Modulhandbuch
M. Sc. IT Security

Fachbereich Informatik
Technische Universität Darmstadt

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Informatik

Modulhandbuch M. Sc. IT Security

Technische Universität Darmstadt

Fachbereich Informatik

Hochschulstr. 10

64289 Darmstadt

Redaktion

Dipl.-Inform. Tim Neubacher

Jasmin Boghrat, M.A.

Stand: 14.02.24

Inhaltsverzeichnis

Modulhandbuch
M. Sc. IT Security

Wahlbereich Cryptography and Foundations

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Einführung in die Kryptographie</td></tr>
<tr><td>Modul Nr.
20-00-0085</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0085-iv</td><td>Einführung in die Kryptographie</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Math. Grundlagen:
● Berechnungen in Kongruenz- und Restklassenringen

Grundlagen der Verschlüsselung:
● Symmetrische vs. Asymmetrische Kryptosysteme
● Block- und Stromchiffren, AES, DES
● Kryptanalyse
● Wahrscheinlichkeit und Perfekte Sicherheit
● Verschlüsselung mit öffentlichen Schlüsseln
● RSA, Diffie-Hellman, ElGamal
● Faktorisierung großer Zahlen
● Diskrete Logarithmen
● Kryptografische Hashfunktionen
● Digitale Signaturen
● Identifikation</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
● Verstehen der mathematischen Grundlagen der Kryptographie wie z.B. Berechnungen in Kongruenz- und Restklassenringen, Faktorisierung großer Zahlen, Wahrscheinlichkeit und Perfekte Sicherheit

● Verstehen der Prinzipien von Public und Secret-Key-Verschlüsselung und der relevanten Verfahren einschließlich ihrer Sicherheit und Effizienz

● Verstehen der Prinzipien digitaler Signaturen und der relevanten Verfahren einschließlich ihre Sicherheit und Effizienz</td></tr>
</table>

4	**Voraussetzung für die Teilnahme** Empfohlen: ● Lineare Algebra ● Funktionale und objektorientierte Programmierkonzepte
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0085-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0085-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** ● Johannes Buchmann: Einführung in die Kryptographie, 5. Auflage, Springer-Verlag, 2010, 278 p. ISBN: 978-3-642-11185-3 ● Johannes Buchmann: Cryptographic Protocols. Vorlesungsskript (u.a. Undeniable, Fail-Stop und Blind Signatures) ● Neal Koblitz: A Course in Number Theory and Cryptography, Springer Verlag, 1994 ● Alfred J. Menezes, Paul C. van Oorschot, Scot A. Vanstone: Handbook of Applied Cryptography, CRC Press, 1997 (erhältlich als PDF) ● Bruce Schneier: Applied Cryptography, John Wiley & Sons, Inc., 1994 ● Douglas R. Stinson: Cryptography - Theory and Practice, CRC Press, 1995 ● Gustavus J. Simmons: Contemporary Cryptology - The Science of Information Integrity, IEEE Press, 1992

10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Formale Methoden der Informationssicherheit</td></tr>
<tr><td>Modul Nr.
20-00-0362</td><td>Leistungspunkte
9 CP</td><td>Arbeitsaufwand
270 h</td><td>Selbststudium
180 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0362-iv</td><td>Formale Methoden der Informationssicherheit</td><td>9</td><td>integrierte Veranstaltung</td><td>6</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
● formale Modellierung sicherheitskritischer Systeme in Prädikatenlogik
● Theoretische Grundlagen von Zugriffskontrollen und Informationsflusskontrollen
● formale Modellierung von Sicherheitseigenschaften in Prädikatenlogik
● Unterscheidung von qualitativen und quantitativen Sicherheitseigenschaften
● Entscheidbarkeits- und Komplexitätsresultate für Sicherheitseigenschaften
● Verifikation von Sicherheitsgarantien in verteilten Systemen
● Auswirkung von Komposition und Verfeinerung auf Sicherheitsgarantien
● formale Sprachen zur Beschreibung von Sicherheitspolitiken und deren Semantik
● Zertifizierung sicherheitskritischer Systeme</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung kennen Studierende relevante formale Sicherheitsmodelle und Analysetechniken. Sie verstehen fundamentale Unterschiede zwischen verschiedenen Klassen von Sicherheitseigenschaften und das Zusammenspiel zwischen schrittweiser Softwareentwicklung und Sicherheitseigenschaften. Sie können Systeme und Sicherheitsanforderungen formal modellieren und sicherheitsrelevante Aspekte basierend auf formalen Spezifikationen formal analysieren.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiengangs Informatik, insbesondere grundlegende Logikkenntnisse und Fähigkeit mit formalen Sprachen und Kalkülen umzugehen</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0362-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0362-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** ● M. Bishop: Computer Security, Addison-Wesley ● J. Biskup: Security in Computing Systems, Springer-Verlag ● C. P. Pfleeger, S. L. Pfleeger: Security in Computing, Prentice Hall ● D. Denning: Cryptography and Data Security, Addison Wesley Die Literaturempfehlungen werden kontinuierlich aktualisiert.
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Kryptoplexität</td></tr>
<tr><td>Modul Nr.
20-00-0585</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0585-iv</td><td>Kryptoplexität</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Algorithmische Komplexität von kryptographischen Bausteinen wie One-Way-Funktionen, digitalen Signaturen, Commitments, Verschlüsselungen etc. Insbesondere ihre Relationen, z.B. ob man aus jedem Signaturverfahren auch ein Verschlüsselungsverfahren bauen kann. Gelegentliche "Ausflüge" in die Komplexitätstheorie, sofern relevant.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme können die Teilnehmer abstrakte kryptographische Eigenschaften und ihr Verhältnis untereinander beurteilen. Die lernen die Zusammenhänge zwischen Kryptographie und Komplexitätstheorie und werden in die Lage versetzt, unter Schranken in der Kryptographie mittels verschiedener Techniken zu beweisen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Einführung in die Kryptographie</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
[20-00-0585-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Leistungspunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:</td></tr>
</table>

	• [20-00-0585-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** ● Arora, Barak: Computational Complexity: A Modern Approach, 2007 (auch online erhältlich). ● Balcazar, Diaz, Gabarro; Structural Complexity I und II, 1995 (nicht mehr als Hardcover verfügbar) ● Katz, Lindell: Introduction to Modern Cryptography, 2007 ● Goldreich: Foundations of Cryptography, Volume I und II, 2001 und 2004 (als Online-Variante erhältlich) ● Goldreich: Computational Complexity: A Conceptual Approach, 2006 (als Online-Variante erhältlich)
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Automatisches Beweisen</td></tr>
<tr><td>Modul Nr.
20-00-0660</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0660-iv</td><td>Automatisches Beweisen</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
● Theoretische Grundlagen der im automatischen Beweisen verwendeten Kalküle für Logik erster Stufe
● Korrektheits- und Vollständigkeitsbeweise
● Algorithmen und Datenstrukturen, die in automatischen Beweisern für Logik erster Stufe eingesetzt werden
● Vergleich verschiedener Ansätze im automatischen Beweisen
● Grundlagen moderner SAT- und SMT-Lösungswerkzeuge</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die erfolgreiche Teilnahme an der Lehrveranstaltung versetzt die Studierenden in die Lage, die wichtigsten modernen automatische Beweisverfahren im Detail zu verstehen, ihre Vor- und Nachteile zu beurteilen und in der Praxis anzuwenden.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Stark empfohlen wird die Teilnahme an der Vorlesung “Aussagen- und Prädikatenlogik” oder vergleichbarer Veranstaltungen.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0660-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Leistungspunkten</td></tr>
</table>

	Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0660-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Robinson, Voronkov: Handbook of Automated Reasoning, 2 vols., North-Holland
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
Forschungsorientierte Kryptographie</td></tr>
<tr><td>Modul Nr.
20-00-0680</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="5">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0680-iv</td><td>Forschungsorientierte Kryptographie</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
Aktuelle Arbeiten aus dem Gebiet der Kryptographie und Komplexitätstheorie verstehen und neue Forschungsansätze herausarbeiten.</td></tr>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Durch eine erfolgreiche Teilnahme am Kurs werden die Teilnehmer in die Lage versetzt, wissenschaftliche Arbeiten weitgehend selbstständig zu lesen und wichtige Details einer Arbeit zu erkennen. Sie können die Arbeiten anderer präsentieren und neue Forschungsfragen ableiten.</td></tr>
<tr><td>4</td><td colspan="5">Voraussetzung für die Teilnahme
Empfohlen:
Einführung in die Kryptographie
Kryptoplexität</td></tr>
<tr><td>5</td><td colspan="5">Prüfungsform
Bausteinbegleitende Prüfung:
[20-00-0680-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.
Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)</td></tr>
<tr><td>6</td><td colspan="5">Voraussetzung für die Vergabe von Leistungspunkten
Bestehen der Prüfung (100%)</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0680-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** ● Arora, Barak: Computational Complexity: A Modern Approach, 2007 (auch online erhältlich). ● Balcazar, Diaz, Gabarro; Structural Complexity I und II, 1995 (nicht mehr als Hardcover verfügbar) ● Katz, Lindell: Introduction to Modern Cryptography, 2007 ● Goldreich: Foundations of Cryptography, Volume I und II, 2001 und 2004 (als Online-Variante erhältlich) ● Goldreich: Computational Complexity: A Conceptual Approach, 2006 (als Online-Variante erhältlich)
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Kryptographie in der Praxis</td></tr>
<tr><td>Modul Nr.
20-00-0993</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0993-iv</td><td>Kryptographie in der Praxis</td><td>6</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Schlüsselableitung, Schlüsselaustausch, sichere Kommunikation, credentials, crypto currencies (TLS, SSH, IPSec, Bitcoin,…).</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Absolvierung verstehen die Teilnehmer das Design und die Sicherheitsgarantien von kryptographischen Verfahren in der Praxis, die heutzutage im alltäglichen Einsatz sind. Die Teilnehmer lernen die Bedeutung und Grenzen von Sicherheitsmodellen und Sicherheitsbeweisen für die Praxis kennen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Einführung in die Kryptographie</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0993-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Leistungspunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:
• [20-00-0993-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)</td></tr>
</table>

8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Blockchain Technology						
Modul Nr. 20-00-1010	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1010-iv	Blockchain Technology	6	Integrierte Veranstaltung	4

2 Lerninhalt

Konzepte von Blockchain Technologies:
- Kryptographische Bausteine: Hash-Funktionen, Signaturen, Commitments.
- Distributed Systems und Fehlertoleranz
- Broadcast- und Konsensverfahren
- Einführung in Bitcoin und Nakamoto Konsensus
- Mining, Inzentivmechanismen und Wallets
- Privacy in Blockchains
- Angriffe auf Kryptowährungen
- Smart Contracts und Anwendungen
- Skalierbarkeit von Blockchain-Systemen
- Blockchain-Ökosystem (insb. DeFi und Altcoins)

3 Qualifikationsziele / Lernergebnisse

Die Teilnehmer*innen verstehen nach erfolgreichem Besuch des Kurses die grundlegenden technischen und theoretischen Konzepte von Blockchain Technologien. Insbesondere werden folgende Fragestellungen behandelt:
- Den Umgang mit kryptographischen Bausteinen und kryptographischen Protokollen und deren Sicherheitsanalyse.
- Die Entwicklung von sicheren verteilten Systemen
- Die grundlegenden Konzepte von Blockchain-Systemen, insbesondere Konsensmechanismen, Wallets und Mining
- Mögliche Angriffe auf Kryptowährungen und die zugrundeliegende Technologie
- Die Grundkonzepte der Entwicklung von Smart Contracts und deren Anwendung
- Neue Lösungsansätze zur Verbesserung von Blockchains in Bezug auf Anonymität, Skalierbarkeit und Sicherheit
- Ein Überblick über verschiedene Altcoins und deren Vor-/Nachteile

4	**Voraussetzung für die Teilnahme** Empfohlen: Besuch der Vorlesung “Introduction to Cryptography / Einführung in die Kryptographie” bzw. entsprechende Kenntnisse aus anderen Studiengängen
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1010-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1010-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Kryptographische Protokolle</td></tr>
<tr><td>Modul Nr.
20-00-1032</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1032-iv</td><td>Kryptographische Protokolle</td><td>6</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Kryptographische Protokolle erlauben es mehreren Parteien mit möglicherweise unterschiedlichen Interessen, gemeinsam bestimmte Aufgaben zu erfüllen. Diese Lehrveranstaltung behandelt grundlegende und fortgeschrittene kryptographische Protokolle und ihre Anwendungen, wie z.B. Commitments, Secure Coin Flipping, Zero-Knowledge Beweise, Mixnetze, Anonyme Credentials, Private Information Retrieval, Sichere Mehrparteienberechnungen und Hardware-unterstützte kryptographische Protokolle.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende kennen grundlegende und fortgeschrittene kryptographische Protokolle, können deren Effizienz und Sicherheit bewerten und vergleichen, und kennen deren grundlegenden Anwendungen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Grundkenntnisse der Kryptographie werden sehr empfohlen, z.B. durch erfolgreiches Bestehen der Veranstaltung "Einführung in die Kryptographie".</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-1032-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Leistungspunkten</td></tr>
</table>

	Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1032-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Einführung in das Quantencomputing					
Modul Nr. 20-00-1136	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1136-iv	Einführung in das Quantencomputing	6	Integrierte Veranstaltung	4

2 Lerninhalt

Allgemeine Einführung und Motivation
Einführung in die Quantenmechanik (Zustände, Messungen, Evolution, ein kurzer Überblick zur linearen Algebra)
Elementare Quantengatter und Schaltkreismodell
Universelle Quantenberechnungen
Quantenparallelismus und der Deutsch-Jozsa-Algorithmus
Simon’s Algorithm
Die Fourier-Transformation
Der Shor-Algorithmus
Das Problem der versteckten Untergruppe
Der Grover-Algorithmus
Quantenfehlerkorrektur und Fehlertoleranz
Verschränkung und Nichtlokalität
Eine grundlegende Einführung in die Quantenschlüsselverteilung
Überblick über Quantencomputerplattformen und Aussagen zur Quantenüberlegenheit

3 Qualifikationsziele / Lernergebnisse

Nach Abschluss des Kurses sind die Studierenden mit allen grundlegenden Konzepten der Quanteninformationsverarbeitung und -berechnung vertraut und können diese mit der Quantenprogrammiersprache Qiskit programmieren. Sie lernen die wichtigsten "Eigenheiten" der Quantenwelt kennen und können diese mit rechnerischen und kryptographischen Aufgabenstellungen verbinden. Am Ende der Vorlesung wird eine Zusammenfassung der neuesten Entwicklungen in Industrie und Wissenschaft gegeben, die es den Studierenden ermöglicht, ihre zukünftigen Interessen in diesem Bereich zu steuern.

4 Voraussetzung für die Teilnahme

Empfohlen werden grundlegende Kenntnisse in elementarer linearer Algebra (Matrixmultiplikation, Ermittlung von Eigenwerten)

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1136-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Empfohlen werden grundlegende Kenntnisse in elementarer linearer Algebra (Matrixmultiplikation, Ermittlung von Eigenwerten)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1136-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulhandbuch

M. Sc. IT Security

Wahlbereich
Systems and Communication Security

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Netzsicherheit</td></tr>
<tr><td>Modul Nr.
20-00-0512</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0512-iv</td><td>Netzsicherheit</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die integrierte Veranstaltung Netzsicherheit umfasst Sicherheits-Prinzipien und -Praxis in Telekommunikationsnetzen und dem Internet. Die grundlegenden Verfahren aus dem Bereich IT Sicherheit und Kryptographie werden auf den Bereich der Kommunikationsnetze übertragen. Hierbei verfolgen wir einen Top-down Ansatz. Beginnend mit der Anwendungsschicht erfolgt eine detaillierte Betrachtung von Prinzipien und Protokollen zur Absicherung von Netzen. Ergänzend zu etablierten Mechanismen werden ausgewählte aktuelle Entwicklungen im Bereich Netzsicherheit erläutert.
Lerninhalte:
- Netzsicherheit: Einführung, Motivation und Herausforderungen
- Grundlagen: Ein Referenzmodell für Netzsicherheit, Sicherheitsstandards für Netze und das Internet, Bedrohungen, Angriffe, Sicherheitsdienste und -mechanismen
- Kryptographische Grundlagen zur Absicherung von Netzen: Symmetrische Kryptographie und deren Anwendung in Netzen, asymmetrische Kryptographie und deren Anwendung in Netzen, unterstützende Mechanismen zur Implementierung von Sicherheitslösungen
- Sicherheit auf der Anwendungschicht
- Sicherheit auf der Transportschicht
- Sicherheit auf der Vermittlungsschicht
- Sicherheit auf der Sicherungsschicht
- Sicherheit auf der Bitübertragungsschit und physische Sicherheit
- Angewandte Netzsicherheit: Firewalls, Intrusion Detection Systeme
- Ausgewählte Themen der Netzsicherheit</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung haben die Studierenden ein umfassendes Wissen auf dem Gebiet der Netzsicherheit mit dem Schwerpunkt auf Internetsicherheit. Sie können die wichtigsten Grundlagen der IT Sicherheit sowie der Kryptographie auf den Bereich Kommunikationsnetze übertragen und anwenden. Die Studierenden können die wichtigsten Basistechnologien zur Absicherung von Netzen</td></tr>
</table>

	unterscheiden. Sie weisen ein tiefgehendes Verständnis von Sicherheitsmechanismen auf den unterschiedlichen Protokollschichten auf (Anwendungschicht, Transportschicht, Vermittlungsschicht, Sicherungsschicht, physikalische Schicht). Somit sind sie in der Lage, die Charakteristiken und Grundprinzipien des Problemraumes Netzsicherheit detailliert zu erläutern und weisen auf diesem Feld ein fundiertes Wissen in Praxis und Theorie auf. Darüber hinaus können sie aktuelle Entwicklungen im Bereich Netzsicherheit erläutern (z.B. Sicherheit in peer-to-peer Systemen, Sicherheit in mobilen Netzen, etc.). Die Übung vertieft das theoretische Wissen durch Literatur-, Rechen- und praktische Implementierungs-/Anwendungsübungen.
4	**Voraussetzung für die Teilnahme** Empfohlen: Grundlagen der IT-Sicherheit, Kryptographie und Kommunikationsnetze
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0512-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0512-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.

9	**Literatur** Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security – Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002, ISBN: 978-0-14-046019-6; weiterhin ausgewählte Buchkapitel und ausgewählte wissenschaftliche Veröffentlichungen
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Embedded System Security</td></tr>
<tr><td>Modul Nr.
20-00-0581</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
135 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0581-iv</td><td>Embedded System Security</td><td>6</td><td>integrierte Veranstaltung</td><td>3</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Trusted Computing
● Authentifiziertes Booten
● Binding und Sealing
● Messen der Plattform-Integrität und Attestierung
● Direct Anonymous Attestation
● Trusted Platform Modules (TPM/MTM)
● On-board Credentials

Mobile Sicherheit mit Fokus auf Smartphones
● Sicherheitsarchitekturen
● Ausgewählte Zugriffsmodelle
● Kontext-basierte Sicherheitsrichtlinien
● Ausgewählte moderne Angriffstechniken

Hardware-basierte Kryptographie
● Sichere Berechnungen basierend auf Hardware
● Einführung in Physikalisch Unklonbare Funktionen (PUFs)</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Durch die erfolgreiche Teilnahme an dieser Veranstaltung erwerben Studierende detailliertes Wissen über ausgewählte Aspekte der eingebetteten Systemsicherheit (Hardware- und Software-basiert).</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Grundlagen der Kryptographie</td></tr>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0581-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0581-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** ● Challener, David, VanDoorn, Leendert, Safford, David, Yoder, Kent, Catherman, Ryan "A Practical Guide to Trusted Computing", IBM Press, 2007 ● Smith, Sean W. "Trusted Computing Platforms: Design and Applications", Springer Verlag, 2005
10	**Kommentar**

Modulbeschreibung

Modulname Physical Layer Security in Drahtlosen Systemen						
Modul Nr. 20-00-0745	**Leistungspunkte** 5 CP	**Arbeitsaufwand** 150 h	**Selbststudium** 105 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0745-iv	Physical Layer Security in Drahtlosen Systemen	5	integrierte Veranstaltung	3

2 Lerninhalt

Physical Layer Security Verfahren zur Absicherung drahtloser Kommunikation versprechen eine informationstheoretische Sicherheit auf der Bitübertragungsschicht (Physical Layer). Die integrierte Veranstaltung betrachtet die Theorie und Praxis von Physical Layer Security. Hierzu werden ausgewählte theoretische Grundlagen eingeführt und die Übertragung dieser Grundlagen hin zu praktikablen Lösungen diskutiert. Angriffe auf (praktische) Physical Layer Security-Verfahren werden erörtert. Theoretische und praktische Übungen sowie die Vorstellung ausgewählter Forschungsergebnisse in Seminarvorträgen vertiefen die Veranstaltung.

Lerninhalte:

- Eigenschaften des Physical Layer
- Grundlagen informationstheorischer Sicherheit und Abgrenzung zur Kryptographie
- Physical Layer Security Verfahren (u.a. Cooperative Jamming, Orthogonal Blinding, Zero-Forcing, Interference Alignment, Key Extraction)
- Praktische Aspekte von Physical Layer Security Verfahren
- Praktische Implementierung von Physical Layer Security-Verfahren mit Software Defined Radios
- Ausgewählte aktuelle Ansätze zu Physical Layer Security

3 Qualifikationsziele / Lernergebnisse

Nach erfolgreicher Teilnahme an der Veranstaltung besitzen die Studierenden ein theoretisches Grundwissen sowie ein fundiertes praktisches Wissen auf dem Gebiet von Physical Layer Security. Sie können die wichtigsten informationstheoretischen Grundlagen erläutern und kennen theoretische wie praktische Verfahren im Detail. Sie sind in der Lage praktische Verfahren zu beurteilen und Schwächen darzulegen. Die Studierenden haben Kompetenzen in der praktischen Realisierung von Physical Layer Security-Verfahren auf Basis von Software-defined Radios. Sie können sich aktuelle Arbeiten zum Stand der

	Forschung zu Physical Layer Security selbstständig aneignen und das erarbeitete Wissen verständlich vermitteln.
4	**Voraussetzung für die Teilnahme** Empfohlen: Grundlagen der Mobilen Netze
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0745-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0745-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Ausgewählte Buchkapitel und ausgewählte wissenschaftliche Veröffentlichungen
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
Drahtlose Netze zur Krisenbewältigung: Grundlagen, Entwurf und Aufbau von Null</td></tr>
<tr><td>Modul Nr.
20-00-0780</td><td>Leistungspunkte
5 CP</td><td>Arbeitsaufwand
150 h</td><td>Selbststudium
105 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="5">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0780-iv</td><td>Drahtlose Netze zur Krisenbewältigung: Grundlagen, Entwurf und Aufbau von Null</td><td>6</td><td>integrierte Veranstaltung</td><td>3</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
Die Kommunikationsfähigkeit der Bevölkerung untereinander ist für die Bewältigung von Krisen von höchster Bedeutung. In dieser Veranstaltung wird der Aufbau von drahtlosen Kommunikationsnetzen von Null behandelt, d.h. unter der Annahme, dass keinerlei Kommunikationsinfrastruktur mehr vorhanden ist. Die Veranstaltung vermittelt theoretische Grundlagen aus den Bereichen der Nachrichtentechnik und des Amateurfunks und vertieft diese um die nötigen Kenntnisse, um Netze für den Krisenfall zu entwerfen und praktisch zu realisieren. Die vorgestellten Verfahren umfassen dabei Reichweiten von lokaler Kommunikation bis hin zur Kommunikation um den ganzen Globus, ohne auf bestehende Infrastruktur angewiesen zu sein.
Theoretische Übungen sowie das Durchführen von Messungen, der Aufbau von Schaltungen und die Vorführung von Funkverfahren in unserer Laborumgebung vertiefen die Veranstaltung.
Lerninhalte:
- Signale, Wellenausbreitung, Antennen und elektrotechnische Grundlagen
- Verfahren zur Modulation und Demodulation analoger und digitaler Signale (OFDM, ATV/SSTV, Packet Radio, SSB, ...)
- Systemaspekte für Kommunikation im Krisenfall
- Entwurf und praktischer Aufbau von drahtlosen Kommunikationssystemen für den Krisenfall von Null</td></tr>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung besitzen die Studierenden theoretisches und praktisches Wissen auf dem Gebiet der drahtlosen, infrastrukturlosen Kommunikation im Krisenfall. Sie verstehen die physikalischen und elektrotechnischen Grundlagen der drahtlosen Kommunikation und kennen theoretische wie praktische Funkverfahren im Detail. Sie sind in der Lage ein Praktisches Kommunikationsystem von Null aufzubauen und zu betreiben. Die Studierenden erwerben Kompetenzen im Bereich Amateurfunk und Software-Defined Radios.</td></tr>
</table>

4	**Voraussetzung für die Teilnahme**
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0780-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0780-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Ausgewählte Buchkapitel und ausgewählte wissenschaftliche Veröffentlichungen
10	**Kommentar**

Modulbeschreibung

Modulname Mensch- und Identitätsfokussiertes Maschinelles Lernen						
Modul Nr. 20-00-1118	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1118-iv	Mensch- und Identitätsfokussiertes Maschinelles Lernen	6	Integrierte Veranstaltung	4

2 Lerninhalt

Hintergründe und Konzepte von Human-Centric Machine Learning: Das Ziel von Identität und Human-Centric Machine Learning. Die Unterschiede zwischen Identitätslernen und anderen gängigen Klassifikationsarten.

Repräsentationsextraktion für subjektbezogene Daten: Methoden für die Feature Erstellung für identitätsbezogene Anwendungen. Grundlagen und Hintergründe für handgefertigte oder Deep Learning Features.

Deep-Learning Strategien für Identitätsrepräsentationen: Erlernen von Identitätsrepräsentationen mit Hilfe von Deep Learning. Lernstrategien und Loss-Funktionen.

Netzwerkarchitekturen und identitätsspezifische Komponenten.

Knowledge Transfer und Distillation: Transfer Learning und Identitätsrepräsentation. Konzepte und Anwendungen von Knowledge Distillation.

Effizientes Machine Learning: Beziehung zwischen Ressourcenbeschränkungen, Green-AI und Deep Learning. Methoden zum Aufbau effizienter Lösungen für Maschinelles Lernen.

Synthetische Identität: Die Notwendigkeit einer synthetischen Identität. Synthetische Identität als Adversarial. Generierung synthetischer identitätsgesteuerter Daten unter verschiedenen Einschränkungen.

Machine Learning Biases: Analyse der demografischen Fairness und der Ursachen der Fairnessprobleme. ML-basierte Abmilderung von demografischen Bias.

Privatsphäre erlernen: Analyse von unbeabsichtigt gelernten Informationen. Lernstrategien zur gezielten Unterdrückung von Informationen auf verschiedenen Repräsentationsebenen.

