.Sc.: Compulsory elective module in complex „Software-basierte Systeme“<br>• Study programme Cyber Security M.Sc.: Compulsory elective module in complex „Computer Science"<br>• Study programme Medizininformatik B.Sc.: Compulsory elective module in complex „Informatik" |
| **Module Components** | • Lecture: Explainable Machine Learning<br>• Accompanying laboratory<br>• Accompanying Examination |
| **Components to be offered in the Current Semester** | **140220** Lecture<br>Explainable Artificial Intelligence - 2 Hours per Term<br>**140221** Exercise<br>Explainable Artificial Intelligence - 2 Hours per Term<br>**140224** Examination<br>Explainable Artificial Intelligence |

**Erläuterungen**

Das Modulhandbuch bildet als Teil der Prüfungsordnung die Rechtsgrundlage für ein ordnungsgemäßes Studium. Darüber hinaus soll es jedoch auch Orientierung bei der Gestaltung des Studiums geben.

Dieses Modulhandbuch wurde am 06. November 2025 automatisch für den Master (universitär)-Studiengang Cyber Security (universitäres Profil), PO-Version 2017, aus dem Prüfungsverwaltungssystem auf Basis der Prüfungsordnung generiert. Es enthält alle zugeordneten Module einschließlich der ausführlichen Modulbeschreibungen mit Stand vom 06. November 2025. Neben der Zusammensetzung aller Veranstaltungen zu einem Modul wird zusätzlich das Veranstaltungsangebot für das jeweils aktuelle Semester gemäß dem Veranstaltungsverzeichnis der BTU ausgegeben.

The module catalogue is part of the examination regulation and as such establishes the legal basis for studies according to the rules. Furthermore, it should also give orientation for the organisation of the studies.

This module catalogue was generated automatically by the examination administration system on the base of the examination regulation on the 6 November 2025, for the Master (universitär) of Cyber Security (research-oriented profile). The examination version is the 2017, Catalogue contains all allocated modules including the detailed module descriptions from 6 November 2025. Apart from the composition of all components of a module, the list of lectures, seminars and events for the current semester according to the catalogue of lectures of the BTU is displayed.