	Data Utility: Verständnis der Auswirkungen von Data Utility im Lernprozess. Verstehen von Sample Utility im Betrieb. ML-Konzepte und Strategien zur Schätzung von Sample Utilities. Angriffe auf Sample-Level: Überblick über Adversarial, Sample Manipulation und andere Angriffe auf Human-Centric ML. Deep Learning Konzepte, Netzwerkblöcke und LossStrategien um Sample-Level Angriffe zu erkennen und zu umgehen. Explainability: Überblick über den Bedarf von Explainability in verschiedenenen Entscheidungsprozessen. Verschiedene Strategien um Explainability für Themen aus vergangenen Vorlesungen.
3	**Qualifikationsziele / Lernergebnisse** Nach erfolgreichem Besuch des Kurses sind die Studierenden mit Konzepten des maschinellen Lernens im Umgang mit personen- und identitätsbezogenen Informationen vertraut. Sie verstehen die grundlegenden Techniken für die Extraktion subjektspezifischer Repräsentationen, einschließlich der damit verbundenen Konzepte für Knowledge Transfer und Distillation. Die Studierenden haben ein Verständnis für demografisch bedingte Verzerrungen beim maschinellen Lernen und Datenschutzbedenken zu Function-Creep erlangt, einschließlich der wichtigsten Konzepte zur Abschwächung dieser Probleme. Sie kennen die Anforderungen und Techniken, die für ein eingebettetes und effizientes HumanCentric Machine Learning erforderlich sind. Ebenfalls sind sie mit den Auswirkungen von Data Utility im Lernprozess und dem Hauptkonzept zur Schätzung der Utility von subjektbezogenen Daten vertraut. Sie werden fundiertes Wissen über die Erklärungsmethoden für ML-Entscheidungen auf der Grundlage von identitätsbezogenen Daten erlangen. Die Studierenden werden in die Konzepte der KI-Ethik und der KIRegulierung im Zusammenhang mit der Verarbeitung und Speicherung personenbezogener Daten eingeführt. Sie sind in der Lage, diese Techniken zur Lösung grundlegender Aufgaben im Bereich von Identitäts- und Human-Centric Machine Learning auf realistische Probleme anzuwenden.
4	**Voraussetzung für die Teilnahme** Empfohlen: Der vorherige Besuch der Veranstaltung „Visual Computing“ oder einer vergleichbaren Veranstaltung. Grundlagen in Mathematik und Wahrscheinlichkeitsrechnung.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1118-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)

6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%).
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1118-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulhandbuch
M. Sc. IT Security

Wahlbereich
Software and Application Security

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Sicherheit in Multimedia Systemen und Anwendungen</td></tr>
<tr><td>Modul Nr.
20-00-0093</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i. d. R. jedes Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0093-iv</td><td>Sicherheit in Multimedia Systemen und Anwendungen</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Studierenden erhalten einen Überblick über die Herausforderungen der Multimedia Sicherheit und den bekannten Lösungsansätzen hierzu. Dazu gehören die Konzepte der Medien-Integrität, -Vertraulichkeit und -Authentizität. Verfahren aus dem Bereichen digitale Wasserzeichen, robuste Hashverfahren, partielle Verschlüsslung, Multimedia Forensik und DRM sind dem Studenten bekannt. Er kann Herausforderungen der Multimedia Sicherheit aus einer Palette von Lösungsmechanismen bedarfsabhängig optimal adressieren.
● Partielle Verschlüsselungsverfahren für Video und Audio zur Sicherung der Vertraulichkeit und der Authentizität
● Digitale Wasserzeichen für Bild und Audio - Anwendungsgebiete, Methoden und Verfahren
● Digital Rights Management und Kopierschutzverfahren
● Visuelle Kryptographie

Neben der Diskussion von Algorithmen, deren Möglichkeiten, Grenzen und Schwachstellen nehmen auch die kommerziellen und gesellschaftlichen Aspekte des Einsatzes von Schutzmaßnahmen ihren Platz in der Vorlesung ein.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Studierenden erhalten einen Überblick über die Herausforderungen der Multimedia Sicherheit und den bekannten Lösungsansätzen hierzu. Dazu gehören die Konzepte der Medien-Integrität, -Vertraulichkeit und -Authentizität. Verfahren aus dem Bereichen digitale Wasserzeichen, robuste Hashverfahren, partielle Verschlüsslung, Multimedia Forensik und DRM sind den Studierenden bekannt. Sie können Herausforderungen der Multimedia Sicherheit aus einer Palette von Lösungsmechanismen bedarfsabhängig optimal adressieren.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Grundkenntnisse in Multimedia-Formaten und IT-Sicherheit.</td></tr>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0093-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0093-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** ● Steinmetz: Multimedia-Technologie. Grundlagen, Komponenten und Systeme, ISBN: 3540673326, Springer, Heidelberg, 2000 ● Dittmann: Digitale Wasserzeichen, Springer Verlag, ISBN 3 - 540 - 66661 - 3, 2000 ● Cox, Miller, Bloom: Digital Watermarking, Academic Press, San Diego, USA, ISBN 1-55860-714-5, 2002 ● und spezifische Veröffentlichungen aus Tagungsbänden
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
IT-Sicherheit</td></tr>
<tr><td>Modul Nr.
20-00-0219</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0219-iv</td><td>IT-Sicherheit</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Ausgewählte Konzepte der IT-Sicherheit (Kryptographie; Sicherheitsmodelle; Authentifikation; Zugriffskontrolle; Sicherheit in Netzen; Trusted Computing; Security Engineering; Privatsphäre und Datenschutz; Web- und Browser-Sicherheit; Informationssicherheitsmanagement, IT-Forensik, Cloud Computing)</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung sind die Studierenden in der Lage kritisch über gängige Mechanismen und Protokolle zur Erhöhung der IT-Sicherheit heutiger Systeme zu diskutieren. Studenten haben nach Abschluss der Veranstaltung in breites Wissen über IT-Sicherheit, Datenschutz und Privatsphäre im Internet.

Studierende sind vertraut mit modernen IT-Schutzkonzepten aus dem Bereich Kryptographie, Identitätmanagement, Web-, Browser- und Netzwerksicherheit. Sie sind in der Lage Angriffsvektoren in IT-Systemen zu erkennen und Gegenmaßnahmen zu entwickeln.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Besuch der Vorlesung Computersystemsicherheit</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0219-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0219-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** • C. Eckert: IT-Sicherheit, 3. Auflage, Oldenbourg Verlag, 2004 • J. Buchmann, Einführung in die Kryptographie, 2.erw. Auflage, Springer Verlag, 2001 • E. D. Zwicky, S. Cooper, B. Chapman: Building Internet Firewalls, 2. Auflage, O'Reilly, 2000 • B. Schneier, Secrets & Lies: IT-Sicherheit in einer vernetzten Welt, dpunkt Verlag, 2000 • W. Rankl und W. Effing: Handbuch der Chipkarten, Carl Hanser Verlag, 1999 • S. Garfinkel und G. Spafford: Practical Unix & Internet Security, O'Reilly & Associates
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Statische und dynamische Programmanalyse</td></tr>
<tr><td>Modul Nr.
20-00-0580</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0580-iv</td><td>Statische und dynamische Programmanalyse</td><td>6</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
- operationelle Semantiken für sequentielle und parallele Programme
- Übersicht über Techniken zur statischen und dynamischen Programmanalyse
- Abstrakte Interpretation
- Datenflussanalysen
- Slicing-Techniken
- typbasierte Programmanalysen
- Konzepte der Laufzeitüberwachung
- Implementierungstechniken zur Laufzeitüberwachung
- Sprachbasierte Sicherheit
- Korrektheit und Präzision von Programmanalysen</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung kennen Studierende ein Spektrum von unterschiedlichen Programmanalysen. Sie verstehen die Funktionsweise der einzelnen Analysetechniken und verstehen die Unterschiede zwischen diesen. Sie können beurteilen, welche Analysetechnik für welche Problemstellung in Frage kommt und haben die Fähigkeit, die ausgewählte Analysetechnik einzusetzen. Sie können Programmanalysen bezüglich ihrer Präzision und Korrektheit beurteilen. Sie können Programmanalysen auch implementieren und Varianten von bekannten Programmanalysen definieren.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiengangs Informatik, insbesondere grundlegende Logikkenntnisse und Fähigkeit, mit formalen Sprachen und Kalkülen umzugehen</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0580-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0580-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Formale Spezifikation und Verifikation von Software					
Modul Nr. 20-00-0794	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0794-iv	Formale Spezifikation und Verifikation von Software	6	Integrierte Veranstaltung	4

2 Lerninhalt

In dieser Vorlesung behandeln wir fortgeschrittene Themen aus dem Gebiet der formalen Spezifikation und deduktiven Verifikation objekt-orientierter Software.

Der Kurs deckt insbesondere folgende Themen ab:
* Spezifikation von Interfaces und Klassen mit Hilfe von Queries, Ghost- und Modellfeldern;
* Das "Framing" Problem: Statische und dynamische Frames
* Programmlogik und -kalkül als Grundlage der deduktiven Verifikation
* Spezifikation und Verifikation rekursiver Methoden und Schleifen
* Modulare Verifikation: Sichtbarkeiten, Beweis und Anwendung von Framing-Eigenschaften
* Automatische Erzeugung von Schleifeninvarianten und Methodenverträgen

Der Kurs behandelt vorwiegend sequentielle Programme. Es werden aber auch aktuelle Ansätze zur Spezifikation und Verifikation nebenläufiger bzw. verteilter Software diskutiert.

Für fast alle Themen wird deren praktische Anwendung mit Hilfe geeigneter Tools demonstriert und in den Übungen vertieft.

3 Qualifikationsziele / Lernergebnisse

* Erwerbung der Fähigkeit zur Spezifikation komplexer objekt-orientierter Software
* Studierende sollen in der Lage sein einen für das vorliegende Problem passenden Spezifikationsansatz auszuwählen und anzuwenden
* Studierende sollen in der Lage sein rekursive Methoden und Schleifen zu spezifizieren
* Studierende sollen in der Lage sein mit Hilfe von deduktiver Verifikation ihre Programme als korrekt zu beweisen

4 Voraussetzung für die Teilnahme

Empfohlen:

Grundlagenwissen über Logik erster Ordnung
Inhalt der Vorlesungen „Aussagen- und Prädikatenlogik“ und „Formale Methoden im Softwareentwurf“ oder vergleichbarer Veranstaltungen

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0794-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0794-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Sicherheitskritische Mensch-Computer-Interaktion</td></tr>
<tr><td>Modul Nr.
20-00-1025</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1025-iv</td><td>Sicherheitskritische Mensch-Computer-Interaktion</td><td>6</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Diese Lehrveranstaltung gibt eine fundierte und praxisbezogene Einführung sowie einen Überblick über Grundlagen, Methoden und Anwendungen der Mensch-Computer-Interaktion im Kontext von Sicherheit, Notfällen, Krisen, Katastrophen, Krieg und Frieden. Dies adressierend werden interaktive, mobile, ubiquitäre und kooperative Technologien sowie Soziale Medien vorgestellt. Hierbei finden klassische Themen wie benutzbare (IT-)Sicherheit, Industrie 4.0, Katastrophenschutz, Medizin und Automobil, aber auch Augmented Reality, Crowdsourcing, Shitstorm Management, Social Media Analytics und Cyberwar ihren Platz. Methodisch wird das Spektrum von Usable Safety- bis Usable Security Engineering von Analyse über Design bis Evaluation abgedeckt.

Details für das aktuelle Semester finden Sie unter www.peasec.de/lehre</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
• Verständnis sicherheitskritischer MCI und der zugrundeliegenden Disziplinen MCI sowie Krisen- und Sicherheitsmanagement
• Überblick über ausgewählte Grundlagen und Methoden sicherheitskritischer MCI (Usable Safety; Usable Security; Analyse, Design, Umsetzung, Evaluation; Recht, Ethik und Kultur)
• Orientierung in Anwendungsdomänen und -feldern
• Kenntnisse über sicherheitskritische interaktive Systeme (Betriebliche Informationssysteme, Krisenmanagementsysteme, Medizintechnik, Warn- und Assistenzsysteme)
• Kenntnisse über sicherheitskritische kooperative Systeme (Soziale Medien, Kooperationssysteme, Freiwillige Partizipation, Frieden und Sicherheit)</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1025-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1025-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Informationstechnologie für Frieden und Sicherheit</td></tr>
<tr><td>Modul Nr.
20-00-1026</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1026-iv</td><td>Informationstechnologie für Frieden und Sicherheit</td><td>6</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
- Grundlagen: Friedens-, Konflikt- und Sicherheitsforschung
o (Naturwissenschaftliche) Friedensforschung
o Informatische Friedensforschung
- Informatik in Militär, Krieg und Konflikten
o Militärische Nutzung von Informatik und Dual-Use-Problematik
o Cyberwar: Konflikte im Cyberspace mit Information Warfare, Vulnerabilität und Resilienz kritischer (IT-)Infrastrukturen, Fake News und Social Bots
o Terrorismus und terroristische Propaganda in sozialen Medien
- Informatik und Frieden
o Mensch-Computer-Interaktion zur Friedensförderung
o IT im Kontext politischer Aktivisten
o Bekämpfung terroristischer Propaganda in sozialen Medien
Themen für das aktuelle Semester finden Sie unter www.peasec.de/lehre</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
- Kenntnisse von Grundlagen der informatischen Friedens-, Konflikt- und Sicherheits-forschung
- Bewertung von IT zur Förderung oder Verhinderung von Frieden und Sicherheit
- Kenntnisse in der Gestaltung und Entwicklung von IT für Frieden</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1026-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.</td></tr>
</table>

	Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1026-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Automatische Softwareverifikation</td></tr>
<tr><td>Modul Nr.
20-00-1069</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1069-iv</td><td>Automatische Softwareverifikation</td><td>6</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Veranstaltung befasst sich mit dem Techniken zur automatischen Softwareverifikation und behandelt dabei folgende Themebereiche:
- operationelle Semantik von sequentiellen Programmen
- konfigurierbare Programmanalyse inklusive Konfiguration für Datenflussanalysen und Model Checking
- counter-example guided abstraction refinement (CEGAR)
- Bounded Model Checking
- k-Induktion
- kooperative Verifikation, insbesondere Conditional Model Checking
- inkrementelle Verifikation
- Nachprüfung von Verifikationsergebnissen (a la Proof-Carrying Code, Witness Validation)
- Generierung von Testeingaben mittels Verifizierern</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung können die Studierenden eine Vielzahl von Verfahren zur automatischen Verfikation benennen. Sie können die den Verfahren zugrunde liegenden Formalismen wiedergeben, die Funktionsweise der Verfahren beschreiben und die Verfahren klassifizieren. Außerdem können die Studierenden die Verfahren auf Beispielen anwenden und neue konfigurierbare Programmanalysen entwickeln.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:
Informatikkenntnisse entsprechend der ersten vier Semester des Bachelorstudiengangs Informatik, insbesondere Kenntnisse aus der Vorlesung „Aussagen- und Prädikatenlogik“ oder Vergleichbares.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1069-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1069-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Automatische Softwareverifikation</td></tr>
<tr><td>Modul Nr.
20-00-1069</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1069-iv</td><td>Automatische Softwareverifikation</td><td>6</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Veranstaltung befasst sich mit dem Techniken zur automatischen Softwareverifikation und behandelt dabei folgende Themebereiche:
- operationelle Semantik von sequentiellen Programmen
- konfigurierbare Programmanalyse inklusive Konfiguration für Datenflussanalysen und Model Checking
- counter-example guided abstraction refinement (CEGAR)
- Bounded Model Checking
- k-Induktion
- kooperative Verifikation, insbesondere Conditional Model Checking
- inkrementelle Verifikation
- Nachprüfung von Verifikationsergebnissen (a la Proof-Carrying Code, Witness Validation)
- Generierung von Testeingaben mittels Verifizierern</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung können die Studierenden eine Vielzahl von Verfahren zur automatischen Verfikation benennen. Sie können die den Verfahren zugrunde liegenden Formalismen wiedergeben, die Funktionsweise der Verfahren beschreiben und die Verfahren klassifizieren. Außerdem können die Studierenden die Verfahren auf Beispielen anwenden und neue konfigurierbare Programmanalysen entwickeln.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:
Informatikkenntnisse entsprechend der ersten vier Semester des Bachelorstudiengangs Informatik, insbesondere Kenntnisse aus der Vorlesung „Aussagen- und Prädikatenlogik“ oder Vergleichbares.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1069-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1069-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Verifikation paralleler Programme</td></tr>
<tr><td>Modul Nr.
20-00-1079</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1079-iv</td><td>Verifikation paralleler Programme</td><td>6</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Veranstaltung befasst sich mit überwiegend automatischen Techniken zur Verifikation von parallelen Programmen, insbesondere multi-threaded Programmen mit gemeinsamen Speicher. Die Veranstaltung behandelt dabei folgende Themenbereiche:
- Semantik von parallelen Programmen (z.B. Interleaving-Semantik, Semantik von ausgewählten schwachen Speichermodellen)
- Statische und dynamische Techniken zur Erkennung von Data Races
- Techniken der Deadlockanalyse
- Analyse von Programmeigenschaften (z.B. mittels Sequentialisierung, Bounded Model Checking, etc.)
- Partial Order Reduction
- Thread-modulare Verifikation
- Verifikation unter schwachen Speichermodellen</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung können die Studierenden Verfahren zur Verifikation von parallelen Programmen, insbesondere Verfahren zur Analyse von Data Races, Deadlocks und Sicherheitseigenschaften (Safety) benennen. Sie können die den Verfahren zugrunde liegenden Formalismen wiedergeben, die Funktionsweise der Verfahren beschreiben und die Verfahren auf Beispielen anwenden. Außerdem können die Studierenden die Stärken und Schwächen der Verfahren beurteilen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Informatikkenntnisse entsprechend der ersten vier Semester des Bachelorstudiengangs Informatik. Vorteilhaft, aber nicht erforderlich ist der Besuch der Veranstaltung „Automatische Software Verifikation“.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1079-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1079-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Programmanalyse</td></tr>
<tr><td>Modul Nr.
20-00-1122</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1122-vl</td><td>Programmanalyse</td><td>6</td><td>Vorlesung und Übung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Statische Analysen sind Werkzeuge die Informationen von Programmen extrahieren ohne diese auszuführen. Statische Analysen haben vielseitige Anwendungen in integrierten Entwicklungsumgebungen (IDEs), Compilern und Continous Integration Servern. Zum Beispiel werden statische Analysen in IDEs verwendet um Programmfehler und Sicherheitslücken zu erkennen. Des Weiteren werden sie in Compilern zum Typechecking und für Optimierungen verwendet.

DIeser Kurs gibt einen Überblick über die zugrundeliegende Konzepte von statischen Analysen. Insbesondere diskutieren wir den Kompromiss zwischen der Performanz, der Präzision, und der Korrektheit von statischen Analysen. Des Weiteren werden Ihnen verschieden Sorten von statischen Analysen vorgestellt, wie zum Beispiel Kontrollflussanalysen, Datenflussanalysen, Zeigeranalysen, sowie Seiteneffekt- und Unveränderlichkeitsanalysen. Abschließend lernen sie verschiedene Analyseframeworks kennen, wie das monotone Framework, Big-Step Abstrakte Interpreter und IFDS/IDE Frameworks.

In der begleitenden Übung wenden Sie die neuen Analysekonzepte praktisch an, und erweitern oder entwickeln existierende Analysen.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Das Ziel dieses Kurses ist es die zugrundeliegenden Konzepte von statischen Analysen zu vermitteln. Dies erlaubt es Studierenden statische Analysen in IDEs effektiver zu verwenden. Des Weiteren sind Studierende nach dem Kurs in der Lage Eigenschaften von statischen Analysen wie Performanz und Präzision zu beurteilen</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Wir erwarten, dass Studierende die Konzepte der Programmiersprachen, wie Zuweisungen, Schleifen, Ausnahmebehandlung, Objekte, und anonyme Funktionen gut verstanden haben. Des Weiteren sollten die Kursteilnehmer*innen mit grundlegender Universitätsmathematik und Logik vertraut sein.</td></tr>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1122-vl] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%).
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1122-vl] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Software-Engineering - Wartung und Qualitätssicherung					
Modul Nr. 18-su-2010	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch			**Modulverantwortliche Person** Prof. Dr. rer. nat. Andreas Schürr		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
18-su-2010-ue	Software-Engineering - Wartung und Qualitätssicherung	0	Übung	1
18-su-2010-vl	Software-Engineering - Wartung und Qualitätssicherung	0	Vorlesung	3

2 Lerninhalt

Die Lehrveranstaltung vertieft Teilthemen der Softwaretechnik, welche sich mit der Pflege und Weiterentwicklung und Qualitätssicherung von Software beschäftigen. Dabei werden diejenigen Hauptthemen des IEEE "Guide to the Software Engineering Body of Knowledge" vertieft, die in einführenden Softwaretechnik-Lehrveranstaltungen nur kurz angesprochen werden. Das Schwergewicht wird dabei auf folgende Punkte gelegt: Softwarewartung und Reengineering, Konfigurationsmanagement, statische Programmanalysen und Metriken sowie vor allem dynamische Programmanalysen und Laufzeittests. In den Übungen werden die in der Vorlesung vorgestellten Analysetechniken und Methoden zur Weiterentwicklung und Qualitätssicherung von Software an Hand von verschiedenen Beispielen untersucht und vertieft.
In der Lehrveranstaltung wird zudem großer Wert auf die Einübung praktischer Fertigkeiten in der Auswahl und im Einsatz von Softwareentwicklungs- Wartungs- und Testwerkzeugen verschiedenster Arten gelegt.

3 Qualifikationsziele / Lernergebnisse

Das Modul vermittelt den Studierenden nach erfolgreichem Abschluss anhand praktischer Beispiele grundlegende Software-Wartungs- und Qualitätssicherungs-Techniken, also eine ingenieurmäßige Vorgehensweise zur zielgerichteten Wartung und Evolution von Softwaresystemen. Die Studierenden sind in der Lage, die im Rahmen der Softwarewartung und -pflege eines größeren Systems anfallenden Tätigkeiten durchzuführen. Dies gilt insbesondere auch für Techniken zur Verwaltung von Softwareversionen und -konfigurationen sowie auf das systematische Testen von Software.

4	**Voraussetzung für die Teilnahme** Grundlagen der Softwaretechnik sowie gute Kenntnisse objektorientierter Programmiersprachen (insbesondere Java).
5	**Prüfungsform** Modulabschlussprüfung: • Modulprüfung (Fachprüfung, Klausur, Dauer 90 Min, Standard)
6	**Voraussetzung für die Vergabe von Leistungspunkten**
7	**Benotung** Modulabschlussprüfung: • Modulprüfung (Fachprüfung, Klausur, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** MSc ETiT, MSc iST, MSc Wi-ETiT, Informatik
9	**Literatur** https://www.es.tu-darmstadt.de/lehre/aktuelle-veranstaltungen/se-ii-v und Moodle
10	**Kommentar**

Modulhandbuch
M. Sc. IT Security

Wahlbereich Complementary Topics

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Graphische Datenverarbeitung I</td></tr>
<tr><td>Modul Nr.
20-00-0040</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0040-iv</td><td>Graphische Datenverarbeitung I</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Einführung in die Grundlagen der Computergraphik, insb. Ein- u. Ausgabegeräte, Rendering Pipeline am Beispiel von OpenGL, räumliche Datenstrukturen, Beleuchtungsmodelle, Ray Tracing, aktuelle Entwicklungen in der Computergraphik</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreichem Besuch dieser Veranstaltung sind Studierende in der Lage alle Komponenten der Graphikpipeline zu verstehen und dadurch variable Bestandteile (Vertex-Shader, Fragment-Shader, etc.) anzupassen. Sie können Objekte im 3D-Raum anordnen, verändern und effektiv speichern, sowie die Kamera und die Perspektive entsprechend wählen und verschiedene Shading-Techniken und Beleuchtungsmodelle nutzen, um alle Schritte auf dem Weg zum dargestellten 2D-Bild anzupassen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:
● Programmierkenntnisse
● Kentnisse über grundlegende Algorithmen und Datenstrukturen
● Kenntnisse im Bereich Lineare Algebra
● Kenntnisse im Bereich Analysis
● Inhalte der Vorlesung „Visual Computing“ oder einer vergleichbaren Veranstaltung</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0040-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0040-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** ● Real-Time Rendering: Tomas Akenine-Möller, Eric Haines, Naty Hoffman A.K. Peters Ltd., 3rd edition, ISBN 987-1-56881-424-7 ● Fundamentals of Computer Graphics: Peter Shirley, Steve Marschner, third edition, ISBN 979-1-56881-469-8 ● Weitere aktuelle Literaturhinweise werden in der Veranstaltung gegeben.
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Graphische Datenverarbeitung II</td></tr>
<tr><td>Modul Nr.
20-00-0041</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0041-iv</td><td>Graphische Datenverarbeitung II</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Grundlagen der verschiedenen Objekt- und Oberflächen-Repräsentationen in der graphischen Datenverarbeitung. Kurven und Oberflächen (Polynome, Splines, RBF) Interpolation und Approximation, Displaytechniken, Algorithmen: de Casteljau, de Boor, Oslo, etc. Volumen und implizite Oberflächen. Visualisierungstechniken, Iso-Surfaces, MLS, Oberflächen-Rendering, Marching-Cubes. Polygonnetze. Netz Kompression , Netz-Vereinfachung, Multiskalen Darstellung, Subdivision. Punktwolken: Renderingtechniken, Oberflächen-Rekonstruktion, Voronoi-Diagramme und Delaunay-Triangulierung.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreichem Besuch dieser Veranstaltung sind Studierende in der Lage mit diversen Objekt- und Oberflächen-Repräsentationen umzugehen, das heißt diese zu verwenden, anzupassen, anzuzeigen (rendern) und effektiv zu speichern. Dazu gehören mathematisch polynomiale Repräsentationen, Iso-oberflächen, volumen Darstellungen, implizite Oberflächen, Polygonnetze, Subdivision-Kontrollnetze und Punktwolken.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Der vorherige Besuch von „Algorithmen und Datenstrukturen“ und „Graphische Datenverarbeitung I“ oder vergleichbaren Veranstaltungen

Kenntnisse über Grundlagen aus der Höheren Mathematik

Programmierkenntnisse in C / C++</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0041-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0041-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** ● Real-Time Rendering: Tomas Akenine-Möller, Eric Haines, Naty Hoffman A.K. Peters Ltd., 3rd edition, ISBN 987-1-56881-424-7 ● Weitere aktuelle Literaturhinweise werden in der Veranstaltung gegeben.
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
Data Mining und Maschinelles Lernen</td></tr>
<tr><td>Modul Nr.
20-00-0052</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="5">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0052-iv</td><td>Data Mining und Maschinelles Lernen</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
Durch die rasante Entwicklung der Informationstechnologie sind immer größere Datenmengen verfügbar. Diese enthalten oft implizites Wissen, das, wenn es bekannt wäre, große wirtschaftliche oder wissenschaftliche Bedeutung hätte. Data Mining ist ein Forschungsgebiet, das sich mit der Suche nach potentiell nützlichem Wissen in großen Datenmengen beschäftigt, und Maschinelles Lernverfahren gehören zu den Schlüsseltechnologien innerhalb dieses Gebiets.
Die Vorlesung bietet eine Einführung in das Gebiet des Maschinellen Lernens unter dem besonderen Aspekt des Data Minings. Es werden Verfahren aus verschiedenen Paradigmen des Maschinellen Lernens mit exemplarischen Anwendungen vorgestellt. Um das Wissen zu operationalisieren, werden in den Übungen prak-tisch-e Erfahrungen mit Lernalgorithmen gesammelt.
● Einführung (Grundbegriffe, Lernprobleme, Konzepte, Beispiele, Repräsentation)
● Regel-Lernen
○ Lernen einzelner Regeln (Generalisierung und Spezialisierung, Strukturierte Hypothesenräume, Version Spaces)
○ Lernen von Regel-Mengen (Covering Strategie, Evaluierungsmaße für Regeln, Pruning, Mehr-Klassenprobleme)
● Evaluierung und kosten-sensitives Lernen (Accuracy,X-Val,ROC-Kurven,Cost-Sensitive Learning)
● Instanzenbasiertes Lernen (kNN,IBL,NEAR,RISE)
● Entscheidungsbaum-Lernen (ID3, C4.5, etc.)
● Ensemble-Methoden (Bias/Variance, Bagging, Randomization, Boosting, Stacking, ECOCs)
● Pre-Processing (Feature Subset Selection, Diskretisierung, Sampling, Data Cleaning)
● Clustering und Lernen von Assoziationsregeln (Apriori)</td></tr>
</table>

3	**Qualifikationsziele / Lernergebnisse** Nach der erfolgreichen Absolvierung dieser Lehrveranstaltung sind die Studierenden in der Lage ● grundlegende Techniken des Data Mining und Maschinellen Lernens zu verstehen und erklären ● praktische Data Mining Systeme selbständig einsetzen und deren Stärken und Schwächen verstehen ● neue Entwicklungen auf diesem Gebiet kritisch beurteilen
4	**Voraussetzung für die Teilnahme**
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0052-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0052-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.

9	**Literatur** ● Mitchell: Machine Learning, McGraw-Hill, 1997 ● Ian H. Witten and Eibe Frank: Data Mining: Practical Machine Learning Tools and Techniques with Java Implementations, Morgan-Kaufmann, 1999
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Computer Vision</td></tr>
<tr><td>Modul Nr.
20-00-0157</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0157-iv</td><td>Computer Vision</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
● Grundlagen der Bildformierung
● Lineare und (einfache) nichtlineare Bildfilterung
● Grundlagen der Mehransichten-Geometrie
● Kamerakalibrierung & -posenschätzung
● Grundlagen der 3D-Rekonstruktion
● Grundlagen der Bewegungsschätzung aus Videos
● Template- und Unterraum-Ansätze zur Objekterkennung
● Objektklassifikation mit Bag of Words
● Objektdetektion
● Grundlagen der Bildsegmentierung</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende beherrschen nach erfolgreichem Besuch der Veranstaltung die Grundlagen der Computer Vision. Sie verstehen grundlegende Techniken der Bild- und Videoanalyse, und können deren Annahmen und mathematische Formulierungen benennen, sowie die sich ergebenden Algorithmen beschreiben. Sie sind in der Lage diese Techniken praktisch so umzusetzen, dass sie grundlegende Bildanalyseaufgaben an Hand realistischer Bilddaten lösen können.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Der vorherige Besuch von „Visual Computing“ oder einer vergleichbaren Veranstaltung</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0157-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0157-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Literaturempfehlungen werden regelmässig aktualisiert und beinhalten beispielsweise: ● R. Szeliski, "Computer Vision: Algorithms and Applications", Springer 2011 ● D. Forsyth, J. Ponce, "Computer Vision -- A Modern Approach", Prentice Hall, 2002
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
Virtuelle und Erweiterte Realität</td></tr>
<tr><td>Modul Nr.
20-00-0160</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="5">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0160-iv</td><td>Virtuelle und Erweiterte Realität</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
Im Rahmen dieser Lehrveranstaltung werden zuerst die Grundlagen, Begriffsbildungen und Referenzmodelle zur Einordnung der Thematik im Rahmen der Computer-Graphik/Computer-Vision aufgezeigt. Aufbauend darauf werden die besonderen Technologien, Algorithmen und Standards der Augmented Reality (AR) und der Virtual Reality (VR) behandelt. Dazu gehören:
● Datenschnittstellen (Standards, Vorverarbeitung, Systeme, etc.)
● Interaktionstechniken (z.B. Interaktion mit Hilfe von Rangekameras)
● Darstellungsverfahren (z.B. Echtzeit-Rendering)
● Web-basierte VR/AR
● Computer-Vision-basiertes Tracking für Augmented-Reality
● Augmented Reality mit Rangekamera-Technologien
● Augmented Reality auf Smartphonesystemen
Schließlich werden diese Techniken an Beispielen aktueller Forschungsarbeiten aus den Bereichen „AR/VR-Wartungsunterstützung“ und „AR/VR-gestützte Präsentation von Kulturgütern“ dokumentiert.</td></tr>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Studierende kennen nach erfolgreichem Besuch der Veranstaltung die Anforderungen und Problematiken von Virtual/Augmented Reality und sie wissen, für welche Problemstellungen diese Technologien eingesetzt werden können. Sie kennen die Standards, mit deren Hilfe VR/AR-Anwendungen spezifiziert werden, insb. wissen die Studierenden, welche Computer-Vision-Technologien eingesetzt werden können, um in verschiedenen Umgebungen die Kamerapose stabil zu tracken.</td></tr>
<tr><td>4</td><td colspan="5">Voraussetzung für die Teilnahme
Empfohlen: Grundlagen der Graphischen Datenverarbeitung (GDV)</td></tr>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0160-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0160-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M.Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Dörner, R., Broll, W., Grimm, P., Jung, B. Virtual und Augmented Reality (VR / AR)
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
Informationsvisualisierung und Visual Analytics</td></tr>
<tr><td>Modul Nr.
20-00-0294</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="5">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0294-iv</td><td>Informationsvisualisierung und Visual Analytics</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
Diese Vorlesung wird eine detaillierte Einführung in die Informationsvisualisierung geben, um sich dann intensiv den wissenschaftlichen Fragestellungen und praxisnahen Anwendungsszenarien von Visual Analytics zu widmen.
•Überblick der Informationsvisualisierung und Visual Analytics (Definitionen, Modelle, Historie)
•Datenpräsentierung und Datentransformation
•Abbildung von Daten auf visuelle Strukturen
• Visuelle Repräsentierungen und Interaktion fuer bivariate, multivariate Daten, Zeitreihen, Graphen und Geographische Daten
• Grundlagen von Data Mining
•Grundlagen von Visual Analytics: - Analytische Beweisführung - Data Mining
• Evaluation von Visual Analytics Systemen

Anwendungsgebiete: Medizin, Biologie, Finanzen und Wirtschaft, Meteorologie, Rettungsdienst,....</td></tr>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Studierende können nach erfolgreichem Besuch der Veranstaltung

•Informationsvisualisierungsmethoden für verschiedene Datentypen benutzen

•interactive Visualisierungsysteme für Daten aus verschiedenen Anwendungsgebieten designen

•Visualisierung und automatische Datenverarbeitung kombinieren um Big Data Probleme zu lösen</td></tr>
</table>

	•Wissen über Hauptcharakteristika menschlicher visuellen Wahrnehmung in Informationsvisualisierung und Visual Analytics anwenden •geeignete Evaluationsmethode für spezifische Situationen und Szenarien auswählen
4	**Voraussetzung für die Teilnahme** Empfohlen: Interesse an Methoden der Computergrafik und Visualisierung
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0294-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0294-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M.Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Wird in der Vorlesung bekanntgegeben. Beispiele für verwendete Literatur könnten sein: C. Ware: Information Visualization: Perception for Design Ellis et al: Mastering the Information Age
10	**Kommentar**

Modulbeschreibung

Modulname Statistisches Maschinelles Lernen						
Modul Nr. 20-00-0358	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0358-iv	Statistisches Maschinelles Lernen	6	integrierte Veranstaltung	4

2 Lerninhalt

- Statistische Methodik für das Maschinelle Lernen
- Auffrischung zu Statistik, Optimierung und Linearer Algebra
- Bayes'sche Entscheidungstheorie
- Wahrscheinlichkeitsdichtenschätzung
- Nichtparametrische Modelle
- Mixtur Modelle und der EM-Algorithmus
- Lineare Modele zur Klassifikation und Regression
- Statistische Lerntheorie
- Kernel Methoden zur Klassification und Regression

3 Qualifikationsziele / Lernergebnisse

Die Lehrveranstaltung ist eine systematische Einführung in die Grundlagen und Methodik des statistischen maschinellen Lernens. Nach erfolgreichen Abschluss der Lehrveranstaltung, verstehen Studierende die wichtigsten Methoden und Ansätze des Statischen Maschinellen Lernens. Sie können maschinelle Lernverfahren anwenden, um eine Vielzahl neuer Probleme zu lösen.

4 Voraussetzung für die Teilnahme

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-0358-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

	Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0358-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** 1. C.M. Bishop, Pattern Recognition and Machine Learning (2006), Springer 2. K.P. Murphy, Machine Learning: a Probabilistic Perspective (expected 2012), MIT Press 3. D. Barber, Bayesian Reasoning and Machine Learning (2012), Cambridge University Press 4. T. Hastie, R. Tibshirani, and J. Friedman (2003), The Elements of Statistical Learning, Springer Verlag 5. D. MacKay, Information Theory, Inference, and Learning Algorithms (2003), Cambridge University Press 6. R.O. Duda, P.E. Hart, and D.G. Stork, Pattern Classification (2nd ed. 2001), Willey-Interscience 7. T.M. Mitchell, Machine Learning (1997), McGraw-Hill
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Ambient Intelligence</td></tr>
<tr><td>Modul Nr.
20-00-0390</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0390-iv</td><td>Ambient Intelligence</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Vorlesung führt in aktuelle Entwicklungen von Ambient Intelligence ein. Im Vordergrund der Vorlesung steht die Mensch-Maschine-Interaktion (MMI) in intelligenten Umgebungen in einem allgegenwärtigen Informationsraum, wie sie beispielsweise zunehmend durch eingebettete Systeme in alltägliche Gebrauchsobjekte gegeben ist. Spezieller Fokus wird auf den mobilen Aspekt eines allgegenwärtigen Informationszugriffs und der Informationsaufbereitung und -darstellung in mobilen Endgeräten gelegt. Dabei soll einerseits ein Einblick in die grundlegenden Technologien, Anwendungen und Experimente gegeben werden und anderseits (nicht im Schwerpunkt) auch die sozio-kulturellen Implikationen und Aspekte neuer Ambient Intelligence Lösungen diskutiert werden. Zusätzliche Themen der Vorlesung sind System-Architekturen für verteilte Umgebungen, Kontext-Awareness und Kontext-Management, Benutzermodelle und deren Implikationen, Sensornetzwerke und Interaktionstechniken. Die Vorlesung wird Beispiele aktueller Projekte diskutieren und die internationalen Forschungslinien von Ambient Intelligence beleuchten.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nachdem Studierende die Veranstaltung erfolgreich besucht haben, können sie Technologietrends und Forschungserkenntnisse im Bereich Ambient Intelligence beschreiben. Die wichtigsten Konzepte zur Realisierung „intelligenter Umgebungen“ - intelligente Netzwerke und Objekte, Techniken der erweiterten, mobilen Realität, ubiquitäre und allgegenwärtige Informationsräume, nomadische Kommunikationen, Echt-Zeit-Kommunikation und relevante Middleware, Eingebettete Systeme, Sensor Netzwerke und Wearable Computing - können diskutiert und eingeordnet werden. Nach Abschluss der zugehörigen Übung können Studierende die Projektphasen der Entwicklung einer Ambient-Intelligence Anwendung eigenständig planen und realisieren.</td></tr>
</table>

4	**Voraussetzung für die Teilnahme** Empfohlen: Der vorherige Besuch von “Visual Computing“ und „Multimodale Interaktion mit intelligenten Umgebungen“ oder vergleichbarer Veranstaltungen
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0390-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0390-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Wird jeweils passend zu den aktuellen Themen bekanntgegeben
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Computer Vision II</td></tr>
<tr><td>Modul Nr.
20-00-0401</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0401-iv</td><td>Computer Vision II</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
● Computer Vision als (probabilistische) Inferenz
● Robuste Schätzung und Modellierung
● Grundlagen der Bayes’schen Netze und Markov’schen Zufallsfelder
● Grundlegende Inferenz- und Lernverfahren der Computer Vision
● Bildrestaurierung
● Stereo
● Optischer Fluß
● Bayes’sches Tracking von (artikulierten) Objekten
● Semantische Segmentierung
● Aktuelle Themen der Forschung</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende haben nach erfolgreichem Besuch der Veranstaltung ein vertieftes Verständnis der Computer Vision. Sie formulieren Fragestellungen der Bild- und Videoanalyse als Inferenzprobleme und berücksichtigen dabei Herausforderungen reeller Anwendungen, z.B. im Sinne der Robustheit. Sie lösen das Inferenzproblem mittels diskreter oder kontinuierlicher Inferenzalgorithmen, und wenden diese auf realistische Bilddaten an. Sie evaluieren die anwendungsspezifischen Ergebnisse quantitativ.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Der vorherige Besuch von „Visual Computing“ und „Computer Vision I“ oder vergleichbaren Veranstaltungen ist empfohlen.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0401-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0401-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Literaturempfehlungen werden regelmässig aktualisiert und beinhalten beispielsweise: ● S. Prince, “Computer Vision: Models, Learning, and Inference”, Cambridge University Press, 2012 ● R. Szeliski, "Computer Vision: Algorithms and Applications", Springer 2011
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Programmierung Massiv-Paralleler Prozessoren</td></tr>
<tr><td>Modul Nr.
20-00-0419</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0419-iv</td><td>Programmierung Massiv-Paralleler Prozessoren</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
- Grundlagen massiv-paralleler Hardware mit einem Schwerpunkt auf modernen Beschleunigern
- parallele Algorithmen
- effiziente Programmierung massiv-paralleler Systeme
- praktische Programmierprojekte mit Co-Betreuung durch einen Wissenschaftler au seiner Anwendungsdomain</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach dem erfolgreichen Besuch der Veranstaltung sind Studierende dazu in der Lage, Problemstellungen im Kontext massiv-paralleler Systeme zu analysieren. Sie können selbständig neue Anwendungen entwickeln und ihre Performanz systematisch verbessern. Sie verstehen grundlegende parallele Algorithmen und Programmierparadigmen und können sich selbständig aktuelle Literatur erarbeiten.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:
solide Programmierkenntnisse in C/C++
Kentnisse in paralleler Programmierung</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0419-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.</td></tr>
</table>

	Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0419-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** wird in der Veranstaltung bekanntgegeben
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Natural Language Processing and the Web</td></tr>
<tr><td>Modul Nr.
20-00-0433</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0433-iv</td><td>Natural Language Processing and the Web</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Das Web beinhaltet mehr als 10 Milliarden indexierbare Webseiten, die mittels Stichwortsuche zugänglich sind. Die Vorlesung behandelt Methoden der automatischen Sprachverarbeitung bzw. des Natural Language Processing (NLP) zur Verarbeitung großer Mengen unstrukturierter Texte im Web und zur Analyse von Online-Inhalten als wertvolle Ressource für andere sprachtechnologische Anwendungen im Web.

Zentrale Inhalte:
● Verarbeitung unstrukturierter Texte im Web
○ NLP-Grundlagen: Tokenisierung, Wortartenerkennung, Stemming, Lemmatisierung, Chunking
○ UIMA: Grundlagen und Anwendungen
○ Web-Inhalte und ihre Charakteristika, u.a. verschiedene Genres, z.B. persönliche Seiten, Nachrichtenportale, Blogs, Foren, Wikis
○ Das Web als Korpus, insb. innovative Verwendung des Webs als sehr großes, verteiltes, verlinktes, wachsendes und multilinguales Korpus
● NLP-Anwendungen für das Web
○ Einführung in das Information Retrieval
○ Web-Suche und natürlichsprachliche Suchschnittstellen
○ Web-basierte Beantwortung von natürlichsprachlichen Fragen
○ Web-Mining im Web 2.0, z.B. Wikipedia, Wiktionary
○ Qualitätsbewertung von Web-Inhalten
○ Multilingualität
○ Internet-of-Services: Service Retrieval
○ Sentimentanalyse und Community Mining
○ Paraphrasen, Synonyme, semantische Verwandtschaft und das Web</td></tr>
</table>

3	**Qualifikationsziele / Lernergebnisse** Nachdem Studierende die Veranstaltung besucht haben, können sie ● Methoden und Ansätze zur Verarbeitung unstrukturierter Texte verstehen und differenzieren, ● die Arbeitsweise von Web-Suchmaschinen nachvollziehen und erläutern, ● exemplarische Anwendungen der Sprachverarbeitung im Web selbständig aufbauen und analysieren, ● das Potenzial von Web-Inhalten für die Verbesserung von sprachtechnologischen Anwendungen analysieren und einschätzen.
4	**Voraussetzung für die Teilnahme** Empfohlen: Grundlegende Kenntnisse über Algorithmen und Datenstrukturen sowie Programmierkenntnisse in Java werden erwartet
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0433-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0433-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security

	Kann in anderen Studiengängen verwendet werden.

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Medizinische Visualisierung</td></tr>
<tr><td>Modul Nr.
20-00-0467</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0467-iv</td><td>Medizinische Visualisierung</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Medizinische Bilddaten; Bildaufbereitung; Medizinische Visualisierung mit VTK; Indirekte Volumenvisualisierung; Direkte Volumenvisualisierung; Transfer-Funktionen; Interaktive Volumenvisualisierung; Illustratives Rendering; Beispiel: Visualisierung von Tensor-Bilddaten; Beispiel: Visualisierung von Baumstrukturen; Beispiel: Virtuelle Endoskopie; Beispiel: Bildgestützte Chirurgie</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende kennen nach erfolgreichem Besuch der Veranstaltung Techniken der Volumenvisualisierung. Sie verstehen die Notwendigkeit der Bildverbesserung für die Visualisierung. Sie können das "Visualization Toolkit“ (VTK) anwenden, um mit dessen Hilfe Anwendungen für die Visualisierung von medizinischen Bilddaten für Diagnose, Planung und Therapie zu erstellen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: GDV I, (Medizinische) Bildverarbeitung</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
[20-00-0467-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Leistungspunkten
Bestehen der Prüfung (100%)</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0467-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Preim, Botha: Visual Computing for Medicine
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
Capturing Reality</td></tr>
<tr><td>Modul Nr.
20-00-0489</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="5">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0489-iv</td><td>Capturing Reality</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
Dieser Kurs deckt ein breites Spektrum von Techniken zur Digitalisierung und Modellierung unserer Welt mit einem Fokus auf Anwendungen in der Computergraphik und Computer Vision ab. Dies beinhaltet insbesondere:
- grundlegende Werkzeuge und Kalibrationstechniken für die Digitalisierung
- Digitalisierungs- und Modellierungstechniken für verschiedenste Objekt- und Szeneneigenschaften (z.B. Geometrie, Reflexionseigenschaften)
- grundlegende mathematische Modellierungs- und Optimierunstechniken
- Implementierung und praktische Anwendung einer Reihe von Techniken</td></tr>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Nach dem erfolgreichen Besuch der Veranstaltung sind Studierende dazu in der Lage, Digitalisierungs- und Modellierungsprobleme für Objekte und Szenen in Computergraphik und Computer Vision sowie die zugrunde liegenden Techniken zu analysieren. Sie können selbständig neue Versuchsaufbauten entwickeln, Experimente durchführen und die Ergebnisse auswerten.</td></tr>
<tr><td>4</td><td colspan="5">Voraussetzung für die Teilnahme
Empfohlen: Der vorherige Besuch der Veranstaltungen „Graphische Datenverarbeitung I“ oder „Computer Vision I“ oder vergleichbaren Veranstaltungen sowie grundlegende Programmierkenntnisse in C/C++</td></tr>
<tr><td>5</td><td colspan="5">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0489-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.</td></tr>
</table>

	Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0489-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Noriko Kurachi: The Magic of Computer Graphics. A K Peters/CRC Press Richard Szeliski: Algorithms and Applications, Springer Marcus Magnor, Oliver Grau, Olga Sorkine-Hornung, Christian Theobalt: Digital Representations of the Real World: How to Capture, Model, and Render Visual Reality Wolfgang Förstner, Bernhard P. Wrobel: Photogrammetric Computer Vision - Geometry, Orientation and Reconstruction
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
TK2: Human Computer Interaction</td></tr>
<tr><td>Modul Nr.
20-00-0535</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="5">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0535-vl</td><td>TK2: Human Computer Interaction</td><td>3</td><td>integrierte Veranstaltung</td><td>2</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
Die Vorlesung stellt verschiedene grundlegende Konzepte, Modelle und Theorien aus dem Bereich der Human Computer Interaction (HCI) vor. Die Veranstaltung umfasst die folgenden Inhalte:
• Theoretische Grundlagen aus Psychologie und Interaktionsgestaltung als Basis für die Gestaltung von Nutzerschnittstellen
• Überblick über verschiedene Typen von Nutzerschnittstellen
• Command-line interfaces
• Grafische Nutzerschnittstellen, u.a. Mac OS und Windows
• Interaktive Oberflächen, u.a. Tabletops, Multitouch
• Mobile user interfaces, u.a. basierend auf iPhone OS, Android
• Pen-based user interfaces, u.a. elektronische Stifte
• Tangible user interfaces, Organic user interfaces
• Sprachbasierte user interfaces
• Beurteilung, Messung, Bewertung von Nutzerschnittstellen
• Nutzerstudien
• Quantitative Evaluationsmethoden
• Qualitative Evaluationsmethoden
• Nutzerzentrierte Softwareentwicklung</td></tr>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Nach der Teilnahme an dieser Lehrveranstaltung haben Studierende

● Verständnis der psychologischen Grundlagen des Designs von Benutzerschnittstellen erworben

● Methoden des user-centric design process kennengelernt

● Überblickswissen über die gängigen UI Konzepte erworben</td></tr>
</table>

	● Evaluationstechniken kennen gelernt und angewandt
4	**Voraussetzung für die Teilnahme**
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0535-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0535-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Literaturempfehlungen werden kontinuierlich aktualisiert, Beispiele für verwendete Literatur könnten sein: Ausgewählte Kapitel aus den folgenden Standardwerken: • Donald Norman: The Design of Everyday Things • Alan Dix, Janet Finlay, Gregory Abowd and Russel Beale: Human-Computer Interaction • Jenny Preece , Yvonne Rogers and Helen Sharp: Interaction Design: Beyond Human-Computer Interaction
10	**Kommentar**

Modulbeschreibung

Modulname Lernende Roboter						
Modul Nr. 20-00-0629	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0629-vl	Lernende Roboter	6	integrierte Veranstaltung	4

2 Lerninhalt

- Grundlagen aus der Robotik und des Maschinellen Lernens für Lernende Roboter
- Maschinellen Lernen von Modellen
- Representation einer Policy. Hierarchische Abstraktion mit Bewegungsprimitiven
- Imitationslernen
- Optimale Steuerung mit gelernten Modellen
- Reinforcement Learning und Policy Search-Verfahren
- Inverses Reinforcement Learning

3 Qualifikationsziele / Lernergebnisse

Nach erfolgreichen Abschluss der Lehrveranstaltung verstehen Studierende die Grundlagen des Maschinellen Lernens und der Robotik. Sie können maschinelle Lernverfahren anwenden um einen Roboter zu befähigen, neue Aufgaben zu erlernen. Studierende verstehen die Grundlagen von Reinforcement Learning und können verschiedene Algorithmen anwenden um eine Policy des Roboters aufgrund von Interaktion mit der Umgebung zu erlernen. Sie verstehen den Unterschied zwischen Imitation Learning, Reinforcement Learning, Policy Search und Inverse Reinforcement Learning und können einschätzen, wann sie welchen Ansatz verwenden sollen. Sie können diese Ansätze auch problemlos auf geeignete Aufgabenstellungen anwenden.

4 Voraussetzung für die Teilnahme

Empfohlen: Gute Programmierkenntnisse in Matlab und der vorherige Besuch von „Statistisches Maschinelles Lernen“ oder einer vergleichbaren Veranstaltung sind hilfreich aber nicht zwingend erforderlich

5 Prüfungsform

	Bausteinbegleitende Prüfung: • [20-00-0629-vl] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0629-vl] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Deisenroth, M. P.; Neumann, G.; Peters, J. (2013). A Survey on Policy Search for Robotics, Foundations and Trends in Robotics Kober, J; Bagnell, D.; Peters, J. (2013). Reinforcement Learning in Robotics: A Survey, International Journal of Robotics Research C.M. Bishop, Pattern Recognition and Machine Learning (2006), R. Sutton, A. Barto. Reinforcement Learning - an Introduction Nguyen-Tuong, D.; Peters, J. (2011). Model Learning in Robotics: a Survey
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Fortgeschrittener Compilerbau</td></tr>
<tr><td>Modul Nr.
20-00-0701</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
150 h</td><td>Selbststudium
105 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0701-vl</td><td>Fortgeschrittener Compilerbau</td><td>6</td><td>integrierte Veranstaltung</td><td>3</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
- Compilierung und Laufzeitumgebung für objektorientierte Programmiersprachen
- Kontrollflussgraphen als Zwischendarstellung
- Statische Datenflußanalyse
- Static Single Assignment Form
- Eliminierung totaler und partieller Redundanz
- Skalare Optimierung
- Registerallokation
- Ablaufplanung
- Schleifenoptimerung
- Aufbau realer Compiler (z.B. Phasen, Zwischendarstellung, Compilefluß)</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende verstehen nach erfolgreichem Besuch Techniken für die Übersetzung und Ausführung von objektorientierten Programmen auf Maschinenebene. Sie können die statische Datenflussanalyse auf Kontrollflussgraphen anwenden und sind geübt im praktischen Umgang mit deren SSA-Darstellung. Sie beherrschen Optimierungsverfahren für eine Reihe von Aufgaben sowie fundamentale Verfahren für die Registerallokation. Sie kennen die interne Struktur von realen Compilern für den Produktivbetrieb.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Erfolgreicher Besuch der Veranstaltung “Einführung in den Compilerbau” oder vergleichbarer Veranstaltungen</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0701-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0701-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Literaturempfehlungen werden kontinuierlich aktualisiert, Beispiele für verwendete Literatur könnten sein: Cooper/Torczon: Engineering a Compiler Muchnick: Advanced Compiler Design and Implementation Aho/Lam/Sethi/Ullman: Compilers - Principles, Techniques, and Tools
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Mobile Netze</td></tr>
<tr><td>Modul Nr.
20-00-0748</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0748-iv</td><td>Mobile Netze</td><td>6</td><td>integrierte Veranstaltung</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Mobilkommunikation und drahtlose Kommunikationstechniken haben sich in den letzten Jahren rapide weiterentwickelt. Die integrierte Veranstaltung erläutert Charakteristiken und Grundprinzipien mobiler Netze, und praktische Lösungsansätze werden vorgestellt. Der Fokus der Veranstaltung liegt hierbei auf der Vermittlungsschicht (Netzwerkschicht). Zusätzlich zum Stand der Technik werden in der Veranstaltung aktuelle Forschungsfragen diskutiert und Methoden und Werkzeuge zur systematischen Behandlung dieser Fragen erläutert. Die Inhalte werden in Übungseinheiten vertieft.
Lerninhalte:
- Einleitung: Drahtlose und mobile Kommunikation: Anwendungen, Geschichte, Marktchancen
- Überblick über drahtlose Kommunikation: Drahtlose Übertragung, Frequenzen und Frequenzregulierung, Signale, Antennen, Signalausbreitung, Multiplex, Modulation, Spreizband-Technik, Zellulare Systeme
- Medienzugriff: SDMA, FDMA, CDMA, TDMA (Feste Zuordnung, Aloha, CSMA, DAMA, PRMA, MACA, Kollisionsvermeidung, Polling)
- Drahtlose Lokale Netze (Wireless LAN): IEEE 802.11 Standard inklusive Bitübertragungsschicht, Sicherungsschicht und Zugriffverfahren, Dienstgüte, Energieverwaltung
- Drahtlose Stadtnetze, drahtlose Mesh Netze, IEEE 802.16 Standard inklusive Betriebsmodi, Medienzugriff, Dienstgüte, Ablaufkoordination
- Mobilität auf der Netzwerkschicht: Konzepte zur Mobilitätsunterstützung, Mobile IP
- Ad hoc Netze: Terminologie, Grundlagen und Applikationen, Charakteristika von Ad hoc Kommunikation, Ad hoc Routing Paradigmen und Protokolle
- Leistungsbewertung von mobilen Netzen: Einführung in die Leistungsbewertung, systematischer Ansatz/häufige Fehler und wie man sie vermeiden kann, experimentelles Design und Analyse
- Mobilität auf der Transportschicht: Varianten von TCP (Indirect TCP, Snoop TCP, Mobile TCP, Wireless TCP)
- Mobilität auf der Anwendungsschicht: Anwendungen für mobile Netze und drahtlose Sensornetze</td></tr>
</table>

3	**Qualifikationsziele / Lernergebnisse** Nach erfolgreicher Teilnahme an der Veranstaltung haben Studierende ein umfassendes Wissen der Funktionsweise mobiler Kommunikationsnetze. Sie können die wichtigsten Grundlagen drahtloser Kommunikationstechniken erläutern. Die Studierenden können weiterhin Medienzugriffsverfahren kategorisieren und die Funktionsweise dieser Verfahren im Detail erklären. Insbesondere weisen sie ein tiefgehendes Verständnis von Verfahren auf Vermittlungsschicht und Transportschicht auf, mit Schwerpunktsetzung auf Ad hoc und Mesh Netze. Die Studierenden erlangen Wissen über die Zusammenhänge zwischen unterschiedlichen Protokollschichten und können ihr erworbenes Wissen auf die methodische Analyse von realen Kommunikationssystemen anwenden. Sie sind somit in der Lage, die Charakteristiken und Grundprinzipien des Problemraumes drahtloser und mobiler Kommunikation detailliert zu erläutern und weisen auf diesem Feld ein fundiertes Wissen in Praxis und Theorie auf. Die Übungsteile der integrierten Veranstaltung vertiefen das theoretische Wissen durch Literatur-, Rechen- und praktische Implementierungs-/Anwendungsübungen.
4	**Voraussetzung für die Teilnahme** Empfohlen: Grundlagen der Kommunikationsnetze
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0748-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0748-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard) In dieser Veranstaltung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 6. Novelle der Allgemeinen Prüfungsbestimmungen der TU Darmstadt und den vom Fachbereich Informatik am 14.07.2022 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. IT Security

	Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Ausgewählte Buchkapitel und ausgewählte wissenschaftliche Veröffentlichungen
10	**Kommentar**

Modulbeschreibung

Modulname Multithreading in C++						
Modul Nr. 20-00-0953	**Leistungspunkte** 10 CP	**Arbeitsaufwand** 300 h	**Selbststudium** 210 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0953-iv	Multithreading in C++	10	Integrierte Veranstaltung	6

2 Lerninhalt

C++ bietet eine der fortschrittlichsten Threadschnittstellen, die heute verfügbar sind. Am Beispiel C++ führt dieser Kurs in die parallele Programmierung für gemeinsamen Speicher mit Threads ein.

- Architekturen mit gemeinsamem Speicher
- Management von Threads
- Zugriff auf gemeinsame Daten
- Synchronisierung nebenläufiger Operationen
- Entwurf lockbasierter nebenläufiger Datenstrukturen
- Entwurf von nebenläufigem Code
- Testen und Fehlersuche

3 Qualifikationsziele / Lernergebnisse

Kompetenz in der Entwicklung paralleler Programme

- Systematisch korrekte und effiziente parallele Programme entwickeln
- Parallele Datenstrukturen entwerfen und umsetzen

4 Voraussetzung für die Teilnahme

Empfohlen: Kenntnisse in C/C++

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-0953-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)

6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0953-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Fortgeschrittenes Multithreading in C++</td></tr>
<tr><td>Modul Nr.
20-00-0977</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0977-iv</td><td>Fortgeschrittenes Multithreading in C++</td><td>6</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
C++ bietet eine der modernsten Threadschnittstellen, die heute verfügbar sind. Am Beispiel C++ führt dieser Kurs in die fortgeschrittene parallele Programmierung für gemeinsamen Speicher mit Threads ein.

Aufbauend auf den Inhalten der Vorlesung Multithreading in C++ werden die folgenden Themen behandelt:
• C++ Speichermodell und atomare Operationen
• Entwurf lockfreier nebenläufiger Datenstrukturen
• Forstgeschrittenes Thread-Management (z.B. Thread Pools)</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nachdem Studierende die Veranstaltung besucht haben, haben Sie erweiterte Kompetenz in der Entwicklung paralleler Programme und sind in der Lage
- Systematisch korrekte und effiziente parallele Programme zu entwickeln
- Parallele Datenstrukturen zu entwerfen und umzusetzen</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

• Kenntnisse in C/C++
• Basiskenntnisse der Programmierung von Threads in C++ (lockbasierte Synchronisation und lockbasierte nebenläufige Datenstrukturen)</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-0977-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.</td></tr>
</table>

	Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0977-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Skalierbare Datenmanagement-Systeme						
Modul Nr. 20-00-1017	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1017-iv	Skalierbares Datenmanagement	6	Integrierte Veranstaltung	4

2 Lerninhalt

Diese Vorlesungen ist eine Einführung in die Basiskonzepte und die wesentlichen Paradigmen für skalierbare Datenmanagement-Systeme. Der Fokus der Vorlesung ist auf die system-orientieren Aspekten und Interna solcher Systeme gerichtet, um große Datenmengen zu speichern, zu ändern, und zu analysieren.

Themen der Vorlesung sind:

Database Architectures
Parallel and Distributed Databases
Data Warehousing
MapReduce and Hadoop
Spark and its Ecosystem
Optional: NoSQL Databases, Stream Processing, Graph Databases, Scalable Machine Learning

3 Qualifikationsziele / Lernergebnisse

Nach dem Kurs haben die Studierenden einen Überblick über die wichtigsten Konzepte, Algorithmen und System-Aspekte für skalierbare Datenmanagement-Systeme erworben. Das Hauptziel ist es, dass die Studierenden das Wissen besitzen, solche Systeme zu designen und zu entwickeln, inklusive praktischer Übungen auf Basis von bestehenden Systemen wie Spark.

4 Voraussetzung für die Teilnahme

Empfohlen:

Programmierkenntnisse in C++ and Java
Der vorherige Besuch von Informationsmanagement oder einer vergleichbaren Veranstaltung

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1017-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1017-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Deep Learning: Architectures & Methods						
Modul Nr. 20-00-1034	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1034-iv	Deep Learning: Architectures & Methods	6	Integrierte Veranstaltung	4

2 Lerninhalt

- Auffrischung des Hintergrundwissens
- Deep Feedforward Netze
- Regularisierung im Deep Learning
- Optimierung zum Training tiefer Netze
- Convolutional tiefe Netze
- Modelierung von Sequenzen durch Rekordernte und Rekursive Netze
- Lineare Faktor Modelle
- Autoenkoder
- Repräsentationslernen
- Strukturierte Probabilistische Modelle zum Deep Learning
- Monte Carlo Methoden
- Approximative Inferenz
- Tiefe generative Modelle
- Deep Reinforcement Learning
- Deep Learning in Vision
- Deep Learning in NLP

3 Qualifikationsziele / Lernergebnisse

Dieser Kurs richtet sich an Studierende mit fortgeschrittenem Erfahrung im maschinellen Lernen und vermittelt diesen Studierenden das notwendige Wissen, um eigenständig Forschungsprojekte im Bereich der Deep Learning durchzuführen, z.B. im Rahmen einer Bachelor- oder Masterarbeit. Dies betrifft sowohl ein grundlegendes Verständnis der algorithmischen Ansätze zum Deep Learning als auch die der Architekturen der tiefen tiefen Netze.

4 Voraussetzung für die Teilnahme

Empfohlen: Der vorherige Besuch von „Statistisches Maschinelles Lernen“ und „Data Mining und Maschinelles Lernen“ oder vergleichbarer Veranstaltungen

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1034-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1034-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Reinforcement Learning: Von Grundlagen zu den tiefen Ansätzen</td></tr>
<tr><td colspan="2">Modul Nr.
20-00-1047</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="4">Sprache
Deutsch und Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1047-iv</td><td>Reinforcement Learning: Von Grundlagen zu den tiefen Ansätzen</td><td>6</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
• Auffrischung des Hintergrundwissens
• Black box Reinforcement Learning
• Modellierung als Bandit, Markov Decision Processes und Partially Observable Markov Decision Processes
• Optimale Steuerung und Regelung
• Modellernen
• Wertefunktionslernen
• Policy Search
• Tiefe Wertefunktion Methoden
• Tiefe Policy Search Methoden
• Exploration vs Exploitation
• Hierarchisches Reinforcement Learning
• Intrinsische Motivation</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Dieser Kurs richtet sich an Studierende mit erster Erfahrung im maschinellen Lernen und vermittelt diesen Studierenden das notwendige Wissen, um eigenständig Forschungsprojekte im Bereich der Reinforcement Learning durchzuführen, z.B. im Rahmen einer Bachelor- oder Masterarbeit. Dies betrifft sowohl ein grundlegendes Verständnis der algorithmischen Ansätze zum Reinforcement Learning als auch Anwendungen von tiefen Netzen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Gute Programmierkenntnisse in Python.
Der vorherige Besuch von „Statistisches Maschinelles Lernen“ oder einer vergleichbaren Veranstaltung ist hilfreich aber nicht zwingend erforderlich</td></tr>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1047-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1047-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. Autonome Systeme und Robotik M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Konzepte der Programmiersprachen					
Modul Nr. 20-00-1117	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1117-iv	Konzepte der Programmiersprachen	6	Integrierte Veranstaltung	4

2 Lerninhalt

Kurze Einführung und Geschichte der Programmiersprachen, Kriterien zur Messung von Programmiersprachen, Grundkonzepte der PL wie Syntax, Semantik, Variablen, Namen, Bindungen, Umfang, Subprogram, Expressionen, Arrays, Pointers, abstrakte Typen, funktionale Programme

3 Qualifikationsziele / Lernergebnisse

Die Studierenden werden am Ende des Kurses in der Lage sein, die zugrundeliegenden Mechanismen der wichtigsten Konzepte hinter Programmiersprachen zu verstehen. Die Studierenden werden auch Erfahrung erhalten, eine einfache Programmiersprache mit einer beliebten Sprache Workbench namens MPS als Gruppenprojekt zu bauen.

4 Voraussetzung für die Teilnahme

Keine

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1117-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Klausur (Dauer 60 oder 90 oder 120 Minuten), Mündliche Prüfung (Dauer 15 oder 30 Minuten), Hausübungen (optional: einschließlich Testaten)

6 Voraussetzung für die Vergabe von Leistungspunkten

Bestehen der Prüfung (100%).

7 Benotung

Bausteinbegleitende Prüfung:

	• [20-00-1117-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulhandbuch

M. Sc. IT Security

Wahlbereich Studienbegleitende Leistungen

Praktika, Projektpraktika und ähnliche Veranstaltungen

Modulbeschreibung

Modulname Hacker Contest						
Modul Nr. 20-00-0114	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0114-pr	Hacker Contest	6	Praktikum	4

2 Lerninhalt

Das Praktikum wird jedes mal an einem neuen Szenario ausgerichtet. Dieses Szenario (z.B. Internet Service Provider) gibt den Rahmen vor, welche Systeme aufgebaut und welche Arten von Attacken untersucht werden sollen.
Allgemein verläuft das Praktikum in mehreren Runden:

- Aufbau der Systeme
- Angriffe
- Dokumentation der Angriffe und mögliche Gegenmaßnahmen
- Härten der Systeme

3 Qualifikationsziele / Lernergebnisse

- Arbeit im Team
- Systematisches und sicheres Planen und Warten von IT-Systemen
- Erkennen von Angriffen auf IT-Systeme
- Analyse und Behebung von Schwachstellen
- Verständnis für praktische Sicherheitsprobleme
- Anwendung und Weiterentwicklung von Sicherheitstools

4 Voraussetzung für die Teilnahme

Empfohlen:

	Grundkenntnisse in IT-Sicherheit und der Administration von Netzen und Rechnern
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0114-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0114-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Implementierung von Programmiersprachen</td></tr>
<tr><td>Modul Nr.
20-00-0306</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0306-pr</td><td>Implementierung von Programmiersprachen</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Es werden Konzepte der Implementierung von Programmiersprachen vermittelt. Ferner werden diese Konzepte angewendet, um Erweiterungen für Programmiersprachen zu implementieren.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Fähigkeit, eine professionelle Aufgabe aus der Informatik selbstständig und erfolgreich nach den anerkannten Grundsätzen der Profession zu bearbeiten.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Es wird kein Vorwissen vorausgesetzt. Jedoch sind gute Programmiererfahrungen sowie Kenntnisse über Kompilerbau und virtuelle Maschinen von Vorteil.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0306-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Leistungspunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:
• [20-00-0306-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)</td></tr>
</table>

8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Praktikum Sichere Mobile Netze</td></tr>
<tr><td>Modul Nr.
20-00-0552</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0552-pr</td><td>Praktikum Sichere Mobile Netze</td><td>6</td><td>Praktikum</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Das Praktikum Sichere Mobile Netze behandelt die angewandte Softwareentwicklung und Hardware-Software Entwicklung in den Themenbereichen Kommunikationsnetze, Sicherheit, Mobile Netze und Drahtloser Kommunikation bzw. der Kombination dieser Bereiche. Ziel ist das Lösen einer Problemstellung im Team aus den genannten Bereichen durch Implementierung in Software bzw. Hardware/Software.

Lerninhalte:
- Lösen einer Fragestellung im Bereich Kommunikationsnetze, Sicherheit, Mobile Netze und Drahtloser Kommunikation
- Rechereche von Lösungsalternativen und Abwägung von Vor-/Nachteilen der Alternativen
- Konzipieren einer Softwarearchitektur bzw. kombinierten Hardware-Software Architektur
- Entwerfen eines auf die Zielplattform angepassten Hardware-/Softwaredesigns
- Prototypische Umsetzung auf der ausgewählten Zielplattform
- Evaluation des Gesamtsystems in Bezug auf verschiedene Gütemaße
- Dokumentation der erstellten Lösung</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung besitzen die Studierenden die Fähigkeit Problemstellungen im Bereich Sichere Mobile Netze softwaretechnisch zu lösen. Die Studierenden haben hierzu Kenntnisse im Entwurf/der Umsetzung komplexer Protokolle bzw. Anwendungen in einem/mehreren der Bereiche Kommunikationsnetze, Sicherheit, Mobile Netze und Drahtloser Kommunikation erlangt. Die Studierenden sind in der Lage die gewählten Protokolle und Anwendungen zu implementieren, zu testen und deren Funktionsfähigkeit und Leistungsfähigkeit zu evaluieren. Sie sind in der Lage die erstellten Softwareartefakte verständlich zu dokumentieren und die erzielten Projektfortschritten und -ergebnissen verständlich zu präsentieren.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Erfolgreiche Teilnahme an einer Integrierten Veranstaltung des Fachgebiets SEEMOO</td></tr>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0553-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bausteinbegleitende Prüfung: • [20-00-0552-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Themenspezifisch ausgewählte, aktuelle wissenschaftliche Veröffentlichungen
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Projektpraktikum Sichere Mobile Netze</td></tr>
<tr><td>Modul Nr.
20-00-0553</td><td>Leistungspunkte
9 CP</td><td>Arbeitsaufwand
270 h</td><td>Selbststudium
180 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0553-pp</td><td>Projektpraktikum Sichere Mobile Netze</td><td>9</td><td>Projektpraktikum</td><td>6</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Das Projektpraktikum Sichere Mobile Netze behandelt die angewandte Softwareentwicklung und Hardware-Software Entwicklung in den Themenbereichen Kommunikationsnetze, Sicherheit, Mobile Netze und Drahtloser Kommunikation bzw. der Kombination dieser Bereiche. Ziel ist das eigenständige Bearbeiten eines Entwicklungsprojektes im Team.

Lerninhalte:
- Eigenständiges Bearbeiten eines Entwicklungsprojektes im Bereich Kommunikationsnetze, Sicherheit, Mobile Netze und Drahtloser Kommunikation
- Projektplanung und Projektmanagement
- Rechereche von Lösungsalternativen und Abwägung von Vor-/Nachteilen der Alternativen
- Konzipieren einer Softwarearchitektur bzw. kombinierten Hardware-Software Architektur
- Entwerfen eines auf die Zielplattform angepassten Hardware-/Softwaredesigns
- Prototypische Umsetzung auf der ausgewählten Zielplattform
- Evaluation des Gesamtsystems in Bezug auf verschiedene Gütemaße
- Dokumentation der erstellten Lösung sowie ausführliche Dokumentation des Projektmanagements</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung besitzen die Studierenden die Fähigkeit komplexe Problemstellungen im Bereich Sichere Mobile Netze softwaretechnisch zu lösen. Die Studierenden können hierzu eigenständig ein Projekt definieren, verwalten und durchführen. Die Studierenden haben Kenntnisse im Entwurf/der Umsetzung komplexer Protokolle bzw. Anwendungen in einem/mehreren der Bereiche Kommunikationsnetze, Sicherheit, Mobile Netze und Drahtloser Kommunikation erlangt. Die Studierenden sind in der Lage die gewählten Protokolle und Anwendungen zu implementieren, zu testen und deren Funktionsfähigkeit und Leistungsfähigkeit zu evaluieren. Sie sind in der Lage die</td></tr>
</table>

	Projektplanung und -verwaltung sowie die erstellten Softwareartefakte verständlich zu dokumentieren und die erzielten Projektfortschritten und -ergebnissen verständlich zu präsentieren.
4	**Voraussetzung für die Teilnahme** Empfohlen: Erfolgreiche Teilnahme an einer Integrierten Veranstaltung des Fachgebiets SEEMOO
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0553-pp] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0553-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Themenspezifisch ausgewählte, aktuelle wissenschaftliche Veröffentlichungen
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Implementierung und Forensik und Mediensicherheit</td></tr>
<tr><td>Modul Nr.
20-00-0603</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0603-pr</td><td>Implementierung und Forensik und Mediensicherheit</td><td>6</td><td>Praktikum</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Praktische Anwendung von Algorithmen in den Bereichen Robuste Hashverfahren, Image Registration, File Forensik, Multimedia Kryptographie, Web Content Retrieval</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Studierenden implementieren ausgewählte Methoden aus der Multimedia Sicherheit und der IT Forensik in verschiedenen aktuellen Hochsprachen abhängig von der konkreten Aufgabenstellung. Ziel ist es, abstrakte Algorithmen und Problemstellungen praxisnah umsetzen und lösen zu lernen. Ziel ist hierbei insbesondere, eine effiziente Lösung zu finden, die das gegebene Problem zuverlässig löst. Die Studierenden werden vertraut mit dem Prozess der softwaretechnischen Problemlösung praxisnaher Fragenstellungen der IT Forensik und Multimedia Sicherheit.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0603-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0603-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Watermarking Petticolas, Katzenbeisser; Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Computer Security Series, ISBN: 1580530354, 2000 Cox I, Miller M, Bloom J, Fridrich J, Kalker T.; Digital watermarking and steganography. Morgan Kaufmann, USA, 2007 Forensik Alexander Geschonneck: "Computer-Forensik". 6., aktualisierte und erweiterte Auflage, dpunkt.verlag GmbH, 2014. ISBN: 978-3864901331 Brian Carrier, File System Forensic Analysis, Addison Wesley,2005
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
Praktikum System and IoT Security</td></tr>
<tr><td>Modul Nr.
20-00-0615</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="5">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0615-pr</td><td>Praktikum System and IoT Security</td><td>6</td><td>Praktikum</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
Dieses Praktikum bietet verschiedene Programmierprojekte auf dem aktuellen Smartphone Betriebssystem Android:
● Entwicklung/Implementierung von ausgewählten Software Angriffen
● Entwicklung von sicheren Benutzerapplikationen
● Einspielen von Kernelerweiterungen
● Systemprogrammierung</td></tr>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Durch die erfolgreiche Teilnahme an dieser Veranstaltung erlangen Studierende Kenntnisse und praktische Erfahrungen mit Sicherheitsmechanismen in moderne Smartphone Betriebssystemen. Außerdem erwerben sie generelle Erfahrung in Systemprogrammierung.</td></tr>
<tr><td>4</td><td colspan="5">Voraussetzung für die Teilnahme
Empfohlen:
● Grundlagen Betriebssysteme
● Programmierkenntnisse in C++ und Java</td></tr>
<tr><td>5</td><td colspan="5">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0615-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)
Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.</td></tr>
</table>

	Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0615-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Wird in der Veranstaltung bekannt gegeben
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
Praktikum: Zuverlässige Softwaresicherheit für mobile Endgeräte</td></tr>
<tr><td>Modul Nr.
20-00-0640</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="5">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0640-pr</td><td>Praktikum: Zuverlässige Softwaresicherheit für mobile Endgeräte</td><td>6</td><td>Praktikum</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
● Einführung in Android und in die Programmierung von Apps
● mögliche Bedrohungen der Privatheit durch die Ausführung von Apps
● Entdecken möglicher Informationslecks durch Informationsflussanalysen
● statische und dynamische Sicherheitsanalysen
● Proof-Carrying-Code
● eigenständige Entwicklung von Apps und Sicherheitsanalyse dieser Apps
● eigenständige Erweiterung einer bestehenden Infrastruktur zur formal fundierten Sicherheitsanalyse von Android Apps</td></tr>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung kennen Studierende grundlegende Konzepte von Android wie das Berechtigungssystem. Sie verstehen Sicherheitsprobleme, die durch die Ausführung von Apps entstehen können und verstehen wie diese durch Informationsflussanalysen verhindert werden. Sie verstehen die Vorteile der Verwendung von Proof-Carrying Code. Sie können Apps eigenständig entwickeln und die durch ihre Ausführung entstehenden Informationsflüsse bezüglich Privatheitsanforderungen evaluieren. Sie können Erweiterungen für eine existierende Sicherheitsinfrastruktur entwickeln und funktionsfähig integrieren.</td></tr>
<tr><td>4</td><td colspan="5">Voraussetzung für die Teilnahme
Empfohlen: Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiengangs Informatik, insbesondere Programmierkenntnisse in Java und die Fähigkeit, mit formalen Sprachen und Kalkülen umzugehen.</td></tr>
<tr><td>5</td><td colspan="5">Prüfungsform
Bausteinbegleitende Prüfung:</td></tr>
</table>

	• [20-00-0640-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0640-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** ausgewählte Konferenz- und Zeitschriftenartikel
10	**Kommentar**

Modulbeschreibung

Modulname Softwaresecurity durch Laufzeitüberwachung					
Modul Nr. 20-00-0719	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0719-pr	Softwaresecurity durch Laufzeitüberwachung	6	Praktikum	4

2 Lerninhalt

Benutzer vertrauen Computeranwendungen in zunehmendem Maße sensible Daten wie z.B. Kontakt- und Kontodaten oder Bilder an. Bösartige oder fehlerhafte Anwendungen können durch Missbrauch solcher Daten großen Schaden verursachen. Es ist somit wünschenswert, Nutzeranforderungen an Informationssicherheit und Privacy durch geeignete Mechanismen sicherzustellen. Mit Laufzeitüberwachung existiert eine Technik für Mechanismen, die zur Laufzeit einer Anwendung deren Verhalten überwachen und geeignete Gegenmaßnahmen ergreifen sobald nötig. Besondere Bedeutung für die Informationssicherheit kommt zunehmend den verteilten Systemen wie sozialen Netzen und Cloud-Speichernlösungen zu. Laufzeitüberwachung für derartige verteilte Systeme ist der Fokus dieses Praktikums.

Dieses Praktikum bietet Studenten die Möglichkeit, praktische Erfahrung beim Implementieren, Einsetzen und Evaluieren von Mechanismen zur Laufzeitüberwachung zu erlangen.

3 Qualifikationsziele / Lernergebnisse

Praktische Erfahrung mit Laufzeitüberwachung zur Anwendungssicherheit, insbesondere zu: Inlining von Mechanismen zur Laufzeitüberwachung; formale Spezifikation von Sicherheitsanforderungen; Laufzeitüberwachung von Sicherheit in verteilten Systemen; Schwachstellenanalyse von Laufzeitmechanismen; Testen und Evaluation von Laufzeitmechanismen

4 Voraussetzung für die Teilnahme

Empfohlen:

Programmiererfahrung in Java; Informatikkenntnisse entsprechend dem 4. Semester des Bachelorstudiengangs

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-0719-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten**
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0719-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Praktikum: Formale Spezifikation und Verifikation in Isabelle/HOL</td></tr>
<tr><td>Modul Nr.
20-00-0778</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0778-pr</td><td>Praktikum: Formale Spezifikation und Verifikation in Isabelle/HOL</td><td>6</td><td>Praktikum</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
● Logik höherer Stufe (HOL)
● Einführung in das Werkzeug Isabelle/HOL
● Definition von Typen, Funktionen, Mengen und anderen grundlegenden Konzepten in der Spezifikationssprache von Isabelle/HOL
● Führen von Beweisen für einfache Aussagen in Isabelle/HOL
● Modellierung von Systemen und Eigenschaften sowie Beweis von Aussagen von schrittweise wachsender konzeptioneller Komplexität
● Diskussion und Bewertung von formalen Modellen und Beweisen</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung kennen Studierende die Formalismen auf denen Isabelle/HOL basiert, und sie könnnen dieses moderne Verifikationswerkzeug verwenden. Sie können in Isabelle/HOL sowohl eigenständig als auch im Team formale Modelle von Systemen und Eigenschaften konstruieren und Aussagen beweisen. Sie können erstellte formale Modelle und Beweise beurteilen, anderen präsentieren und im Team fundiert diskutieren.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiengangs Informatik, insbesondere grundlegende Logikkenntnisse und Fähigkeit mit formalen Sprachen und Kalkülen umzugehen</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0778-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0778-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** ● T. Nipkow, L. C. Paulson, M. Wenzel: Isabelle/HOL: A Proof Assistant for Higher-Order Logic; Springer ● online documentation material on Isabelle and Higher-Order Logic (HOL) Die Literaturempfehlungen werden kontinuierlich aktualisiert.
10	**Kommentar**

Modulbeschreibung

Modulname Dynamische Kontrolle von Systemanforderungen					
Modul Nr. 20-00-0797	**Leistungspunkte** 9 CP	**Arbeitsaufwand** 270 h	**Selbststudium** 180 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0797-pp	Dynamische Kontrolle von Systemanforderungen	9	Praktikum	6

2 Lerninhalt

- grundlegende Konzepte der dynamischen Kontrolle in verteilten Systemen
- Einführung in Werkzeuge zur Laufzeitkontrolle wie CliSeAu, JavaMOP und Polymer
- Spezifikation von Systemanforderungen in unterschiedlichen Formalismen
- Kombination von dynamischen Kontrollmechanismen mit Zielprogrammen
- zentrale vs dezentrale Kontrolle in verteilten Systemen
- Protokolle zur Koordination zwischen dezentralen Kontrollmechanismen in verteilten Systemen
- eigenständige Adaption von dynamischen Kontrollmechanismen für Zielprogramme
- eigenständige Erweiterung einer bestehenden Infrastruktur zur dynamischen Kontrolle von Anforderungen in verteilten Systemen und Evaluation von Erweiterungen

3 Qualifikationsziele / Lernergebnisse

Nach erfolgreicher Teilnahme an der Veranstaltung kennen Studierende grundlegende Konzepte der dynamischen Kontrolle in verteilten Systemen.
Sie verstehen wie Schwachstellen in verteilten Softwaresystemen, wie z.B. Sicherheitslücken, mit Hilfe von dynamischen Kontrollen beseitigt werden können. Sie verstehen, wie Anforderungen als Politiken formalisiert werden können und können solche Formalisierungen von Anforderungen in verschiedenen Sprachen durchführen. Sie können Mechanismen zur dynamischen Kontrolle für konkrete Systeme und Anforderungen einsetzen und adaptieren. Sie können Mechanismen zur dynamischen Kontrolle entwickeln, evaluieren und mit anderen Mechanismen integrieren.

4 Voraussetzung für die Teilnahme

Empfohlen:

Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiengangs Informatik, insbesondere Programmierkenntnisse in Java und die Fähigkeit, mit formalen Sprachen umzugehen

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0797-pp] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0797-pp] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Zuverlässige Softwaresicherheit für mobile Endgeräte					
Modul Nr. 20-00-0799	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0799-pr	Zuverlässige Softwaresicherheit für mobile Endgeräte	6	Praktikum	4

2 Lerninhalt

- Einführung in Android und in die Programmierung von Apps
- mögliche Bedrohungen der Privatheit durch die Ausführung von Apps
- Entdecken möglicher Informationslecks durch Informationsflussanalysen
- statische und dynamische Sicherheitsanalysen
- Proof-Carrying-Code
- eigenständige Entwicklung von Apps und Sicherheitsanalyse dieser Apps
- eigenständige Erweiterung einer bestehenden Infrastruktur zur formal fundierten Sicherheitsanalyse von Android Apps

3 Qualifikationsziele / Lernergebnisse

Nach erfolgreicher Teilnahme an der Veranstaltung kennen Studierende grundlegende Konzepte von Android wie das Berechtigungssystem. Sie verstehen Sicherheitsprobleme, die durch die Ausführung von apps entstehen können und verstehen wie diese durch Informationsflussanalysen verhindert werden. Sie verstehen die Vorteile der Verwendung von Proof-Carrying-Code. Sie können apps eigenständig entwickeln und die durch ihre Ausführung entstehenden Informationsflüsse bezüglich Privatheitsanforderungen evaluieren.
Sie können Erweiterungen für eine existierende Sicherheitsinfrastruktur entwickeln und funktionsfähig integrieren.

4 Voraussetzung für die Teilnahme

Empfohlen:

Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiengangs Informatik, insbesondere Programmierkenntnisse in Java und die Fähigkeit mit formalen Sprachen und Kalkülen umzugehen.

5 Prüfungsform

Bausteinbegleitende Prüfung:

	• [20-00-0799-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0799-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Distributed Systems Programming: Projektpraktikum</td></tr>
<tr><td>Modul Nr.
20-00-0984</td><td>Leistungspunkte
9 CP</td><td>Arbeitsaufwand
270 h</td><td>Selbststudium
180 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0984-pp</td><td>Distributed Systems Programming: Projektpraktikum</td><td>9</td><td>Praktikum</td><td>6</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Das "DSP-Projektpraktikum" adressiert Forschungsthemen im Bereich von distributed systems (DS, deutsch verteilten Anwendungen) und Programmiersprachen für DS. Die angebotenen Themen hängen von der aktuellen Forschung der DSP Gruppe ab und umfassen unter anderem:

• Software-defined networking (SDN)
• Network function virtualization (NFV) and in-network processing (INP)
• Traffic engineering (TE)
• Network monitoring
• Resource management in datacenters (RMF)
• Big data analytics (Spark, YARN, OpenStack, ..)
• Event-based systems
• Security in SDN, INP, and big data
• Geo-distributed data processing
• Compiler infrastructures for DS
• Language abstractions for DS
• Session types / calculi for DS
• Network Protocols

Die teilnehmenden Studierenden realisieren ein Forschungsprojekt welches zusammen mit den Betreuern definiert wird.
Das “DSP: Projektpraktikum” hat im Vergleich zum “DSP: Praktikum” einen größeren Umfang.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach der Teilnahme am "DSP-Projektpraktikum" können Studierende technische und wissenschaftliche Probleme im Bereich DS lösen.

Je nach ausgewähltem Thema erlernen Studierende folgende Kompetenzen:

Entwurf komplexer DS
Methodische Analyse und Auswertung von:</td></tr>
</table>

	• Modellen • Experimenten • Software • Entwurf von Programmiersprachen • Schreiben von technischen Dokumenten oder Projektberichten • Erstellen und vortragen eines Abschlussvortrages
4	**Voraussetzung für die Teilnahme** Empfohlen: Interesse am Erarbeiten von Lösungsvorschlägen für herausfordernde Probleme im Bereich DS, eigenverantwortliches arbeiten und ein großes Interesse an aktuellen Forschungsthemen. Da die angebotenen Themen ein großes Themengebiet abdecken, sind die Anforderungen sehr verschieden und projektabhängig. Eine detaillierte Beschreibung der Themen als auch der Anforderungen wird während des ersten Termins präsentiert.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0984-pp] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0984-pp] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
Distributed Systems Programming: Praktikum</td></tr>
<tr><td>Modul Nr.
20-00-0985</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="5">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0985-pr</td><td>Distributed Systems Programming: Praktikum</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
Das "DSP-Praktikum" adressiert Forschungsthemen im Bereich von distributed systems (DS, deutsch verteilten Anwendungen) und Programmiersprachen für DS. Die angebotenen Themen hängen von der aktuellen Forschung der DSP Gruppe ab und umfassen unter anderem:
Software-defined networking (SDN)
Network function virtualization (NFV) and in-network processing (INP)
Traffic engineering (TE)
Network monitoring
Resource management in datacenters (RMF)
Big data analytics (Spark, YARN, OpenStack, ..)
Event-based systems
Security in SDN, INP, and big data
Geo-distributed data processing
Compiler infrastructures for DS
Language abstractions for DS
Session types / calculi for DS
Network Protocols
Die teilnehmenden Studierenden realisieren ein Forschungsprojekt welches zusammen mit den Betreuern definiert wird.
Das “DSP: Projektpraktikum” hat im Vergleich zum “DSP: Praktikum” einen größeren Umfang.</td></tr>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Nach der Teilnahme am "DSP-Praktikum" können Studierende technische und wissenschaftliche Probleme im Bereich DS lösen.

Je nach ausgewähltem Thema erlernen Studierende folgende Kompetenzen:

Entwurf komplexer DS
Methodische Analyse und Auswertung von:
Modellen</td></tr>
</table>

	• Experimenten • Software • Entwurf von Programmiersprachen • Schreiben von technischen Dokumenten oder Projektberichten • Erstellen und vortragen eines Abschlussvortrages
4	**Voraussetzung für die Teilnahme** Empfohlen: Interesse am Erarbeiten von Lösungsvorschlägen für herausfordernde Probleme im Bereich DS, eigenverantwortliches Arbeiten und ein großes Interesse an aktuellen Forschungsthemen. Da die angebotenen Themen ein großes Themengebiet abdecken, sind die Anforderungen sehr verschieden und projektabhängig. Eine detaillierte Beschreibung der Themen als auch der Anforderungen wird während des ersten Termins präsentiert.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0985-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0985-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Artificial Intelligence and Machine Learning M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Cybersecurity Lab</td></tr>
<tr><td>Modul Nr.
20-00-1018</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1018-pr</td><td>Cybersecurity Lab</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
In diesem Praktikum werden wir grundlegende als auch weiterführende Aspekte von Netzwerksicherheit erlernen. Wir werden die grundlegenden Protokolle, wie BGP und DNS, Infrastruktur Modelle, wie z.B. Router, Switches und Firewalls besprechen und wir werden ebenso die Anwendung von Sicherheit besprechen. Wir werden Attacks und Defences besprechen als auch demonstrieren. Jede/r Studierende/r wird ein spezifisches Thema, welches während des Semesters unter Anleitung zu bearbeiten ist, erhalten.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Am Ende des Kurses werden die Studierenden gute Kenntnisse in Netzwerksicherheit, und speziell auf den Gebieten der durch sie bearbeitenden Projekte, erlangen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Die Studierenden sollten einen Background in Netzwerk- und Operating Systems haben.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-1018-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Leistungspunkten
Bestehen der Prüfung (100%)</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1018-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Praktikum Friedens-, Sicherheits- und Kriseninformatik</td></tr>
<tr><td>Modul Nr.
20-00-1020</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1020-pr</td><td>Praktikum Friedens-, Sicherheits- und Kriseninformatik</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Das Praktikum beinhaltet Entwicklungsthemen aus der aktuellen Forschung des Fachgebiets „Wissenschaft und Technik für Frieden und Sicherheit“ (PEASEC). Neben einem generellen Überblick über aktuelle Themen wird ein tiefgehender Einblick in ein spezielles Entwicklungsgebiet vermittelt. Die Themen bestimmen sich aus den spezifischen Arbeitsgebieten der Mitarbeiter und vermitteln technische und einleitende wissenschaftliche Kompetenzen. Die Bearbeitung erfolgt in kleinen Gruppen.
Themen für das aktuelle Semester finden Sie unter www.peasec.de/lehre</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Fähigkeit eine praktische Aufgabe ggf. im Team erfolgreich nach Vorgabe zu bearbeiten und deren Ergebnisse angemessen zu präsentieren. Beispiele sind:
• Anforderungserhebung und (empirische) Vorstudien
• Konzeption und Implementierung innovativer Anwendungen
• Evaluation und Weiterentwicklung bestehender Anwendungen</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Grundlagen der Informatik/“Funktionale und objektorientierte Programmierkonzepte“</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-1020-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1020-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Reuter, C. (2018) Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement, 660 S., Wiesbaden: Springer Vieweg – im Druck Altmann, J., Bernhardt, U., Nixdorff, K., Ruhmann, I., & Wöhrle, D. (2016). Naturwissenschaft - Rüstung - Frieden - Basiswissen für die Friedensforschung (Vol. 49), Wiesbaden: Springer Vieweg. Weitere Literatur wird in der Veranstaltung je nach gewähltem Thema genannt.
10	**Kommentar**

Modulbeschreibung

Modulname Projektpraktikum Friedens- und Kriseninformatik					
Modul Nr. 20-00-1027	**Leistungspunkte** 9 CP	**Arbeitsaufwand** 270 h	**Selbststudium** 180 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1027-pp	Projektpraktikum Friedens- und Kriseninformatik	9	Projekt	6

2 Lerninhalt

Das Projektpraktikum beinhaltet Entwicklungsthemen aus der aktuellen Forschung des Fachgebiets „Wissenschaft und Technik für Frieden und Sicherheit“ (PEASEC). Neben ei-nem generellen Überblick über aktuelle Themen wird ein tiefgehender Einblick in ein spezi-elles Entwicklungsgebiet vermittelt. Die Themen bestimmen sich aus den spezifischen Ar-beitsgebieten der Mitarbeiter und vermitteln technische und einleitende wissenschaftliche Kompetenzen. Die Bearbeitung erfolgt in kleinen Gruppen. Projektmanagement und die Selbstorganisation im Team ist explizit Teil der Aufgabenstellung.
Themen für das aktuelle Semester finden Sie unter www.peasec.de/lehre

3 Qualifikationsziele / Lernergebnisse

Die Fähigkeit eine praktische Aufgabe ggf. im Team erfolgreich nach Vorgabe zu bearbeiten und deren Ergebnisse angemessen zu präsentieren. Beispiele sind:

- Anforderungserhebung und (empirische) Vorstudien
- Konzeption und Implementierung innovativer Anwendungen
- Evaluation und Weiterentwicklung bestehender Anwendungen

4 Voraussetzung für die Teilnahme

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1027-pp] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)

6 Voraussetzung für die Vergabe von Leistungspunkten

	Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1027-pp] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Reuter, C. (2018) Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement, 660 S., Wiesbaden: Springer Vieweg Altmann, J., Bernhardt, U., Nixdorff, K., Ruhmann, I., & Wöhrle, D. (2016). Naturwissenschaft - Rüstung - Frieden - Basiswissen für die Friedensforschung (Vol. 49), Wiesbaden: Springer Vieweg. Weitere Literatur wird in der Veranstaltung je nach gewähltem Thema genannt.
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Projektpraktikum Softwareentwicklung zum Schutz der Privatsphäre</td></tr>
<tr><td colspan="2">Modul Nr.
20-00-1053</td><td>Leistungspunkte
9 CP</td><td>Arbeitsaufwand
270 h</td><td>Selbststudium
180 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="4">Sprache
Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1053-pp</td><td>Projektpraktikum Softwareentwicklung zum Schutz der Privatsphäre</td><td>9</td><td>Projekt</td><td>6</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
In dieser Veranstaltung entwickeln die Studierenden systematisch eine beispielhafte Anwendung, ein Werkzeug, oder einen Demonstrator zum Schutz der Privatsphäre. Dies beinhaltet die Spezifikation der Anforderungen und des Designs, sowie eine Implementierung mit Tests, Evaluierung und Dokumentation.

Wir bieten zwei Varianten dieser Veranstaltung an: PRIVDEV-M (Praktikum, 6 CP, 4 SWS) und PRIVDEV-L (Projektpraktikum, 9 CP, 6 SWS) mit komplexeren Themen und detaillierteren Anforderungen an das Projektmanagement. Bitte stellen Sie sicher, dass Sie sich für die richtige Variante anmelden.

Eine Liste möglicher Themen mit Bezug zu aktuellen Forschungsthemen des Fachgebiets ENCRYPTO, eine detaillierte Beschreibung des Prozesses und weitere Informationen finden Sie unter https://encrypto.de/PRIVDEV.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
- Tieferes Verständnis warum Privatheit benötigt wird und wie sie sichergestellt werden kann
- Mehr Erfahrung in Softwareentwicklung und Projektmanagement
- Planung und Verfolgung eines Prozesses zur Entwicklung einer Privatsphäre-schützenden Anwendung oder Werkzeug: Anforderungen, Design, Implementierung, Test, Evaluierung und Dokumentation.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

- Grundwissen in angewandter Kryptographie, z.B. durch erfolgreiches Bestehen der Veranstaltung "Einführung in die Kryptographie" und idealerweise auch "Kryptographische Protokolle (CRYPROT)" und/oder "Secure Computation".
- Sehr gute Programmierkenntnisse und zumindest Grundkenntnisse in der in der jeweiligen Themenbeschreibung angegebenen Programmiersprache sind erforderlich.
- Eventuelle weitere Anforderungen sind in der jeweiligen Themenbeschreibung angegeben.</td></tr>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1053-pp] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1053-pp] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname

Praktikum Softwareentwicklung zum Schutz der Privatsphäre

Modul Nr.	Leistungspunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-1054	6 CP	180 h	120 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Englisch	Koordinatoren/Koordinatorinnen IT Security

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1054-pr	Praktikum Softwareentwicklung zum Schutz der Privatsphäre	6	Praktikum	4

2 Lerninhalt

In dieser Veranstaltung entwickeln die Studierenden systematisch eine beispielhafte Anwendung, ein Werkzeug, oder einen Demonstrator zum Schutz der Privatsphäre. Dies beinhaltet die Spezifikation der Anforderungen und des Designs, sowie eine Implementierung mit Tests, Evaluierung und Dokumentation.

Wir bieten zwei Varianten dieser Veranstaltung an: PRIVDEV-M (Praktikum, 6 CP, 4 SWS) und PRIVDEV-L (Projektpraktikum, 9 CP, 6 SWS) mit komplexeren Themen und detailierteren Anforderungen an das Projektmanagement. Bitte stellen Sie sicher, dass Sie sich für die richtige Variante anmelden.

Eine Liste möglicher Themen mit Bezug zu aktuellen Forschungsthemen des Fachgebiets ENCRYPTO, eine detailierte Beschreibung des Prozesses und weitere Informationen finden Sie unter https://encrypto.de/PRIVDEV.

3 Qualifikationsziele / Lernergebnisse

- Tieferes Verständnis warum Privatheit benötigt wird und wie sie sichergestellt werden kann
- Mehr Erfahrung in Softwareentwicklung und Projektmanagement
- Planung und Verfolgung eines Prozesses zur Enwicklung einer Privatsphäre-schützenden Anwendung oder Werkzeug: Anforderungen, Design, Implementierung, Test, Evaluierung und Dokumentation.

4 Voraussetzung für die Teilnahme

Empfohlen:

- Grundwissen in angewandter Kryptographie, z.B. durch erfolgreiches Bestehen der Veranstaltung "Einführung in die Kryptographie" und ideallerweise auch "Kryptographische Protokolle (CRYPROT)" und/oder "Secure Computation".
- Sehr gute Programmierkenntnisse und zumindest Grundkenntnisse in der in der jeweiligen Themenbeschreibung angegebenen Programmiersprache sind erforderlich.
- Eventuelle weitere Anforderungen sind in der jeweiligen Themenbeschreibung angegeben.

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1054-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1054-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Praktikum Security Engineering</td></tr>
<tr><td>Modul Nr.
20-00-1056</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1056-pr</td><td>Praktikum Security Engineering</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Im Rahmen dieses Praktikums sollen Implementierungen zu Forschungszwecken mit den Schwerpunkten Kryptographie und Privatheit vorgenommen worden. Die angebotenen Praktika stammen aus den folgenden Bereichen:

- IT-Sicherheit im autonomen Fahrzeug
- Bahnsicherheit
- Hardwaresicherheit (IoT)
- Seitenkanalangriffe
- Attestierung</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Ziel dieses Praktikums ist die Ausweitung von Programmierkentnissen sowie die Partizipation in Forschungsprojekten. Zusätzlich werden die Teilnehmer*innen Wissen in den genannten Bereichen erlangen und erfahren den jeweils aktuellen Forschungsstand.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-1056-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Leistungspunkten
Bestehen der Prüfung (100%)</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1056-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
IoT- und Funkprotokolle in eingebetteten Systemen</td></tr>
<tr><td>Modul Nr.
20-00-1064</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="5">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1064-pr</td><td>IoT- und Funkprotokolle in eingebetteten Systemen</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
Im Rahmen des Praktikums lernen die Studierenden IoT- und Funkprotokolle kennen und führen eigenständig ein Projekt mit eingebetteter Hardware durch. Darüber hinaus werden auch Aspekte der IT-Sicherheit mitberücksichtigt.
Der Fokus liegt auf Bluetooth LE, Bluetooth Mesh, LoRaWAN sowie die Kommunikation über OOB Kanäle. Abhängig vom gewählten Projekt-Thema werden Hardware (Mikrocontroller, FPGAs, RF-Transceiver, Software Defined Radio uvm.) sowie Laborumgebung (Logikanalysatoren, RF Analysatoren, Oszilloskope uvm.) zur Verfügung gestellt.</td></tr>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Am Ende der Veranstaltung sind die Studierenden in der Lage, mit komplexen Spezifikationen von Funkprotokollen umzugehen und in die Praxis zu transferieren. Weiterhin wird der praktische Umgang mit eingebetteten Systemen und Laborequipment vermittelt.</td></tr>
<tr><td>4</td><td colspan="5">Voraussetzung für die Teilnahme
Empfohlen sind Vorkenntnisse in Computernetzwerken und in Eingebetteten Systemen. Kenntnis der Programmiersprache C und Grundkenntnisse der Elektrotechnik sind hilfreich, ebenso Kenntnisse aus einschlägigen Vorlesungen des Bereichs.</td></tr>
<tr><td>5</td><td colspan="5">Prüfungsform
Bausteinbegleitende Prüfung:
[20-00-1064-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)
Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.
Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1064-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Praktikum Verantwortung und Sicherheit in der Informatik</td></tr>
<tr><td>Modul Nr.
20-00-1072</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1072-pr</td><td>Praktikum Verantwortung und Sicherheit in der Informatik</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Das Praktikum beinhaltet Entwicklungsthemen aus der aktuellen Forschung des Fachgebiets „Wissenschaft und Technik für Frieden und Sicherheit“ (PEASEC). Neben einem generellen Überblick über aktuelle Themen wird ein tiefgehender Einblick in ein spezielles Entwicklungsgebiet vermittelt. Die Themen bestimmen sich aus den spezifischen Arbeitsgebieten der Mitarbeiter_innen und vermitteln technische und einleitende wissenschaftliche Kompetenzen. Die Bearbeitung erfolgt in kleinen Gruppen.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Fähigkeit eine praktische Aufgabe ggf. im Team erfolgreich nach Vorgabe zu bearbeiten und deren Er-gebnisse angemessen zu präsentieren. Beispiele sind:
- Lösen einer Fragestellung im Bereich von Verantwortung und Sicherheit in der Informatik
- Anforderungserhebung und (empirische) Vorstudien
- Recherche von Lösungsalternativen und Abwägung von Vor-/Nachteilen der Alternativen
- Entwurf, prototypische Implementierung oder Weiterentwicklung innovativer Anwendungen
- Evaluation bestehender Anwendungen in Bezug auf verschiedene Gütemaße
- Dokumentation der erstellten Lösung</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Grundlagen in mindestens einem der Bereiche: Informatik, IT-Sicherheit, Mensch-Computer-Interaktion oder Friedens- und Konfliktforschung; Kenntnisse in der Softwareentwicklung und Programmierung</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1072-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1072-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Projektpraktikum Interaktive resiliente Informationstechnik</td></tr>
<tr><td>Modul Nr.
20-00-1073</td><td>Leistungspunkte
9 CP</td><td>Arbeitsaufwand
270 h</td><td>Selbststudium
180 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1073-pp</td><td>Projektpraktikum Interaktive resiliente Informationstechnik</td><td>9</td><td>Projekt</td><td>6</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Das Projektpraktikum beinhaltet Entwicklungsthemen aus der aktuellen Forschung des Fachgebiets „Wissen-schaft und Technik für Frieden und Sicherheit“ (PEASEC). Neben einem generellen Überblick über aktuelle Themen wird ein tiefgehender Einblick in ein spezielles Entwicklungsgebiet vermittelt. Die Themen bestimmen sich aus den spezifischen Arbeitsgebieten der Mitarbeiter_innen und vermitteln technische und einleitende wissenschaftliche Kompetenzen. Die Bearbeitung erfolgt in kleinen Gruppen. Projektmanagement und die Selbstorganisation im Team ist explizit Teil der Aufgabenstellung.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Fähigkeit eine praktische Aufgabe ggf. im Team erfolgreich nach Vorgabe zu bearbeiten und deren Er-gebnisse angemessen zu präsentieren. Beispiele sind:
- Lösen einer Fragestellung im Bereich der interaktiven resilienten Informationstechnik
- Anforderungserhebung und (empirische) Vorstudien
- Recherche von Lösungsalternativen und Abwägung von Vor-/Nachteilen der Alternativen
- Entwurf, prototypische Implementierung oder Weiterentwicklung innovativer Anwendungen
- Evaluation bestehender Anwendungen in Bezug auf verschiedene Gütemaße
- Dokumentation der erstellten Lösung</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Grundlagen in mindestens einem der Bereiche: Informatik, IT-Sicherheit, Mensch-Computer-Interaktion oder Friedens- und Konfliktforschung; Kenntnisse in der Softwareentwicklung und Programmierung</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1073-pp] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1073-pp] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
Bug Hunting Praktikum</td></tr>
<tr><td>Modul Nr.
20-00-1083</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="5">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1083-pr</td><td>Bug Hunting Praktikum</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
In diesem Praktikum beschäftigen sich die Studierenden mit dem automatischen oder manuellen Aufdecken von Schwachstellen und Verwundbarkeiten in realen Open Source Softwareprojekten. Die Studierenden lernen gängige Methoden zur Identifizierung von Angriffsflächen, Erstellung eines Angreifermodells und das Finden und Dokumentieren von Schwachstellen. Diese Schritte werden eigenständig in einem praktischen Teil von den Studierenden umgesetzt.

Folgende Themen und Tätigkeiten sind Teil des Praktikums:
- Einarbeitung in Open Source Softwareprojekte aus Sicht eines Penetration Testers
- Einarbeitung in gängige Tools zur Identifizierung von Angriffsflächen oder möglichen Schwachstellen
- Praktisches Anwenden der gelernten Methoden zur Schwachstellenidentifikation
- Dokumentation der Schwachstellen und Identifikation von Gegenmaßnahmen
- Präsentation der Ergebnisse</td></tr>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Ein theoretischer Teil vermittelt den Studierende Methoden zur Schwachstellenidentifikation und Bedrohungsmodellierung von Softwareprojekten. In einem praktischen Teil sammeln die Studenten selbstständig Erfahrungen im Identifizieren von Schwachstellen. Die Studierenden sind nach erfolgreichem Absolvieren des Praktikums in der Lage, selbstständig und strukturiert Sicherheitslücken in Softwareprojekten zu finden und zu dokumentieren. Die Studierenden können nach dem Praktikum die Schwere und die Folgen von Sicherheitslücken einschätzen, sowie Gegenmaßnahmen benennen.</td></tr>
<tr><td>4</td><td colspan="5">Voraussetzung für die Teilnahme
Empfohlen:

- Gute Teamfähigkeit
- Interesse an Schwachstellenidentifikation, Programmanalyse und Exploitation</td></tr>
</table>

	- Gute Programmierkenntnisse - Linux Kenntnisse
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1083-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1083-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Praktikum Seitenkanalanalyse</td></tr>
<tr><td>Modul Nr.
20-00-1090</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1090-pr</td><td>Praktikum Seitenkanalanalyse</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Seitenkanäle sind Kommunikationskanäle, die auf Ausführungsmerkmalen basieren, die nicht zur Kommunikation vorgesehen waren. Die zugrundeliegenden Ausführungsmerkmale können beispielsweise die Ausführungszeit, der Stromverbrauch und elektromagnetische Abstrahlung sein. Seitenkanäle sind seit vielen Jahren als ernste Bedrohung für kryptographische Implementierungen bekannt. Technologischer Fortschritt bringt üblicherweise neue Möglichkeiten für Seitenkanalangriffe mit sich. Beispielsweise hat das Internet of Things die Anzahl der möglichen Zielgeräte erhöht und die Bedrohung durch Seitenkanäle damit noch relevanter gemacht.

Das Praktikum deckt die Schritte ab, die zur Ausführung von Seitenkanalangriffen gegen kryptographische Implementierungen, zur Extraktion von geheimen Informationen, sowie zur Verminderung solcher Schwachstellen benötigt werden. Beispielthemen sind:
- Auswahl von Zielimplementierungen für Seitenkanalangriffe
- Manipulation von Strom-, Zeit-, oder EM-Messkurven
- Implementierung von Modellen für Seitenkanalschwachstellen
- Differential Side-Channel Analysis
- Seitenkanalgegenmaßnahmen</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an diesem Praktikum, werden die Studierenden:
- das Ausmaß der Gefahr durch Seitenkanalschwachstellen einschätzen können,
- verstehen wie Seitenkanalangriffe funktionieren,
- fähig sein, Seitenkanalangriffe gegen kryptographische Implementierungen auszuführen, um geheime Informationen zu extrahieren und
- wissen, wie Seitenkanalangriffe abgewehrt werden können.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme</td></tr>
</table>

	Empfohlen werden Informatikkenntnisse entsprechend der ersten vier Semester des Bachelorstudiengangs Informatik, insbesondere Programmierkenntnisse.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1090-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1090-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
BOOTS: Build your own tech startup</td></tr>
<tr><td>Modul Nr.
20-00-1104</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1104-pr</td><td>BOOTS: Build your own tech startup</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Studierenden erhalten in der Veranstaltung einen umfassenden Überblick über die verschiedenen Aspekte von Unternehmensgründungen (Entrepreneurship). Im Rahmen der Blockveranstaltung wird ein praktisches Forum geboten, um Geschäftsmodelle im High-Tech Bereich zu fördern. Es wird eine Unternehmensgründung von der anfänglichen Idee bis zur Gründung eines realisierbaren Unternehmens durchgespielt.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach Abschluss des Praktikums sind Studierende in der Lage
- unternehmerischen Kompetenzen anzuwenden
- einen strukturierten Geschäftsplan zu entwickeln
- einen Demonstrators für ein High-Tech Produkt aufzubauen
- ihre Idee (Pitch) zu präsentieren</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Programmierkenntnisse sind erwünscht</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1104-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Leistungspunkten
Bestehen der Prüfung (100%).</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1104-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Blockchain Projektpraktikum					
Modul Nr. 20-00-1119	**Leistungspunkte** 9 CP	**Arbeitsaufwand** 270 h	**Selbststudium** 180 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1119-pp	Blockchain Projektpraktikum	9	Projekt	6

2 Lerninhalt

Diese Veranstaltung richtet sich an Studierende, die die Vorlesung Cryptocurrencies besucht oder sich anderweitig mit Blockchain-Technologien beschäftigt haben und einige Aspekte dieses Themenkomplexes eingehender verstehen und untersuchen wollen. Sie bietet eine Plattform, um neuartige Anwendungen basierend auf Blockchain Technologie auf ihre Umsetzbarkeit und Sinnhaftigkeit zu überprüfen.

Nach einer Einführung zu den Themen Blockchain Konzepte, Projektmanagement und Blockchain Development, sollen komplexe kryptographische Systeme und Bausteine aus dem Bereich Kryptowährung und Blockchain in Teamarbeit verstanden und in einem dezentralen System implementiert werden. Dabei wird die eigenständige Konzeption eines Projektes gefordert, das im Verlauf der Veranstaltung von den Studierenden geplant und umgesetzt werden soll.

Die Studierenden erhalten in diesem Praktikum erste Erfahrungen mit der Umsetzung eines komplexeren Entwicklungsprojektes.
Im Rahmen des Projektpraktikums erarbeiten die Studierenden weiter fortgeschrittene Konzepte im Bereich Blockchain und Blockchain Entwicklung, wie beispielsweise Performance- und Sicherheitsaspekte, präsentieren diese in der Gruppe und integrieren sie in ihre Anwendung.

3 Qualifikationsziele / Lernergebnisse

Studierende verstehen nach erfolgreichem Besuch der Veranstaltung die technischen und praktischen Implikationen von verteilten kryptographischen Systemen. Dazu gehören zum Beispiel erste Erfahrungen in den folgenden Bereichen:

- Entwicklung von Smart Contracts und verteilten Applikationen
- Kommunikation von Systemen durch dezentrale Peer-to-Peer Netze
- Entwicklung von Software unter Nutzung kryptographischer Bausteine
- Sicherheit und Anonymität von Nutzern von kryptographischen Währungen
- Mögliche Angriffe auf Smart Contracts und Cryptocurrencies

4	**Voraussetzung für die Teilnahme** Empfohlen: Dieser Kurs richtet sich an Studierende mit Interesse und Grundkenntnissen im Bereich Blockchain. Weiterhin sollten gute Programmierkenntnisse, Begeisterung für innovative Ideen und Interesse am strukturierten Bearbeiten komplexer Entwicklungsprojekte vorhanden sein.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1119-pp] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%).
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1119-pp] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Forschungsmethodik in der Kryptographie					
Modul Nr. 20-00-1126	**Leistungspunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1126-pr	Forschungsmethodik in der Kryptographie	6	Praktikum	4

2 Lerninhalt

Die moderne Kryptographie bietet eine Vielzahl von innovativen Werkzeugen und Techniken, die zur Lösung komplexer Sicherheitsprobleme eingesetzt werden können. Ziel der Veranstaltung ist das Erlernen der wissenschaftlichen Methodik der modernen Kryptographie. Dazu soll in einer kleinen Gruppe zusammen mit den Lehrenden eine wissenschaftliche Arbeit in der Kryptographie verfasst werden. Es soll der gesamte Prozess von der initialen Forschungsidee bis zur Einreichung einer Publikation durchlaufen werden. Unter anderem werden Techniken zur Literaturrecherche, Diskussion über Forschungsfragen und das Verfassen von wissenschaftlichen Arbeiten behandelt. Voraussetzung für den Kurs ist die Vorlesung „Einführung in die Kryptographie“. Der Besuch weiterer Spezialveranstaltungen im Bereich Kryptographie und IT Sicherheit ist von Vorteil. Insbesondere sollten Teilnehmer mit den Grundtechniken der modernen Kryptographie vertraut sein (kryptographische Bausteine, Sicherheitsdefinitionen, Reduktionsbeweise).

3 Qualifikationsziele / Lernergebnisse

Lernergebnis:

- Verfassen von wissenschaftlichen Arbeiten in der Kryptographie
- Erlernen von fortgeschrittenen Techniken der modernen Kryptographie
- Durchführen von Literaturrecherche in der Kryptographie

4 Voraussetzung für die Teilnahme

Die Vorlesung „Einführung in die Kryptographie“ wird empfohlen.

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1126-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

	Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%).
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1126-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Projektpraktikum - Systematische Analyse und Entwicklung von innovativen Systeme</td></tr>
<tr><td>Modul Nr.
20-00-1137</td><td>Leistungspunkte
9 CP</td><td>Arbeitsaufwand
270 h</td><td>Selbststudium
180 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1137-pp</td><td>Projektpraktikum - Systematische Analyse und Entwicklung von innovativen Systeme</td><td>9</td><td>Projekt</td><td>6</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Diese Veranstaltung behandelt aktuelle Themen aus der Forschung und Entwicklung mit Schwerpunkt auf Sicherheit.

Analysieren und Entwickeln von Sicherheitslösungen sind komplexe Aufgaben, die Kenntnisse aus unterschiedlichen Gebieten der Informatik voraussetzen. Das Ziel dieser Veranstaltung ist es Kompetenzen aus unterschiedlichen Bereichen im Rahmen eines Projekts aus dem Sicherheitsbereich zu vereinen.

Im Rahmen dieser Veranstaltung, werden Aufgaben aus einem sehr breiten Spektrum (von Algorithmik, Raumfahrt, und maschinellem Lernen bis hin zur Softwareanalyse, Hardwareentwicklung und Reverse Engineering) präsentiert.
Die endgültigen Aufgaben werden individuell und entsprechend der Interessen/Kompetenzen der Teilnehmer festgelegt.

Abhängig von dem Umfang und dem Niveau der Aufgabe, wird diese Veranstaltung als Praktikum (InoSys-Lab mit 6CP) oder als Projektpraktikum (InoSys-Projekt mit 9CP) zu absolvieren sein. Diese Art wird individuell und aufgabenspezifisch festgelegt. Bei der Wahl zwischen beiden Arten, und sofern wie die Natur der Aufgabe es erlaubt, bekommen die Studierenden die Möglichkeit sich intellektuell in der Gestaltung der Aufgabe beteiligen.

Bemerkung:
- Abhängig vom Thema, werden die Teilnehmer die Gelegenheit/Unterstützung in/beim Erwerben neuer Kompetenzen erhalten.
- Gruppenarbeit wird zwar bevorzugt und stark empfohlen jedoch ist eine Einzelteilnahme auch möglich.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreichem Absolvieren dieser Veranstaltung haben die Studierenden praxis/forschungsnahe Erfahrungen in Analysieren und Entwicklung von komplexen</td></tr>
</table>

	Projekten gesammelt. Sie werden in der Lage sein diese Erfahrungen zu reproduzieren und Projekte von vergleichbarer Komplexität eigenständig zum Erfolg führen.
4	**Voraussetzung für die Teilnahme** Die Anforderungen sind aufgabenabhängig und werden bei der Einführungsveranstaltung bekannt gegeben.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1137-pp] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%).
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1137-pp] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Praktikum - Systematische Analyse und Entwicklung von innovativen Systeme</td></tr>
<tr><td>Modul Nr.
20-00-1138</td><td>Leistungspunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1138-pr</td><td>Praktikum - Systematische Analyse und Entwicklung von innovativen Systeme</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Diese Veranstaltung behandelt aktuelle Themen aus der Forschung und Entwicklung mit Schwerpunkt auf Sicherheit.

Analysieren und Entwickeln von Sicherheitslösungen sind komplexe Aufgaben, die Kenntnisse aus unterschiedlichen Gebieten der Informatik voraussetzen. Das Ziel dieser Veranstaltung ist es Kompetenzen aus unterschiedlichen Bereichen im Rahmen eines Projekts aus dem Sicherheitsbereich zu vereinen.

Im Rahmen dieser Veranstaltung, werden Aufgaben aus einem sehr breiten Spektrum (von Algorithmik, Raumfahrt, und maschinellem Lernen bis hin zur Softwareanalyse, Hardwareentwicklung und Reverse Engineering) präsentiert.
Die endgültigen Aufgaben werden individuell und entsprechend der Interessen/Kompetenzen der Teilnehmer festgelegt.

Abhängig von dem Umfang und dem Niveau der Aufgabe, wird diese Veranstaltung als Praktikum (InoSys-Lab mit 6CP) oder als Projektpraktikum (InoSys-Projekt mit 9CP) zu absolvieren sein. Diese Art wird individuell und aufgabenspezifisch festgelegt. Bei der Wahl zwischen beiden Arten, und sofern wie die Natur der Aufgabe es erlaubt, bekommen die Studierenden die Möglichkeit sich intellektuell in der Gestaltung der Aufgabe beteiligen.

Bemerkung:
- Abhängig vom Thema, werden die Teilnehmer die Gelegenheit/Unterstützung in/beim Erwerben neuer Kompetenzen erhalten.
- Gruppenarbeit wird zwar bevorzugt und stark empfohlen jedoch ist eine Einzelteilnahme auch möglich.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreichem Absolvieren dieser Veranstaltung haben die Studierenden praxis/forschungsnahe Erfahrungen in Analysieren und Entwicklung von komplexen Projekten gesammelt. Sie werden in der Lage sein diese Erfahrungen zu reproduzieren</td></tr>
</table>

	und Projekte von vergleichbarer Komplexität eigenständig zum Erfolg führen.
4	**Voraussetzung für die Teilnahme** Die Anforderungen sind aufgabenabhängig und werden bei der Einführungsveranstaltung bekannt gegeben.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1138-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Bericht (optional: einschließlich der Abgabe von Quellcode), Kolloquium (optional: einschließlich Präsentation)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%).
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1138-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulhandbuch
M. Sc. IT Security

Wahlbereich Studienbegleitende Leistungen

Seminare

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Forschungsseminar zu Netzen, Sicherheit, Mobilität und Drahtloser Kommunikation</td></tr>
<tr><td>Modul Nr.
20-00-0549</td><td>Leistungspunkte
4 CP</td><td>Arbeitsaufwand
120 h</td><td>Selbststudium
75 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0549-se</td><td>Forschungsseminar zu Netzen, Sicherheit, Mobilität und Drahtloser Kommunikation</td><td>4</td><td>Seminar</td><td>3</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Das Forschungsseminar zu Netzen, Sicherheit, Mobilität und Drahtloser Kommunikation erarbeitet aktuelle Fragstellungen, die als hoch-relevant für die zukünftige Entwicklung der genannten Themenfelder eingeschätzt werden. Es umfasst das Studium, die kritische Analyse und Diskussion, das Zusammenfassen und die Präsentation ausgewählter erstklassiger Forschungsbeiträge. Ein Einblick in wissenschaftliche Arbeitsweise wird vermittelt. Ein Kurzreferat und ein abschließendes Referat sowie eine schriftliche Ausarbeitung werden erstellt.
Die Themen des Forschungsseminars speisen sich aus den aktuellen Forschungsthemen der Arbeitsgruppe SEEMOO.

Lernziele:
- Eigenständiges Einarbeiten in ein Thema auf dem Gebiet Kommunikationsnetze, Sicherheit, Mobilität und Drahtloser Kommunikation (i.d.R. englischsprachig)
- Eigene darüber hinausgehende Literaturrecherchen
- Interpretation und Einordnen der Ergebnisse der Literaturarbeit
- Erstellen eines einführenden und eines vertiefenden Vortrags über die Thematik einschließlich Folienpräsentationen
- Halten der beiden Vorträge vor einem Publikum mit heterogenem Vorwissen
- Fachdiskussion nach jedem Vortrag
- Feedback an die Vortragenden zu den Vorträgen (u.a. betreffend Rhetorik, Präsentationstechniken) und zur Fachdiskussion
- Kennen des wissenschaftlichen Arbeitsprozesses und Publikationsprozesses</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung besitzen die Studierenden die Fähigkeit selbstständig wissenschaftlich neue Themen zu erschließen. Sie haben ein tiefgreifendes Verständnis ausgewählter Basismechanismen, Methoden und Anwendungen in dem</td></tr>
</table>

	bearbeiteten Themenfeld erworben. Arbeitstechniken wie ausführliche Literaturrecherche, kritische Diskussion und Analyse wissenschaftlicher Artikel und die Presentation der erzielten Arbeitsergebnisse werden von den Studierenden beherrscht. Die Studierenden können ihre Arbeit vor einem kritischen Fachpublikum verteidigen.
4	**Voraussetzung für die Teilnahme** Empfohlen: Erfolgreiche Teilnahme an einer integrierten Veranstaltung des Fachgebiets SEEMOO
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0549-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0549-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Themenspezifisch ausgewählte, aktuelle wissenschaftliche Veröffentlichungen
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Seminar zu Netzen, Sicherheit, Mobilität und Drahtloser Kommunikation</td></tr>
<tr><td>Modul Nr.
20-00-0582</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0582-se</td><td>Seminar zu Netzen, Sicherheit, Mobilität und Drahtloser Kommunikation</td><td>3</td><td>Seminar</td><td>2</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Das Seminar zu Netzen, Sicherheit, Mobilität und Drahtloser Kommunikation erarbeitet aktuelle Fragestellungen auf den genannten Gebieten. Unter Anleitung der Dozenten umfasst es das Studium, die kritische Analyse und Diskussion, das Zusammenfassen und die Präsentation ausgewählter Forschungsbeiträge. Ein Kurzreferat und ein abschließendes Referat sowie eine schriftliche Ausarbeitung werden erstellt.
Die Themen des Seminars speisen sich aus den aktuellen Forschungsthemen der Arbeitsgruppe SEEMOO.
Lernziele:
- Eigenständiges Einarbeiten in ein Thema auf dem Gebiet Kommunikationsnetze, Sicherheit, Mobilität und Drahtloser Kommunikation (i.d.R. englischsprachig)
- Darüber hinausgehende Literaturrecherchen, angeleitet von Betreuer
- Interpretation und Einordnen der Ergebnisse der Literaturarbeit, angeleitet von Betreuer
- Erstellen eines einführenden und eines vertiefenden Vortrags über die Thematik einschließlich Folienpräsentationen, angeleitet von Betreuer
- Halten der beiden Vorträge vor einem Publikum mit heterogenem Vorwissen
- Fachdiskussion nach jedem Vortrag
- Feedback an die Vortragenden zu den Vorträgen (u.a. betreffend Rhetorik, Präsentationstechniken) und zur Fachdiskussion</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung besitzen die Studierenden die Fähigkeit unter Anleitung wissenschaftlich zu arbeiten. Sie kennen die grundlegenden Techniken der wissenschaftlichen Literaturarbeit und können diese für ein definiertes Thema anwenden. Sie haben ein mitteltiefes Verständnis ausgewählter Basismechanismen, Methoden und Anwendungen in dem bearbeiteten Themenfeld. Die Studierenden können dieses erworbene</td></tr>
</table>

	Wissen einem heterogenen Publikum verständlich präsentieren und die technischen Details des bearbeiteten Themas erläutern.
4	**Voraussetzung für die Teilnahme** Empfohlen: Erfolgreiche Teilnahme an einer Integrierten Veranstaltung des Fachgebiets SEEMOO
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0582-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0582-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Themenspezifisch ausgewählte, aktuelle wissenschaftliche Veröffentlichungen
10	**Kommentar**

Modulbeschreibung

Modulname

Seminar - Softwaresicherheit für mobile Endgeräte

Modul Nr.	Leistungspunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-0641	3 CP	90 h	60 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Englisch	Koordinatoren/Koordinatorinnen IT Security

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0641-se	Seminar - Softwaresicherheit für mobile Endgeräte	3	Seminar	2

2 Lerninhalt

Das Ziel dieses Seminars ist eine Verbindung zwischen zwei aktuellen Themen herzustellen: Das erste Thema betrifft Sicherheit-Lösungen und bekannte Schwachstellen auf modernen mobilen Endgeräten. Das zweite Thema ist die Programm-Analyse für Low-Level-Sprachen, z.B. Java oder Android Dalvik Bytecode. Neuere Forschungsartikel aus diesen beiden Bereichen werden im Seminar präsentiert. Ein Teil des Seminars wird in Form einer Diskussion stattfinden, wie Techniken aus dem Bereich Programm-Analyse helfen können, die Sicherheit auf mobilen Geräten zu verbessern.

3 Qualifikationsziele / Lernergebnisse

Kenntnisse von Methoden und aktuellen Forschungsfragestellungen bzgl. Software-Sicherheit für mobile Endgeräte; Verbesserung der Fähigkeiten zum Lesen und Verstehen wissenschaftlicher Artikel; Fähigkeit wissenschaftliche Ergebnisse als solche zu erkennen und inhaltlich zu bewerten; Fähigkeit über wissenschaftliche Arbeiten und Ergebnisse schriftlich zu berichten; Verbesserung der Fähigkeit zum Präsentieren und Diskutieren wissenschaftlicher Projekte und Ergebnisse

4 Voraussetzung für die Teilnahme

Empfohlen:

Programmierkenntnisse in Java. Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiums Informatik, insbesondere die Fähigkeit, mit formalen Sprachen und Kalkülen umzugehen.

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-0641-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

	Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0641-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Mobile Security</td></tr>
<tr><td>Modul Nr.
20-00-0652</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0652-se</td><td>Mobile Security</td><td>3</td><td>Seminar</td><td>2</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
In diesem Seminar werden verschiedene Sicherheitsaspekte von mobilen Endgeräten (mit Fokus auf Smartphones) analysiert und diskutiert. Die Studenten werden eine Anzahl aktueller wissenschaftlicher Publikationen zu einem bestimmten Thema in Form einer Seminararbeit zusammenfassen, vergleichen und bewerten. Zusätzlich wird jeder Teilnehmer am Ende des Semsters seine Seminararbeit vorstellen.
Mögliche Themen sind unter anderem:
● Sicherheitsmodelle von aktuellen mobilen Betriebssystemen (z.B. Android, iOS, Windows Phone, MeeGo, Symbian, RIM)
● Sicherheitsanalyse und Vergleich von aktuellen App Store Modellen
● Mobile Endgeräte im Unternehmenseinsatz
● Sicherheitserweiterungen für Android
● Kernel Sicherheit
● Applikationssicherheit (z.B. mobile Malware und Laufzeitangriffe)
● Datenschutz-relevante Aspekte von mobilen Endgeräten
● Sicherheit von mobilen Netzwerken</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Dieses Seminar behandelt verschieden Themen aus dem Bereich mobiler Sicherheit mit Fokus auf Smartphones. Durch die erfolgreiche Teilnahme erhalten Studierende detaillierte Kenntnisse über Sicherheit und Datenschutz in mobilen Betriebssystemen, Geräten, Infrastrukturen und Anwendungen. Außerdem lernen sie sich in aktuelle wissenschaftliche Themengebiete einzuarbeiten und ihre Ergebnisse sowohl schriftlich als auch mündlich zu präsentieren.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme</td></tr>
</table>

	Empfohlen: Grundlagen der Informatik
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0652-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0652-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Wird in der Veranstaltung bekannt gegeben
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Aktuelle Themen zu Secure Usage</td></tr>
<tr><td>Modul Nr.
20-00-0712</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0712-se</td><td>Aktuelle Themen zu Secure Usage</td><td>3</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Bei der Verarbeitung vertraulicher Daten müssen üblicherweise Regularien beachtet werden, die den Zugriff auf Daten einschränken und kontrollieren. Eine Art, solche Regularien zu formulieren, sind Richtlinien zur Zugriffskontrolle (z. B. Chinese Wall). Nutzungsrichtlinien gehen über Kontrollrichtlinien hinaus, indem sie nicht nur die Zugriffsrechte einschränken, sondern auch die Nutzungsbedingungen (z. B. für welchen Zweck, wie oft, in welchem Zeitraum?). Zur Durchsetzung derartiger Regularien werden geeignete Mechanismen benötigt, insbesondere im Kontext von nicht vertrauenswürdigem Code.

In diesem Seminar werden aktuelle Forschungsartikel präsentiert, die sich mit Sprachen für Sicherheitsrichtlinien, statischer Verifikation für Richtlinienkonformität und Durchsetzungsmechanismen zur Laufzeit befassen.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Kenntnisse von Methoden und aktuellen Forschungsfragestellungen zum Thema Nutzungskontrolle; Verbesserung der Fähigkeiten zum Lesen und Verstehen wissenschaftlicher Artikel; Fähigkeit wissenschaftliche Ergebnisse als solche zu erkennen und inhaltlich zu bewerten; Fähigkeit über wissenschaftliche Arbeiten und Ergebnisse schriftlich zu berichten; Verbesserung der Fähigkeit zum Präsentieren und Diskutieren wissenschaftlicher Projekte und Ergebnisse</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiums Informatik, insbesondere die Fähigkeit, mit formalen Sprachen und Kalkülen umzugehen.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-0712-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0712-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Cyber Security Seminar</td></tr>
<tr><td>Modul Nr.
20-00-0756</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0756-se</td><td>Cyber Security Seminar</td><td>3</td><td>Seminar</td><td>2</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Cyber-Sicherheit ist maßgeblich, um aktuelle Verfügbarkeit und Stabilität sicherzustellen, nicht nur von Internet-Anwendungen und Dienstleistungen, sondern auch von einer breiten Palette von Systemen, die mit dem Internet verbunden sind, wie Kraftwerke, Wasserversorgung und mehr. Zentral für Cyber-Sicherheit sind „Advanced Persistent Threat“ (APT) Attacken. APT-Angriffe sind in der Regel aus einer Reihe von Schwachstellen, welche auf eine raffinierte Weise kombiniert sind.
In diesem Seminar untersuchen wir die Grundbausteine, welche die APT-Attacken sowie die Techniken und Methoden verwenden, um diese anzuwenden. Insbesondere werden wir Themen behandeln wie: Sicheres Routing, anonyme Kommunikation, Malware und Botnets, Cloud-Sicherheit, die Sicherheit von Netzwerktechnologien (SDN und andere), Datenschutz, Sicherheit in Sozialen Netzwerken, Denial-of-Service, Angriffe auf wichtige kryptographische Protokolle, verdeckte Kommunikation, SCADA Sicherheit (Steuerungsnetzwerke) und Funk-Sicherheit.
Das Seminar wird die Erkennung und Vermeidung solcher Angriffe untersuchen sowie in einem kooperativen Ansatz die Erkennung von Angriffen betrachten. Wir werden dabei aktuelle (vorgegebene) Forschungsergebnisse im Bereich Cyber-Sicherheit und APTs diskutieren.
Studenten wählen ein Paper aus einer demnächst auf dieser Seite verfügbaren Liste. Sie können auch ein anderes Paper vorschlagen, solange es innerhalb der Bandbreite dieses Seminars liegt und vom Dozenten zugelassen wird. Die Veröffentlichungen stammen meistens aus führenden Sicherheitskonferenzen (IEEE Security and Privacy, ACM CCS, Usenix Security, Esorics, NDSS) und Zeitschriften (ACM TISSEC, IEEE TDSC).
Jeder Student soll mit dem Dozent per E-Mail (auf FCFS Basis) einen Termin für die Vorstellung des Papers sowie einen Vortrag vereinbaren. Eine Woche vor der Präsentation sendet der Student eine Kurzfassung sowie die Präsentationsfolien an den Dozenten; anhand dieser erläutert der Student sein Paper den anderen Seminarteilnehmern und diskutiert es mit Ihnen.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse</td></tr>
</table>

	Nach erfolgreicher Teilnahme an der Veranstaltung können die Studierenden sich eigenständig in ein Thema anhand von wissenschaftlichen Veröffentlichungen einarbeiten. Sie sind mit den verschiedenen Techniken der Literaturrecherche vertraut. Sie können über mehrere wissenschaftliche Arbeiten hinweg Techniken vergleichen und Forschungsergebnisse übergreifend evaluieren. Sie können die wesentlichen Aspekte der untersuchten Arbeiten erkennen und diese kompakt einem Publikum mit heterogenem Vorwissensstand vortragen, wobei sie dabei effektiv verschiedene Präsentationstechniken anwenden. Nach dem Vortrag können die Vortragenden aktiv eine Fachdiskussion zu dem von ihnen präsentierten Thema bestreiten.
4	**Voraussetzung für die Teilnahme** Empfohlen: Kenntnisse in Networking, Sicherheit, Kryptographie
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0756-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0756-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Eine erste Liste der Themen wird noch zum Beginn des neuen Semesters bekanntgegeben. Eigene Themen können ebenso vorgeschlagen werden.
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Seminar: Aktuelle Werkzeuge für sprachbasierte Sicherheit</td></tr>
<tr><td>Modul Nr.
20-00-0779</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0779-se</td><td>Seminar: Aktuelle Werkzeuge für sprachbasierte Sicherheit</td><td>3</td><td>Seminar</td><td>2</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
● Eigenständiges Einarbeiten in ein aktuelles Thema aus dem Bereich Werkzeuge für sprachbasierte Sicherheit anhand von bereitgestellten wissenschaftlichen Arbeiten (englischsprachig)
● Eigene darüber hinausgehende Literaturrecherchen, angeleitet durch Betreuer
● Reflektion und Einordnen der Ergebnisse der Literaturarbeit, angeleitet von Betreuer
● Erstellen eines Vortrags über die Thematik einschließlich Folienpräsentationen, angeleitet durch Betreuer
● Halten des Vortrags vor einem Publikum mit heterogenem Vorwissen
● Fachdiskussion basierend auf dem Vortrag
● Feedback an die Vortragenden zu den Vorträgen (betreffend u.a. Rhetorik, Präsentationstechnik) und zur Fachdiskussion</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung können die Studierenden sich eigenständig in ein aktuelles Thema anhand von wissenschaftlichen Veröffentlichungen einarbeiten. Sie sind mit den verschiedenen Techniken der Literaturrecherche vertraut. Sie können über mehrere wissenschaftliche Arbeiten hinweg Techniken vergleichen und Forschungsergebnisse übergreifend evaluieren. Sie können die wesentlichen Aspekte der untersuchten Arbeiten erkennen und diese kompakt einem Publikum mit heterogenem Vorwissensstand vortragen, wobei sie dabei effektiv verschiedene Präsentationstechniken anwenden. Nach dem Vortrag können die Vortragenden aktiv eine Fachdiskussion zu dem von ihnen präsentierten Thema bestreiten.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiengangs Informatik, insbesondere grundlegende Logikkenntnisse und Fähigkeit mit formalen Sprachen und Kalkülen umzugehen</td></tr>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0779-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0779-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Wird jeweils passend zu den aktuellen Themen bekanntgegeben
10	**Kommentar**

Modulbeschreibung

Modulname Seitenkanalangriffe gegen Software					
Modul Nr. 20-00-0798	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0798-se	Seitenkanalangriffe gegen Software	3	Seminar	2

2 Lerninhalt

In diesem Seminar sollen Forschungsartikel bezüglich verschiedener Aspekte von Seitenkanalangriffen gegen Software sowie entschpechender Gegenmaßnahmen diskutiert werden; so beispielsweise:

- Seitenkanalangriffe gegen kryptographische Software,
- Seitenkanalangriffe gegen Webanwendungen,
- Seitenkanalangriffe gegen Betriebssysteme,
- Seitenkanalangriffe auf mobile Endgeräte,
- Seitenkanalangriffe in der Cloud.

Seitenkanäle sind indirekte, unbeabsichtigte Informationsflüsse, die durch die physikalische Ausführung eines Computerprogramms aufgedeckt werden. Beispiele hierfür sind Programmlaufzeit, Cache-Verhalten, Stromverbrauch, elektromagnetische Ausstrahlung usw. Da solche unbeabsichtigte Informationsflüsse mit geheimen Dateien wie z. B. privaten kryptographischen Schlüsseln korrelieren können, stellen Seitenkanäle ernste Sicherheitsschwachstellen dar. Während eines Seitenkanalangriffs ist der Hacker in der Lage, durch den Seitenkanal aufgedeckte Informationen zu sammeln, sie zu analysieren und anhand dieser Analyse die geheimen Dateien zu rekonstruieren. Da es dank neuer Sicherheitsmechanismen fortwährend schwieriger wird, herkömmliche Sicherheitsschwachstellen wie z. B. Programmfehler auszunutzen, werden Seitenkanäle für Hacker immer interessanter.

3 Qualifikationsziele / Lernergebnisse

Nach erfolgreicher Teilnahme an diesem Seminar kennen die Studierenden das Konzept von Seitenkanalangriffen gegen Software sowie dazugehörige Beispiele. Sie verstehen die Ernsthaftigkeit der Problematik von Seitenkanälen sowie deren Verbreitung. Die Studierenden verbessern ihre Fähigkeit zum Lesen und Verstehen wissenschaftlicher Artikel, dem Präsentieren wissenschaftlicher Ergebnisse sowie zur Diskussion und Vergleich der Ansätze.

4 Voraussetzung für die Teilnahme

	Empfohlen: Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiengangs Informatik
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0798-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0798-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Privatheit & Anonymität in einer vernetzten Welt					
Modul Nr. 20-00-0807	**Leistungspunkte** 4 CP	**Arbeitsaufwand** 120 h	**Selbststudium** 75 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0807-se	Privatheit & Anonymität in einer vernetzten Welt	4	Seminar	3

2 Lerninhalt

Im Rahmen dieses Seminars werden Privatsphäre und Sicherheit sowie Auswirkungen entstehender Technologien wie das „Internet der Dinge“ diskutiert. Insbesondere werden neue Bedrohungen sowie verschiedene Angriffstechniken und entsprechende Gegenmaßnahmen betrachtet. Beispiele von Themen sind: wearable privacy, smart cars privacy, device fingerprinting, in-store tracking, HTTP(s) Traffic analysis, privacy leaks in Android-Geräte, data anonymization und differential privacy, transparency-enhancing technologies. Die Seminarteilnehmer bekommen ein Thema zugewiesen, sollen aktuelle Forschungsarbeiten lesen, den weiteren Teilnehmern vorstellen und in einer Seminararbeit zusammenfassen. Das primäre Ziel des Seminars ist es, die Fähigkeit der Studenten zu verbessern, ein wissenschaftliches Thema zu bearbeiten, eine Präsentation ähnlich wie bei einer wissenschaftlichen Konferenz zu halten und eine wissenschaftliche Diskussion zu ausgewählten Privacy-Forschungsthemen (mit-) zu gestalten. Die Studierenden simulieren die verschiedenen Phasen einer wissenschaftlichen Konferenz: Einreichung der Arbeiten, Begutachtung der Arbeiten, Feedback, Einreichung der finalen Version, Präsentation des Papiers und ggf. Sitzungsleitung.

3 Qualifikationsziele / Lernergebnisse

Das Seminar richtet sich an Bachelor- und Masterstudenten die sich für das Thema Privatheit in der digitalen Welt interessieren. Sie sollten die Bereitschaft mitbringen, neue veröffentliche Forschungsarbeiten zum Thema "Privacy" zu begutachten bzw. zu diskutieren.

4 Voraussetzung für die Teilnahme

Grundlegendes Verständnis der Computer-Sicherheit und Netzwerkprotokolle könnte hilfreich sein.

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-0807-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0807-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Grundlagen der Computersicherheit					
Modul Nr. 20-00-0925	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0925-se	Grundlagen der Computersicherheit	3	Seminar	2

2 Lerninhalt

In diesem Seminar sollen Forschungsartikel bezüglich verschiedener Aspekte von Computersicherheit und deren Grundlagen diskutiert werden; die Forschungsartikel behandeln beispielsweise:

- Sicherheitsmodelle und Sicherheitseigenschaften,
- Angriffe und Angreifermodelle,
- Komposition, Abstraktion und Verfeinerung im Kontext von Computersicherheit
- Verifizierbare Sicherheit,
- Quantifizierte Sicherheit,
- Zugriffskontrolle und Verwendungskontrolle,
- Sicherheitsmodelle und Sicherheitseigenschaften
- Informationsflusskontrolle, und
- Sprach-basierte Sicherheit.

Die Grundlagen der Computersicherheit umfassen Theorien von Computersicherheit, formale Modelle für diese Theorien und Techniken zur Verifikation von Computersicherheit. Dabei erleichtern Theorien das konzeptuelle Verständnis für Computersicherheit und für Bedrohungen der Computersicherheit. Basierend auf diesem Verständnis bieten formale Modelle ein Gerüst für die Spezifikation der gewünschten Sicherheitseigenschaften, für die Definition des betrachteten Systems und für die eindeutige Definition der Annahmen an die Systemumgebung. Schließlich kann die Erfüllung der spezifizierten Sicherheitseigenschaften durch eine Implementierung des Systems mit Hilfe von Techniken zur Verifikation sicher gestellt werden.

3 Qualifikationsziele / Lernergebnisse

Nach erfolgreicher Teilnahme an diesem Seminar werden die Studierenden fähig sein aktuelle Entwicklungen in den Grundlagen der Computersicherheit mit Bezug zu formalen Methoden zu diskutieren. Des Weiteren, werden die Studierenden ihre Fähigkeit im Lesen und Verstehen wissenschaftlicher Artikel, im Präsentieren wissenschaftlicher Ergebnisse und im Diskutieren und Vergleichen formaler Ansätze der Computersicherheit und derer Implementierung verbessern.

4	**Voraussetzung für die Teilnahme** Empfohlen: Informatikkenntnisse entsprechend der ersten vier Semester des Bachelorstudiengangs Informatik.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0925-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0925-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Privatsphäre-schützende Technologien					
Modul Nr. 20-00-0935	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0935-se	Privatsphäre-schützende Technologien	3	Seminar	2

2 Lerninhalt

Daten sind das Öl des 21. Jahrhunderts und Benutzer hinterlassen immer mehr digitale Spuren, die von Firmen wie Facebook oder Google, sowie von Geheimdiensten zusammengetragen und ausgewertet werden.
In diesem Seminar wollen wir Techniken zum Schutz der Privatsphäre betrachten, die es erlauben sensitive Daten unter Verschlüsselung zu verarbeiten, ohne die Daten selbst Preis zu geben.
Es werden sowohl die theoretischen Hintergründe als auch die praktischen Aspekte solcher Lösungen betrachtet.
Die Studierenden wählen ein Thema und erhalten dazu ein oder zwei Publikationen, die sie in einer Ausarbeitung schriftlich zusammenfassen und in einem Vortrag vorstellen.

Mögliche Themen sind beispielsweise:
- Privatsphäre-schützende biometrische Identifikation
- Privatsphäre-schützende mobile Anwendungen, z.B. für Standort-abhängige Dienste
- Privatsphäre-schützendes Herunterladen von Dateien, z.B. für Medizinische- oder Patent-Datenbanken (Private Information Retrieval)
- Privatsphäre-schützendes Finden gemeinsamer Kontakte oder Kunden (Private Set Intersection)
- Privatsphäre-schützendes Prüfen der Kreditwürdigkeit (Private Function Evaluation)
- Privatsphäre-schützendes Datenbanksystem (Semi-Private Function Evaluation)
- Representation von Funktionen als Daten (Universal Circuits)
- Oblivious RAM in Privatsphären-schützenden Technologien (ORAM + Secure Computation)
- Werkzeuge für Privatsphäre-schützende Anwendungen

3 Qualifikationsziele / Lernergebnisse

Die Studierenden lernen aktuelle und praktikable Techniken zum Schutz der Privatsphäre.

4 Voraussetzung für die Teilnahme

Teilnahme an der Veranstaltung "Einführung in die Kryptographie" ist von Vorteil, aber nicht unbedingt notwendig.

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0935-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0935-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Aktuelle Themen zu Nebenläufigkeit und Parallelität</td></tr>
<tr><td>Modul Nr.
20-00-0960</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0960-se</td><td>Aktuelle Themen zu Nebenläufigkeit und Parallelität</td><td>3</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
In diesem Seminar werden Forschungsartikel zu verschiedenen Aspekten von Nebenläufigkeit und Parallelität diskutiert; die Forschungsartikel behandeln beispielsweise:

- Semantik der Nebenläufigkeit (Interleaving-Sematik, Multicore-Semantik, Weak Memory Models),
- Parallele Architekturen (Grundlagen von parallelen Architekturen, symmetrische Multiprozessorsysteme, Massenparallelrechner),
- Parallele Programmierung (parallele Programmierungsmodelle, Kommunikation, Synchronisation),
- Parallelisierung und Kompilierung (Voll-/Halbautomatische Parallelisierung, Datenabhängigkeiten, Lastverteilung),
- Verifikation von nebenläufigen Programmen (Separation Logic, Rely/Guarantee Reasoning).</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an diesem Seminar werden die Studierenden fähig sein, aktuelle Entwicklungen in den Bereichen Nebenläufigkeit und Parallelität zu diskutieren. Des Weiteren werden die Studierenden ihre Fähigkeiten im Lesen und Verstehen wissenschaftlicher Artikel und im Präsentieren, Diskutieren und Vergleichen wissenschaftlicher Ergebnisse verbessern.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Informatikkenntnisse entsprechend der ersten vier Semester des Bachelorstudiengangs Informatik.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-0960-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0960-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Zivile Sicherheit					
Modul Nr. 20-00-0961	**Leistungspunkte** 4 CP	**Arbeitsaufwand** 120 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0961-se	Zivile Sicherheit	0	Seminar	0

2 Lerninhalt

Unter dem Begriff "zivile Sicherheit" versteht man neben Katastrophenschutz und Terrorismusbekämpfung auch die Aspekte der Sicherheit, die einen direkten Bezug zum Bürger und dessen Alltag aufweisen. Sie ist also auch dann bedroht, wenn der Bürger im täglichen Leben eine latente Unsicherheit hinsichtlich gewöhnlicher Handlungen verspürt.
In dieser Veranstaltung werden drei ausgewählte Szenarien der zivilen Sicherheit adressiert, die einen Bezug zur IT haben: Medikamentenhandel über das Internet, Versicherungsbetrug und Geldwäsche sowie Handel mit Antiken aus Raubgrabungen über das Internet. Dabei sind sowohl die Methoden der Betrüger als auch die der Betrugsaufdeckung von Interesse. Basis für diese Themen sind die BMBF Forschungsprogramme zur Wirtschaftskriminalität und zur organisierten Kriminalität. Es sollen Technologien entwickelt, Dunkelfeldforschung betrieben sowie interdisziplinäre Eigenschaften bezüglich beispielsweise Recht und Wirtschaft betrachtet werden.
Die Veranstaltung kombiniert Vorlesung und Seminar. Zu Beginn wird eine Einführung in die Thematik gegeben, in welcher unter anderem internationale Sicherheitsstrategien, computerisierte Methoden der Aufdeckung von Betrugsfällen und Aspekte des Datenschutzes behandelt werden.
In dem anschließenden Seminar werden einzelne Themen vertieft betrachtet, wie beispielsweise:
• Umschlagplätze für Medikamente im Internet
• Bildmanipulationen als Grundlage für Versicherungsbetrug
• Forensische Erkennung von Identitäten
• Ähnlichkeitssuche: Welche Methoden für Bild und Text werden in der Praxis genutzt
• Wie schützen sich Auktionsplattformen vor illegalen Angeboten?
Die Vertiefung geschieht auf Basis empfohlener Publikationen, von denen ausgehend der Teilnehmer einen Seminarvortrag und eine begleitende Ausarbeitung erstellt und diese mit den übrigen Teilnehmern der Veranstaltung diskutiert.

3 Qualifikationsziele / Lernergebnisse

- Erstellen von wissenschaftlichen Kurzvorträgen
- Verwendung von Zitaten

	- Interdisziplinäre Sicherheitsbetrachtung - Einsatz von Methoden der Betrugserkennung
4	**Voraussetzung für die Teilnahme** Empfohlen: Hilfreich sind Grundkenntnisse in Internettechnologie und IT Security. Für einzelne Seminarthemen werden in der Veranstaltungen weitere Empfehlungen hinsichtlich der Vorkenntnisse ausgesprochen.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0961-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0961-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Aktuelle Themen zu Programmsemantiken</td></tr>
<tr><td>Modul Nr.
20-00-1009</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1009-se</td><td>Aktuelle Themen zu Programmsemantiken</td><td>3</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
In diesem Seminar werden Forschungsartikel zu verschiedenen Aspekten von Programmsemantiken diskutiert. Beispielthemen beinhalten:
- sequentielle Programmsemantiken,
- nebenläufige Programmsemantiken,
- instrumentierte Programmsemantiken,
- Testen von Programmsemantiken, und
- Verifikation basierend auf Programmsemantiken.

Formale Programmsemantiken werden genutzt um ein klares Verständnis von Eigenschaften von Programm zu erreichen. Neben anderen Vorteilen erlauben solche Semantiken das Design und die Implementierung von Programmanalysen, die genutzt werden können um Eigenschaften von Programmen zu verifizieren. Während die höhere Komplexität von Programmiersprachen (z.B. Unterstützung von nebenläufigen und verteilten Systemen) formale Programmsemantiken noch wünschenswerter machen, führt diese Komplexität zu noch größeren Herausforderungen in der Formalisierung von Programmsemantiken.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an diesem Seminar werden die Studierenden fähig sein, aktuelle Entwicklungen im Bereich von Programmsemantiken zu diskutieren. Des Weiteren werden die Studierenden ihre Fähigkeiten im Lesen und Verstehen wissenschaftlicher Artikel und im Präsentieren, Diskutieren und Vergleichen wissenschaftlicher Ergebnisse verbessern.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:Informatik- und Mathematikkenntnisse entsprechend den ersten vier Semestern des Bachelorstudiums Informatik, insbesondere die Fähigkeit, mit formalen Sprachen und Kalkülen umzugehen</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1009-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1009-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Seminar Krisen-, Sicherheits- und Friedenstechnologien					
Modul Nr. 20-00-1019	**Leistungspunkte** 4 CP	**Arbeitsaufwand** 120 h	**Selbststudium** 90 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1019-se	Seminar Krisen-, Sicherheits- und Friedenstechnologien	4	Seminar	2

2 Lerninhalt

Im Seminar werden fortgeschrittene theoretische Themen des Fachgebiets „Wissenschaft und Technik für Frieden und Sicherheit“ (PEASEC) erarbeitet. Basierend auf einer Einführung/Wiederholung der Techniken wissenschaftlichen Arbeitens und einiger Grundlagen werden fortgeschrittene Themen vergeben, die sich an der aktuellen Forschung orientieren. Im Rahmen der Veranstaltung entstehende Arbeiten werden im Anschluss mithilfe eines Review-Verfahrens gegenseitig überprüft und anschließend überarbeitet.
- Grundlagen: Friedens-, Konflikt- und Sicherheitsforschung
o Friedens- und Konfliktforschung
o Sicherheitsforschung und Informationssicherheit
- Informatik in Militär, Krieg und Konflikten
o Militärische Nutzung von Informatik und Dual-Use-Problematik
o Cyberwar: Konflikte im Cyberraum mit Information Warfare, Fake News und Social Bots
o Terrorismus und terroristische Propaganda in sozialen Medien
- Informatik für Frieden
o Mensch-Computer-Interaktion für Cyberpeace und zur Friedensförderung
o IT im Kontext politischer Aktivisten
o Bekämpfung terroristischer Propaganda in sozialen Medien
- Sicherheitskritische Mensch-Computer-Interaktion
o Usable Safety-Engineering sicherheitskritischer interaktiver Systeme
o Recht, Ethik, Kultur
o Betriebliche Informationssysteme
o Krisenmanagementsysteme und Medizintechnik
o Warn- und Assistenzsysteme
o Soziale Medien
o Kooperationssysteme für Einsatzlagen
o Technologien für freiwillige Partizipation
Themen für das aktuelle Semester finden Sie unter www.peasec.de/lehre

3 Qualifikationsziele / Lernergebnisse

Studierende verstehen nach erfolgreichem Besuch der Veranstaltung die technischen und theoretischen Grundkonzepte für Frieden und Sicherheit. Insbesondere lernen sie:
- Grundlagen der Friedens-, Konflikt-, und Sicherheitsforschung aus Blickwinkel der Informatik

	- Herausforderungen der IT-Gestaltung und –Nutzung im Kontext von Frieden und Sicherheit - Methoden zur Entwicklung sicherheitskritischer Mensch-Computer-Interaktion - Selbstständige Auseinandersetzung mit wissenschaftlichen Texten - Verfassen wissenschaftlicher Ausarbeitungen - Begutachtung wissenschaftlicher Texte
4	**Voraussetzung für die Teilnahme** Empfohlen: - Grundlagen der Informatik oder Grundlagen der Konflikt- und Friedensforschung - Offen für Studierende der Informatik - Offen für Internationale Studien/Friedens- und Konfliktforschung (Naturwissenschaftlich-technische Dimension der Friedens- und Konfliktforschung -IS-MA-7) - Offen für Studierende anderer Fachgebiete, Anrechenbarkeit nach Absprache
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1019-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1019-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.

9	**Literatur** Reuter, C. (2018) Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement, 660 S., Wiesbaden: Springer Vieweg – im Druck Altmann, J., Bernhardt, U., Nixdorff, K., Ruhmann, I., & Wöhrle, D. (2016) Naturwissenschaft - Rüstung - Frieden - Basiswissen für die Friedensforschung (Vol. 49), Wiesbaden: Springer Vieweg. Flick, U. (2015) Introducing Research Methodology. Sage Publications Ltd Weitere Literatur wird in der Veranstaltung je nach gewähltem Thema genannt.
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Schutz von verteilten Infrastrukturen und Netzwerken</td></tr>
<tr><td>Modul Nr.
20-00-1022</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1022-se</td><td>Schutz von verteilten Infrastrukturen und Netzwerken</td><td>3</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Das Seminar zum Schutz von verteilten Infrastrukturen und Netzwerken setzt sich aus der strukturierten Arbeit an wissenschaftlichen Veröffentlichungen auseinander. Die Themen befassen sich hierbei mit:
- Vertrauen
- Privatheit
- Resilienz
in Infrastrukturen und Netzwerken.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studenten, die an dem Seminar teilnehmen, haben die Chance die Themen durch strukturierte Forschung, näher kennen zu lernen.
Ihre Aufgabe wird es sein, aktuelle wissenschaftliche Veröffentlichungen zu verstehen, um deren Beitrag zu erklären. Außerdem muss ein Survey über das bearbeitete Thema verfasst werden.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Grundlegendes Verständnis von IT-Sicherheit und verteilten Systemen.

Veranstaltungen:
Computersystemsicherheit
Computer Netze und verteilte Systeme</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1022-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1022-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Seurity Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Seminar Cyber-Sicherheit, -Krieg, und -Frieden					
Modul Nr. 20-00-1024	**Leistungspunkte** 4 CP	**Arbeitsaufwand** 120 h	**Selbststudium** 75 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1024-se	Seminar Cyber-Sicherheit, -Krieg, und -Frieden	4	Seminar	3

2 Lerninhalt

Im Seminar werden fortgeschrittene theoretische Themen des Fachgebiets „Wissenschaft und Technik für Frieden und Sicherheit“ (PEASEC) erarbeitet. Basierend auf einer Einführung/Wiederholung der Techniken wissenschaftlichen Arbeitens und einiger Grundlagen werden fortgeschrittene Themen vergeben, die sich an der aktuellen Forschung orientieren. Im Rahmen der Veranstaltung entstehende Arbeiten werden im Anschluss mithilfe eines Review-Verfahrens gegenseitig überprüft und anschließend überarbeitet.

- Grundlagen: Friedens-, Konflikt- und Sicherheitsforschung
o Friedens- und Konfliktforschung
o Sicherheitsforschung und Informationssicherheit
- Informatik in Militär, Krieg und Konflikten
o Militärische Nutzung von Informatik und Dual-Use-Problematik
o Cyberwar: Konflikte im Cyberspace mit Information Warfare, Fake News und Social Bots
o Terrorismus und terroristische Propaganda in sozialen Medien
- Informatik für Frieden
o Mensch-Computer-Interaktion für Cyberpeace und zur Friedensförderung
o IT im Kontext politischer Aktivisten
o Bekämpfung terroristischer Propaganda in sozialen Medien
- Sicherheitskritische Mensch-Computer-Interaktion
o Usable Safety-Engineering sicherheitskritischer interaktiver Systeme
o Recht, Ethik, Kultur
o Betriebliche Informationssysteme
o Krisenmanagementsysteme und Medizintechnik
o Warn- und Assistenzsysteme
o Soziale Medien
o Kooperationssysteme für Einsatzlagen
o Technologien für freiwillige Partizipation

Themen für das aktuelle Semester finden Sie unter www.peasec.de/lehre

3 Qualifikationsziele / Lernergebnisse

Studierende verstehen nach erfolgreichem Besuch der Veranstaltung die technischen und theoretischen Grundkonzepte für Frieden und Sicherheit. Insbesondere lernen sie:

	- Grundlagen der Friedens-, Konflikt-, und Sicherheitsforschung aus Blickwinkel der Informatik - Herausforderungen der IT-Gestaltung und –Nutzung im Kontext von Frieden und Sicherheit - Methoden zur Entwicklung sicherheitskritischer Mensch-Computer-Interaktion - Selbstständige Auseinandersetzung mit wissenschaftlichen Texten - Verfassen wissenschaftlicher Ausarbeitungen - Begutachtung wissenschaftlicher Texte
4	**Voraussetzung für die Teilnahme** Empfohlen: Grundlagen der Informatik oder Grundlagen der Konflikt- und Friedensforschung
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1024-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1024-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Grundlagen statischer Analysen					
Modul Nr. 20-00-1028	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen Vertiefung Data Science and Engineering		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1028-se	Grundlagen statischer Analysen	3	Seminar	2

2 Lerninhalt

Die Grundlagen statischer Analysen, die zur Implementierung von fortgeschrittenen Qualitäts- und Sicherheitsanalysen gebraucht werden.

Exemplarische Auswahl der Themen:
- Berechnung von Kontrol- und Datenabhängigkeiten in der Gegenwart von unendlichen Schleifen und nicht reduzierbarer Kontrollflussgraphen.
- Slicing von Code
- Identifikation von Schleifen in Machinencode
- Konstruktion von Aufrufgraphen
- Statische Analyse Frameworks (z.B., IDE, IFDS, Reactive Async)
- "Self-Adaptation" und statische Analysen
- Sound(iness)
- Specification Mining

3 Qualifikationsziele / Lernergebnisse

Die Studierenden werden vertraut sein mit den Grundlagen von fortgeschrittenen Analysen und werden in der Lage sein, die Angemessenheit bestimmter Techniken und Algorithmen für konkrete Anwendungsfälle zu beurteilen. Die Studierenden werden weiterhin in der Lage sein fortgeschrittene, technische Themen im Bereich statische Analyse effektiv zu präsentieren.

4 Voraussetzung für die Teilnahme

Das Seminar richtet sich an fortgeschrittene Bachelor- und Masterstudierende. Vertrautheit mit den Grundlagen des Compilerbaus (z.B. SSA Form) ist sehr empfehlenswert.

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1028-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1028-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Sichere Mehrparteienberechnungen</td></tr>
<tr><td>Modul Nr.
20-00-1030</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1030-se</td><td>Sichere Mehrparteienberechnungen</td><td>3</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Mehrparteienberechnungen sind Berechnungen zwischen 2 oder mehr Usern, bei denen jeder User eine Eingabe beiträgt und am Ende alle Benutzer das gleiche Ergebnis berechnen. Im Internet sind solche Berechnungen heutzutage allgegenwärtig: Benutzer und WLAN-Accesspoint haben ein Passwort und möchten einen Schlüssel berechnen, um zukünftige Kommunikation abzusichern. Benutzer einer Kryptowährung wie Bitcoin haben unterschiedliche Versionen aller bisherigen Transaktionen und möchten zusammen herausfinden, welche Version zukünftig verwendet werden soll.

Exemplarische Auswahl der Themen:
- Was ist sichere Mehrparteienberechnung?
- Wie kann man mit blockchains Konsens erreichen?
- Kryptographische Bausteine für sichere Mehrparteienberechnung (Garbled Circuits, blockchain, Oblivious Transfer).
- Sichere Mehrparteienberechnung zur Verhinderung von Seitenkanalangriffen.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Studierenden lernen die theoretischen Grundlagen sicherer Mehrparteienberechnungen und diverse Anwendungsbereiche im Detail kennen. Sie sind in der Lage, einen wissenschaftlichen Artikel aufzuarbeiten und zu präsentieren.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Das Seminar richtet sich an Masterstudierende. Grundlagenvorlesung IT-Sicherheit oder Grundlagenwissen in Kryptografie sind empfehlenswert.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-1030-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1030-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Zero Knowledge Beweissysteme					
Modul Nr. 20-00-1052	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1052-se	Zero Knowledge Beweissysteme	3	Seminar	2

2 Lerninhalt

Zero Knowledge (ZK) Beweise sind Beweissysteme, mit denen ein Prover einem Verifier gegenüber die Wahrheit von Behauptungen wie z.B. "Ich kenne eine Lösung für ein Kreuzworträtsel" beweisen kann, ohne aber die Lösung des Rätsels zu verraten. ZK Beweise finden vielseitige Anwendung in der Kryptographie, beispielsweise im Bereich von sicherer Verschlüsselung und anonymen Kryptowährungen. In diesem Seminar lernen wir verschiedene Arten von ZK Beweissystemen und deren Anwendungsmöglichkeiten kennen.

Exemplarische Auswahl der Themen:
- Was sind ZK Beweise und welche Varianten gibt es?
- Die Fiat-Shamir Transformation und nicht-interaktive Beweissysteme
- Groth-Sahai Beweise
- ZCash
- Succint Arguments of Knowledge (SNARKs) und ihre Anwendungen
- Das Verschlüsselungsverfahren von Naor und Yung

3 Qualifikationsziele / Lernergebnisse

Die Studierenden lernen die theoretischen Grundlagen von Zero Knowledge Beweissystemen und diverse Anwendungsbereiche im Detail kennen. Sie sind in der Lage, einen wissenschaftlichen Artikel aufzuarbeiten und zu präsentieren.

4 Voraussetzung für die Teilnahme

Empfohlen:

Das Seminar richtet sich an Masterstudierende. Grundlagenvorlesung IT-Sicherheit oder Grundlagenwissen in Kryptografie sind empfehlenswert.

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1052-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1052-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Binary Analysis Seminar					
Modul Nr. 20-00-1063	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1063-se	Binary Analysis Seminar	3	Seminar	2

2 Lerninhalt

Thema ist sowohl die Auseinandersetzung mit Programmanalyse von nativem Code (z.B. x86, x64, arm64, ...) als auch das Kennenlernen von Werkzeugen in diesem Bereich.
Die Studenten können ihr Thema aus einem vorgegebenem Themenpool wählen.

Folgende Tätigkeiten sind Teil des Seminars:
- Selbstständige Einarbeitung in ein Themengebiet der Programmanalyse
- Erabeitung der Funktionsweise der Tools im jeweiligen Gebiet
- Erstellung eines Vergleichs der Tools
- Identifikation von Problemstellungen, die mit dem Ansatz gelöst werden können
- Beispielhafte Implementation der identifizierten Problemstellungen

Voraussichtliche Themengebiete:
- Symbolic Execution
- Dynamic Binary Instrumentation
- Recompilation
- Dynamic Taint Analysis
- Fuzzing

3 Qualifikationsziele / Lernergebnisse

Die Veranstaltung vermittelt dem Studierenden ein Grundverständnis der Analyse von nativem Code. Zusätzlich wird durch den Vergleich der Werkzeuge die Fähigkeit des wissenschaftlichen Arbeitens gefördert. Außerdem sammeln die Studierenden praktische Erfahrungen im Umgang mit gängigen Analysewerkzeugen. Die Studierenden sind nach der Veranstaltung in der Lage sich selbstständig in weitere ähnliche und komplexere Themen dieser Art einzuarbeiten.

4 Voraussetzung für die Teilnahme

Empfohlen:

	- Interesse an Programmanalyse, Schwachstellenidentifikation und Exploitation - Programmierkenntnisse in C, C++ und Assembly von Vorteil - Linux Kenntnisse
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1063-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1063-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Aktor-basierte Programmiersprachen						
Modul Nr. 20-00-1074	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1074-se	Aktor-basierte Programmiersprachen	3	Seminar	2

2 Lerninhalt

Im Zentrum des Seminars stehen Aktor-basierte Modellierungs- und Programmiersprachen wie Scala/Akka, ABS, Encore, u.ä.

Teilnehmer_innen dieses Seminars sollen einzelne Vertreter der Aktor-basierten Sprachen vorstellen, die realisierten Konzepte erklären und diskutieren.

3 Qualifikationsziele / Lernergebnisse

* Fähigkeit ein wissenschaftliche Thema aufzuarbeiten und zu präsentieren
* Fähigkeit wissenschaftliche Berichte zu lesen und verwandte Arbeiten zu recherchieren
* Erwerb von Wissen über Aktor-basierte Sprachen und deren Anwendung

4 Voraussetzung für die Teilnahme

Empfohlen: Interesse in Programmiersprachen und verteilten Systemen

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1074-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Kolloquium (optional: einschließlich Präsentation), Hausarbeit

6 Voraussetzung für die Vergabe von Leistungspunkten

Bestehen der Prüfung (100%)

7 Benotung

Bausteinbegleitende Prüfung:

	• [20-00-1074-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Aktuelle Themen zu Modular Verification</td></tr>
<tr><td>Modul Nr.
20-00-1077</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1077-se</td><td>Aktuelle Themen zu Modular Verification</td><td>3</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Bei der Entwicklung von Softwaresystemen spielt Korrektheit eine entscheidende Rolle. Fehler in Softwaresystemen können nicht nur zu erhöhten Kosten führen, sondern im schlimmsten Fall sogar das Leben von Menschen gefährden (z.B. in Flugzeugen, Weltraumfahrzeugen, Nuklearreaktoren, ...). Verifikation von Software ist eine Möglichkeit, die Abwesenheit von Bugs zu zeigen.

Eine Kernfrage hierbei ist, wie man die Skalierbar von formaler Verifikation und Testmethoden für komplexe Systeme sicherstellt. Die Komplexität von Analysen kann von mehrere Faktoren abhängen, z.B. der Größe des Programms oder der Anzahl von parallelen Threads. Modulare Verifikation wirkt dieser Komplexität durch eine Zerlegung der Probelmstellung entgegen. Einzelne Softwarekomponenten werden unabhängig voneinander verifiziert und diese Verifikationsergebnisse werden dann zu Garantien für das gesamte System zusammengesetzt. Die Zusammensetzung von Verifikationsergebnissen muss durch Kompositionalitätsresultate unterstützt werden, damit die modulare Analyse aussagekräftig ist.

In diesem Seminar werden aktuelle Forschungsartikel, die verschiedene Techniken der modularen Verifikation behandeln, präsentiert und im Detail diskutiert.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Studierenden können nach erfolgreicher Durchführung der Veranstaltung ausgewählte Forschungsaktivitäten und -resultaten zu modular Verifikation diskutieren. Des Weiteren werden sie ihre Fähigkeiten im Lesen und Verstehen wissenschaftliche Artikel, im Präsentieren wissenschaftlicher Resultate und im wissenschaftlichen Diskutieren weiterentwickeln.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiums Informatik, insbesondere die Fähigkeit, mit formalen Sprachen und Kalkülen umzugehen.</td></tr>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1077-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1077-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Fortgeschrittene Techniken der Softwareverifikation</td></tr>
<tr><td>Modul Nr.
20-00-1078</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1078-se</td><td>Fortgeschrittene Techniken der Softwareverifikation</td><td>3</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Im Seminar befassen Sie sich mit Themen zu den aktuellen Forschungsinhalten der Arbeitsgruppe Semantik und Verifikation paralleler System. Es werden sowohl klassische als auch aktuelle Forschungsarbeiten im Bereich Softwareverifikation (d.h. Model Checking, Programmanalyse, Testen, etc.) behandelt.

Während des Seminars werden Sie unter Anleitung
- sich auf Basis von vorgegebener und selbst gefundener, wissenschaftlicher Literatur in Ihr Thema einarbeiten
- einen Vortrag über Ihr Thema vorbereiten und vor den anderen Teilnehmern halten, um mit ihnen anschließend über Ihr Thema zu diskutieren,
- eine wissenschaftliche Ausarbeitung verfassen, die einen zusammenfassenden Überblick über Ihr Thema gibt.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreichem Abschluss des Seminars können sich die Studierenden anhand von Ausgangsliteratur eigenständig in ein wissenschaftliches Thema einarbeiten und dieses Thema einem heterogenen Fachpublikum sowohl mündlich als auch schriftlich präsentieren.

Im Detail können die Studierenden Methoden zur Literaturrecherche anwenden und die Relevanz von gefundener Literatur beurteilen. Sie können den wesentlichen Inhalt einer wissenschaftlichen Veröffentlichung ermitteln und diesen kritisch beurteilen. Außerdem sind sie in der Lage verschiedene wissenschaftliche Arbeiten miteinander zu vergleichen. In einem mündlichen Vortrag können die Studierenden ihr Thema und ihre Ergebnisse einem heterogenen Fachpublikum erklären und ihre Ergebnisse vor diesem Publikum verteidigen. Zusätzlich können die Studierenden in einer schriftlichen Ausarbeitung ihr Thema und ihre Ergebnisse beschreiben.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme</td></tr>
</table>

	Empfohlen: Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiengangs Informatik Hilfreich: Besuch einer Veranstaltung des Fachgebietes Semantik und Verifikation paralleler Systeme
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1078-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1078-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Seitenkanalresistente Kryptographie					
Modul Nr. 20-00-1088	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1088-se	Seitenkanalresistente Kryptographie	3	Seminar	2

2 Lerninhalt

Traditionell sind kryptografische Verfahren sicher gegen sogenannte Black-Box-Angriffe. Bei einem Black-Box Angriff nutzt der Angreifer Schwachstellen des kryptographischen Algorithmus aus, um die Sicherheit des Systems zu brechen. Bei praktischen Implementierung der kryptographischen Verfahren sind sogenannte Seitenkanalangriffe eine weitere kritische Sicherheitsbedrohung. Unzählige Beispiele zeigen, dass fast alle heute verwendeten Geräte von Seitenkanalangriffen betroffen sind. Als Paul C. Kocher Ende der neunziger Jahre zeigte, dass die Sicherheit von Smartcards mithilfe von Timing- oder Power-Analyse-Angriffen gebrochen werden kann, wurden zahlreiche weitere Seitenkanalangriffe entdeckt. Vor kurzem haben Beispiele wie Foreshadow gezeigt, dass selbst komplexe Computersysteme anfällig für Seitenkanalangriffe sind.
„Leakage Resilient Cryptography“ ist ein Forschungsbereich der Kryptographie, der diese praktischen Angriffe formalisiert, um formale Methoden zum Nachweis der Sicherheit gegen Seitenkanalangriffe zu verwenden. Insbesondere definiert es neue Sicherheitsmodelle, sogenannte Leakage-Modelle, die Seitenkanalangriffe in die klassischen Sicherheitsmodelle einbeziehen, und entwirft kryptografische Verfahren, die in ihnen nachweislich sicher sind.

3 Qualifikationsziele / Lernergebnisse

Das Ziel des Seminars ist die Vermittlung der einflussreichsten Paper zu Seitenkanalangriffen und Leakage Resilient Kryptographie. Inhalte sind:
- Seitenkanalangriffe (z. B. Power-Analyse-Angriffe, Timing-Angriffe, Foreshadow usw.)
- gängige Gegenmaßnahmen gegen Seitenkanalangriffe (z. B. Kryptographie mit konstanter Zeit, zufällige Ausführung, Maskierungsschemata, algorithmische Gegenmaßnahmen usw.)
- Sicherheitsmodelle in der Leakage Resilient Kryptographie und formale Sicherheitsanalysen von Gegenmaßnahmen für Seitenkanalangriffe

4 Voraussetzung für die Teilnahme

Empfohlen: Das Seminar richtet sich an Master-Studenten.
Grundvorlesung IT-Sicherheit oder Grundkenntnisse in Kryptographie werden empfohlen

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1088-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1088-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Angreifermodelle in der IT-Sicherheit</td></tr>
<tr><td>Modul Nr.
20-00-1091</td><td>Leistungspunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1091-se</td><td>Angreifermodelle in der IT-Sicherheit</td><td>3</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Bei der Einschätzung der Sicherheit von IT Systemen ist es notwendig, die Fähigkeiten und Absichten von potenziellen Angreifern zu berücksichtigen. Der Zweck von Angreifermodellen ist es, die Fähigkeiten, Ziele, oder andere Aspekte von Angreifern explizit zu machen. Formal fundierte Angreifermodelle erlauben es, die Präzision zu erhöhen, Unklarheiten zu vermeiden und eine Basis für automatisierte Sicherheitsanalysen zu schaffen. Sprachen für Angreifermodelle gehen oft mit graphischen Notationen zur Veranschaulichung einher, die das Verstehen der Modelle und den Aufbau von Intuition vereinfacht.

Angreifermodelle genießen eine weite Verbreitung in der industriellen Praxis und sind der Gegenstand von intensiven Forschungsvorhaben. Sicherheitsanalysen, die auf Angreifermodellen aufbauen, sind nicht auf eine Einschätzung des Sicherheitsgrades von Systemen beschränkt, sondern können auch als Grundlage für wirtschaftliche Entscheidungen herangezogen werden, bspw. um den erwarteten Nutzen von Sicherheitsinvestitionen zu maximieren.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an diesem Seminar werden die Studierenden fähig sein, aktuelle Entwicklungen im Bereich Angreifermodelle zu diskutieren. Des Weiteren werden die Studierenden ihre Fähigkeiten im Lesen und Verstehen wissenschaftlicher Artikel und im Präsentieren, Diskutieren und Vergleichen wissenschaftlicher Ergebnisse verbessern.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen werden Informatik- und Mathematikkenntnisse entsprechend den ersten 4 Semestern des Bachelorstudiums Informatik, insbesondere die Fähigkeit, mit formalen Sprachen und Kalkülen umzugehen.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1091-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

	Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1091-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Seminar Informatik, Ethik und Gesellschaft					
Modul Nr. 20-00-1102	**Leistungspunkte** 4 CP	**Arbeitsaufwand** 120 h	**Selbststudium** 75 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1102-se	Seminar Informatik, Ethik und Gesellschaft	4	Seminar	3

2 Lerninhalt

Im Seminar werden fortgeschrittene wissenschaftliche Themen des Fachgebiets „Wissenschaft und Technik für Frieden und Sicherheit“ (PEASEC) bearbeitet. Basierend auf einer Einführung/Wiederholung der Methoden wissenschaftlichen Arbeitens und ausgewählter Grundlagen werden fortgeschrittene Themen vergeben, die sich an der aktuellen Forschung des Fachgebiets orientieren, und von Studierenden mit wissenschaftlichen Methoden bearbeitet werden. Im Laufe des Semesters werden wissenschaftliche Artikel („Paper“) erarbeitet und präsentiert. Wie bei wissenschaftlichen Arbeiten üblich werden diese mithilfe eines studentischen Review-Verfahrens gegenseitig konstruktiv begutachtet und anschließend zur Fertigstellung und Abgabe überarbeitet.

BEISPIELHAFTE THEMENBEREICHE:
- Verantwortung und Ethik in der Informatik (Leitlinien des GI/ACM/VDI, praktische Rolle der Ethik in der Informatik)
- Verantwortung im Design (Responsible Research and Innovation, Wertsensitives Design, Technikfolgenabschätzung, Dual-Use-Assessment, ELSI-Design)
- Privatsphäre, Datenschutz und Überwachung
- Kritische Informatik (Machtstrukturen, Werteauffassungen, politische Dimensionen)
- Autonome Systeme, Künstliche Intelligenz und Verantwortung
- Frieden, Sicherheit, Militärtechnologie und Dual-Use
- Diversität in der Informatik (Barrierefreiheit, Accessibility, Disability, Gender, Aging, Kultur)
- Sprache: Propaganda, Fake News, Trolling und Hate Speech
- Transparenz, Explainable AI, White Box Algorithmen, Gerechte Algorithmen, Steuerbarkeit

3 Qualifikationsziele / Lernergebnisse

Nach Abschluss des Moduls sind Studierende in der Lage,

- ethische und soziale Aspekte der Informatik sowie ihre professionellen ethischen Leitlinien zu beschreiben.
- Lösungsansätze zum ethischen und sozialen Umgang mit Informatik zu nennen.
- Kriterien für gutes wissenschaftliches Arbeiten zu nennen

	- wissenschaftliche Forschungsfragen im Kontext ethischer Aspekte der Informatik zu erarbeiten und unter Anwendung einer wissenschaftlichen Methode zu beantworten - ihr wissenschaftliches Vorgehen reflektiert in einer Fachdiskussion zu verteidigen - wissenschaftliche Beiträge Anderer in einem „Peer-Review“ konstruktiv zu begutachten
4	**Voraussetzung für die Teilnahme** Empfohlen werden Grundlagen in mindestens einem der Bereiche: Informatik, IT-Sicherheit, Mensch-Computer-Interaktion oder Friedens- und Konfliktforschung, Grundkenntnisse in den Themengebieten des Fachgebiets PEASEC
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1102-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%).
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1102-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Seminar Kryptographie						
Modul Nr. 20-00-1103	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1103-se	Seminar Kryptographie	3	Seminar	2

2 Lerninhalt

Im Seminar werden aktuelle Forschungsresultate aus dem Gebiet der Kryptographie von den Studierenden vorgestellt.

3 Qualifikationsziele / Lernergebnisse

Im Bereich der fachlichen und fachlich methodischen Kompetenzen werden die Studierenden nach der Veranstaltung das Vorwissen aus dem Bereich der Kryptographie auf neue wissenschaftliche Arbeiten anwenden können. Im Bereich der kommunikativen Kompetenzen werden die Studierenden dann wissenschaftliche Arbeiten so analysieren können, dass sie den fachlichen Stoff daraus präsentieren können.

4 Voraussetzung für die Teilnahme

Empfohlen werden:

Einführung in die Kryptographie, andere weiterführende Veranstaltungen im Bereich Kryptographie

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1103-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Kolloquium (optional: einschließlich Präsentation), Hausarbeit

6 Voraussetzung für die Vergabe von Leistungspunkten

Bestehen der Prüfung (100%)

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1103-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Verfassen und Beurteilen Wissenschaftlicher Veröffentlichungen in der IT-Sicherheit						
Modul Nr. 20-00-1105	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1105-se	Verfassen und Beurteilen Wissenschaftlicher Veröffentlichungen in der IT-Sicherheit	3	Seminar	2

2 Lerninhalt

Die Studierenden verfassen eine kurze wissenschaftliche Arbeit im Bereich IT-Sicherheit und beurteilen die Arbeiten der anderen in einer konferenz-ähnlichen Umgebung.

3 Qualifikationsziele / Lernergebnisse

Im Bereich der kommunikativen Kompetenzen werden die Studierenden gelernt haben, wie man wissenschaftliche Resultate darstellt und wie man wissenschaftliche Arbeiten bewertet. Im Bereich der organisatorischen Kompetenzen werden sie die Abläufe von Konferenzen und den Einsatz entsprechender Systeme erlernt haben.

4 Voraussetzung für die Teilnahme

Empfohlen: Kenntnisse in IT-Sicherheit, erste Erfahrungen im Verfassen von wissenschaftlichen Arbeiten, z.B. Bachelor-Arbeit

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1105-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Kolloquium (optional: einschließlich Präsentation), Hausarbeit

6 Voraussetzung für die Vergabe von Leistungspunkten

Bestehen der Prüfung (100%).

7 Benotung

Bausteinbegleitende Prüfung:

	• [20-00-1105-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Sicherheit und Privatheit in vernetzten Systemen					
Modul Nr. 20-00-1106	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1106-se	Sicherheit und Privatheit in vernetzten Systemen	3	Seminar	2

2 Lerninhalt

Im Seminar werden fortgeschrittene wissenschaftliche Themen der IT-Sicherheit bearbeitet. Studierende können aus einer Reihe vorgestellter Themen wählen und dieses mit wissenschaftlichen Methoden bearbeiten. Im Laufe des Semesters wird ein eigener wissenschaftlicher Artikel erarbeitet und am Ende präsentiert.

BEISPIELHAFTE THEMENBEREICHE:
• IoT- und Funkprotokolle (u.a. Bluetooth LE, Bluetooth Mesh, LoRaWAN)
• Physical Layer
Security (u.a. Distance Bounding, Direction Finding)
• Eingebettete Systeme
• Software Defined Radio

3 Qualifikationsziele / Lernergebnisse

Am Ende der Veranstaltung sind die Studierenden in der Lage, sich in ein wissenschaftliches Thema einzuarbeiten, den aktuellen Stand der Forschung zu einer bestimmten Fragestellung zu beantworten sowie die Ergebnisse im Stil einer Publikation festzuhalten und zu präsentieren.

4 Voraussetzung für die Teilnahme

Vorwissen im Bereich IT-Sicherheit, beispielsweise durch Besuch entsprechender Lehrveranstaltungen, wird empfohlen.

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1106-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Kolloquium (optional: einschließlich Präsentation), Hausarbeit

6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%).
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1106-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Deduktive und Interaktive Verifikationswerkzeuge					
Modul Nr. 20-00-1128	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1128-se	Deduktive und Interaktive Verifikationswerkzeuge	3	Seminar	2

2 Lerninhalt

In dem Seminar werden aktuelle Verifikationstools und Beweisassistenten vorgestellt.

Es werden dabei sowohl die theoretischen Grundlagen auf denen die Werkzeuge aufbauen vorgestellt, als auch deren praktische Anwendung anhand einer gemeinsamen Beispielsammlung. Damit soll ein Vergleich der unterschiedlichen Ansätze ermöglicht werden.

3 Qualifikationsziele / Lernergebnisse

Nachdem Studierende das Seminar besucht haben, können sie
* sich kritisch mit einer wissenschaftlichen Arbeit auseinandersetzen
* einen wissenschaftlichen Vortrag halten
* Stärken und Schwächen verschiedener Ansätze zur deduktiven Verifikation, des interaktiven Theorembeweisens sowie der existierenden Werkzeuge einschätzen und vergleichen
* Verifikationswerkzeuge auf praktische Problemstellungen anwenden
* einen Überblick über den aktuellen Stand der Forschung im Bereich der deduktiven Verifikation und des interaktiven Beweisen gebe

4 Voraussetzung für die Teilnahme

Empfohlen werden grundlegende Kenntnisse in Logik (Aussagen- und Prädikatenlogik) sowie ein starkes Interesse an deduktiver Verifikation.

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1128-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

	Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%).
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1128-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Aktuelle Forschungstrends der Kryptographie					
Modul Nr. 20-00-1146	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1146-se	Aktuelle Forschungstrends der Kryptographie	3	Seminar	2

2 Lerninhalt

In diesem Seminar werden sich die Studierenden mit aktuellen Forschungstrends in der Kryptographie auseinandersetzen. Insbesondere sollen die Studierenden lernen, eine Forschungsarbeit selbstständig zu lesen, zu verstehen und vor anderen zu präsentieren. Wir fokussieren uns hierbei auf Forschungsarbeiten, die aktuell auf Konferenzen der kryptographischen Forschung vorgestellt werden. Eine Auswahl möglicher Themen sind die folgenden:
1.“Distributed Cryptography” beschäftigt sich mit der Verteilung von kryptografischen Operationen (wie Verschlüsseln oder Signieren) auf eine große Anzahl an Maschinen.
2.“Zero-knowledge proof systems” erlauben es, die Wahrheit einer Aussage zu beweisen, ohne dass Informationen, die über die Aussage selbst hinausgehen, preisgegeben werden.
3.Beweisbar sichere Maßnahmen gegen sogenannte “side-channel attacks”, um Geräte gegen physikalische Attacken wie die Messung von Stromverbrauch oder Laufzeit einer Berechnung zu schützen.
4.“Multiparty Computation" erlaubt mehreren Parteien die Berechnung einer beliebigen Funktion auf privaten Eingaben. Dabei werden keine Informationen außer der Ausgabe der Funktion selbst bekannt gegeben.

3 Qualifikationsziele / Lernergebnisse

Am Ende des Kurses werden die Studierenden in der Lage sein, komplexe Forschungsthemen im Bereich der Kryptographie zu verstehen und anderen Studierenden zu präsentieren. Das Seminar stellt eine ausgezeichnete Vorbereitung für eine Masterarbeit oder eine Promotion im Bereich der Kryptographie dar und bietet einen ersten Einblick in die wissenschaftliche Arbeit an der Universität.

4 Voraussetzung für die Teilnahme

Empfohlen:
vorheriger Besuch von Einführung in die Kryptographie, idealerweise noch weiterer Vorlesungen im Bereich der Kryptographie

5 Prüfungsform

Bausteinbegleitende Prüfung:

	• [20-00-1146-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard) Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen. Kolloquium (optional: einschließlich Präsentation), Hausarbeit
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%).
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1146-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Grundlagen der Post-Quanten Kryptographie						
Modul Nr. 20-00-1149	**Leistungspunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1149-se	Grundlagen der Post-Quanten Kryptographie	3	Seminar	2

2 Lerninhalt

Das Seminar „Grundlagen der Post-Quanten Kryptographie“ beschäftigt sich mit der Sicherheit heutiger kryptographischer Systeme unter Berücksichtigung der Fähigkeiten von Quantencomputern. Dabei werden neben den Fähigkeiten und Grenzen von Quantencomputern verschiedene kryptographische Verfahren aus den Bereichen Hash-, Gitter- und Code-basierte Kryptographie, als auch dem Feld der multivariaten Kryptographie vorgestellt, sowie deren Anwendung in in der Praxis erarbeitet

3 Qualifikationsziele / Lernergebnisse

Nach der Veranstaltung werden die Studierende ein Verständnis der Grundlagen von Gitter-, Hash-, Code-, und Multivariate-basierten kryptographischen Verfahren haben. Weiter werden Sie ein Verständnis von Post-quanten Kryptographie in der Praxis haben.

4 Voraussetzung für die Teilnahme

Empfohlen:
vorheriger Besuch von Einführung in die Kryptographie und solide mathematische Grundkenntnisse

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1149-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Kolloquium (optional: einschließlich Präsentation), Hausarbeit

6 Voraussetzung für die Vergabe von Leistungspunkten

Bestehen der Prüfung (100%).

7 Benotung

	Bausteinbegleitende Prüfung: • [20-00-1149-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulhandbuch
M. Sc. IT Security

Wahlbereich Studienbegleitende Leistungen

Praktikum in der Lehre

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Praktikum in der Lehre - Computersystemsicherheit</td></tr>
<tr><td>Modul Nr.
20-00-0986</td><td>Leistungspunkte
5 CP</td><td>Arbeitsaufwand
150 h</td><td>Selbststudium
105 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0986-pl</td><td>Praktikum in der Lehre – Computersystemsicherheit</td><td>5</td><td>Praktikum in der Lehre</td><td>3</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
- Ausarbeitung neuer Übungs- und Programmieraufgaben
- Konzeption von Übungsblättern</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nachdem Studierende die Veranstaltung besucht haben, können sie Lerninhalte als Übungs- und Programmieraufgaben aufbereiten.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: erfolgreiche Teilnahme an der Lehrveranstaltung "Computersystemsicherheit"</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0986-pl] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Kolloquium (optional: einschließlich Präsentation), Portfolio, Bericht (Optional: einschließlich der Abgabe von Lehrmaterial)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Leistungspunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:
• [20-00-0986-pl] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)</td></tr>
</table>

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Praktikum in der Lehre - Einführung in die Kryptographie</td></tr>
<tr><td>Modul Nr.
20-00-1059</td><td>Leistungspunkte
5 CP</td><td>Arbeitsaufwand
150 h</td><td>Selbststudium
105 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-1059-pl</td><td>Praktikum in der Lehre - Einführung in die Kryptographie</td><td>5</td><td>Praktikum in der Lehre</td><td>3</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Betreuung und Durchführung von Übungen sowie vorlesungsbegleitende Praktika der Vorlesung „Einführung in die Kryptographie“</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende sind in der Lage:

• Lehrinhalte in Übungen zu präsentieren und zu erklären
• Praktikumsgruppen zu betreuuen
• Methoden zur Kontrolle des Lernerfolges systematisch anzuwenden</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfehlung:

• Studierende im Master
• Interesse an Kryptographie
• Bestehen der Vorlesung „Einführung in die Kryptographie“
• Deutsch</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-1059-pl] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Kolloquium (optional: einschließlich Präsentation), Portfolio, Bericht (Optional: einschließlich der Abgabe von Lehrmaterial)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Leistungspunkten
Bestehen der Prüfung (100%)</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1059-pl] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname

Praktikum in der Lehre - Internetsicherheit und Sicherheit in Mobilen Netzen</td></tr>
<tr><td>Modul Nr.
20-00-0957</td><td>Leistungspunkte
5 CP</td><td>Arbeitsaufwand
150 h</td><td>Selbststudium
105 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
Jedes 2. Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT Security</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td>20-00-0957-pl</td><td>Praktikum in der Lehre - Internetsicherheit und Sicherheit in Mobilen Netzen</td><td>5</td><td>Praktikum in der Lehre</td><td>3</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Dieser Kurs befasst sich mit damit Lehrinhalte der Themenschwerpunkte Internetsicherheit und Sicherheit in Mobilen Netzen didaktisch aufzubereiten und durch begleitende praktische Übungen besser verständlich zu machen.

Dies umfasst unter anderem: Die Implementierung von Systemen die in der Vorlesung behandelte Schwachstellen aufweisen und den Studierenden für praktische Übungen verfügbar gemacht werden; die Erstellung von Minitests zur Leistungskontrolle; die Konzeption von Materialien für leistungsschwache wie leistungsstarke Studenten um Inhalte der Vorlesung zu vertiefen; das Erstellen von anspruchsvollen Bonussystemen.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Studierenden können nach erfolgreicher Durchführung der Veranstaltung:
- Lehrinhalte aus der Vorlesung für Haus- und Präsenzübungen aufbereiten
- Praxisnahe Übungsformen konzipieren und erstellen
- Übungen mit Studierendengruppen aller Leistungsniveaus konzipieren und durchführen
- Ein Konzept für aufeinander aufbauende praktische Übungen entwickeln
- Methoden der Lernkontrolle für die Lerninhalte der Vorlesung anwenden</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Erfolgreicher Besuch der SEEMOO Veranstaltung für die das PIDL durchgeführt wird.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-0957-pl] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.</td></tr>
</table>

	Kolloquium (optional: einschließlich Präsentation), Portfolio, Bericht (Optional: einschließlich der Abgabe von Lehrmaterial)
6	**Voraussetzung für die Vergabe von Leistungspunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0957-pl] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. Computer Science M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Praktikum in der Lehre - SIT						
Modul Nr. 20-00-1045	**Leistungspunkte** 5 CP	**Arbeitsaufwand** 150 h	**Selbststudium** 105 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT Security			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1045-pl	Praktikum in der Lehre - SIT	5	Praktikum in der Lehre	3

2 Lerninhalt

Unterstützung der Lehre wie z.B., Betreuung von Übungsgruppen, Sprechstunden, o.ä.

3 Qualifikationsziele / Lernergebnisse

Die Teilnehmer am Praktikum in der Lehre vertiefen ihre Kenntnisse in verschiedenen Bereiche der IT Sicherheit. Zusätzlich erhalten sie Einblicke in die Lehrtätigkeit durch Betreuung von Studierenden und Überarbeitung von Aufgaben.

4 Voraussetzung für die Teilnahme

Empfohlen:
Erfolgreiche Absolvierung der "zugehörigen SIT" Veranstaltung (z.B. Einführung in die IT-Sicherheit beim PidL für die Veranstaltung IT-Sicherheit) oder entsprechende Kenntnisse.

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1045-pl] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Die Form der Prüfung wird zu Beginn der Lehrveranstaltung bekannt gegeben. Möglich ist eine oder eine Kombination von maximal zwei der nachfolgend aufgeführten Formen.

Kolloquium (optional: einschließlich Präsentation), Portfolio, Bericht (Optional: einschließlich der Abgabe von Lehrmaterial)

6 Voraussetzung für die Vergabe von Leistungspunkten

Bestehen der Prüfung (100%)

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1045-pl] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M. Sc. IT Security Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulhandbuch
M. Sc. IT Security

Masterarbeit

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Masterarbeit IT Security</td></tr>
<tr><td>Modul Nr.
20-AM-xxxx</td><td>Leistungspunkte
30 CP</td><td>Arbeitsaufwand
900 h</td><td>Selbststudium
900 h</td><td>Moduldauer</td><td colspan="2">Angebotsturnus
Jedes Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch/Englisch</td><td colspan="4">Modulverantwortliche Person
Studiendekan/Studiendekanin</td></tr>
<tr><td>1</td><td colspan="6">Kurse des Moduls
<table>
<tr><th>Kurs Nr.</th><th>Kursname</th><th>Arbeitsaufwand (CP)</th><th>Lehrform</th><th>SWS</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Selbständige Bearbeitung einer wissenschaftlichen Fragestellung aus dem Bereich der IT Sicherheit nach wissenschaftlichen Grundsätzen in begrenzter Zeit. Die Problemstellung, Vorgehensweise sowie die Ergebnisse werden schriftlich dokumentiert und mündlich in einem Kolloquium präsentiert.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse / Kompetenzen
Die Studierenden sind nach der Masterarbeit in der Lage,
• eine komplexere wissenschaftliche Fragestellung mit Forschungsbezug zur IT Sicherheit nach wissenschaftlichen Grundsätzen selbstständig zu bearbeiten,
• die im Studium erworbenen Kenntnisse, Methoden und Kompetenzen zu verknüpfen und anzuwenden,
• geeignete Methoden und Verfahren auszuwählen, weiterzuentwickeln, erfolgreich anzuwenden und zu evaluieren,
• die relevante Literatur zu recherchieren, einzugrenzen und auszuwerten,
• das Thema sinnvoll zu systematisieren und einen Argumentationsstrang aufzubauen,
• die Validität von Pro- und Kontraargumenten nachvollziehbar abzuwägen,
• die Ergebnisse in die aktuelle Forschung einzuordnen und zu bewerten,
• die Ergebnisse schriftlich nach wissenschaftlichen Grundsätzen niederzulegen,
• die Ergebnisse zu präsentieren und argumentativ zu vertreten.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Thesis</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Leistungspunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard (Ziffernote)</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
M. Sc. IT Security</td></tr>
</table>

9	**Literatur** - Sandberg, Berit: Wissenschaftlich Arbeiten von Abbildung bis Zitat: Lehr- und Übungsbuch für Bachelor, Master und Promotion. De Gruyter Oldenbourg; Auflage: 3, 2017 Ergänzt durch Literatur entsprechend dem Themengebiet der Abschlussarbeit.
10	**Kommentar** Die Abschlussarbeit muss innerhalb von 26 Wochen angefertigt und eingereicht werden. Sie hat einen Arbeitsaufwand von 900 Stunden. Ein Studium in Regelstudienzeit setzt voraus, dass bei Beginn der Masterarbeit im 4. Semester bei voller Ausschöpfung der Bearbeitungszeit von 26 Wochen nicht später als Anfang Februar bei Studienbeginn zum Jedes 2. Semester bzw. Anfang August bei Studienbeginn zum Jedes 2. Semester begonnen werden muss.