Modulhandbuch
M. Sc. IT-Sicherheit

Fachbereich Informatik
Technische Universität Darmstadt

TECHNISCHE UNIVERSITÄT DARMSTADT

Modulhandbuch M. Sc. IT-Sicherheit

Technische Universität Darmstadt

Fachbereich Informatik

Hochschulstr. 10

64289 Darmstadt

Redaktion

Dipl.-Inform. Tim Neubacher

Jasmin Boghrat, M.A.

Stand: 07.04.2021

Inhaltsverzeichnis

Modulhandbuch
M. Sc. IT-Sicherheit

Pflichtbereich

Modulbeschreibung

Modulname Einführung in die Kryptographie					
Modul Nr. 20-00-0085	**Kreditpunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** i.d.R. jedes Wintersemester
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0085-iv	Einführung in die Kryptographie	6	integrierte Lehrveranstaltung	4

2 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

3 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

4 Voraussetzung für die Teilnahme

	Empfohlen: ● Lineare Algebra ● Funktionale und objektorientierte Programmierkonzepte
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Internet- und Web-basierte Systeme M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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
IT-Sicherheit</td></tr>
<tr><td>Modul Nr.
20-00-0219</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>4</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
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard

In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.</td></tr>
</table>

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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
Embedded System Security</td></tr>
<tr><td>Modul Nr.
20-00-0581</td><td>Kreditpunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
135 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>3</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 Studenten 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>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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**

Modulhandbuch
M. Sc. IT-Sicherheit

Wahlbereich
Cryptography

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Public Key Infrastrukturen</td></tr>
<tr><td>Modul Nr.
20-00-0063</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</td></tr>
<tr><td rowspan="2">1</td><td colspan="6">Kurse des Moduls</td></tr>
<tr><td>Kurs Nr.</td><td colspan="2">Kursname</td><td>Arbeitsaufwand (CP)</td><td>Lehrform</td><td>SWS</td></tr>
<tr><td></td><td>20-00-0063-iv</td><td colspan="2">Public Key Infrastrukturen</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
1. Security Goals
1. Confidentiality
2. Integrity
3. Authenticity of Data
4. Entity Authentication/Identification
5. Non-repudiation
6. Availability
7. Other Goals
2. Public Key Cryptography
1. Encryption (symmetric, assymetric, hybrid, cryptosystems, key exchange, performance, security, computational problems)
2. Cryptographic Hash Functions
3. Message Authentication Codes
4. Digital Signatures (performance, standards)
3. Certificates
1. X.509 Public Key Certificates (properties, content, extensions)
2. PGP
3. WAP Certificates
4. Attribute Certificates
4. Trust Models
1. Direct Trust (fingerprints, examples of)
2. Web of Trust (key legitimacy, owner trust, trusted introducers)
3. Use of PGP
4. Hierarchical Trust (trusted list, common root, cross-certification, bridge)
5. Private Keys
1. Software Personal Security Environments (PKCS#12, Java Keystore, application specific)
2. Hardware Personal Security Environments (smart cards, hardware security modules, java cards)
3. Private Key Life-cycle</td></tr>
</table>

	6. Revocation 1. Revocation (reaons for, requirements, criteria) 2. Certificate Revocation Lists 3. Delta Certificate Revocation Lists 4. Other Certificate Revocation Lists (over-issued, indirect, redirect) 5. OCSP 6. Other Revocation Mechanisms (NOVOMODO) 7. Policies 1. Certificate Life-cycle 2. Certificate Policy and Certification Practice Statement 3. Set of Provisions 8. Validity Models 1. Shell Model 2. Modified Shell Model 3. Chain Model 9. Certification Path Validation 10. Trust Center 1. Registration Authority (registration protocols, proof-of-possession, extended validation certificates) 2. Certification Authority 3. Certificate Management Authority 11. Certification Paths and Protocols 1. Construction 2. LDAP and other methods 3. SCVP 4. Timestamping 5. Long Term Archiving Signatures
3	**Qualifikationsziele / Lernergebnisse** Nachdem Studierende die Veranstaltung Public Key Infrastrukturen besucht haben, können Sie ● die IT Sicherheitsziele und die kryptographischen Primitive zu deren Realisierung verstehen. ● die Grundlagen von Public Key Infrastrukturen, insbesondere die verschiedenen Komponenten (bspw. private Schlüssel, Zertifikate, Policies), Akteure (bspw. Trust Center, Schlüsselinhaberinhaber) und Prozesse (bspw. Zertifikatsbeantragung, Zertifikatserstellung, Revokation, Zertifikatsvalidierung) verstehen und erklären. ● die zugrundeliegenden theoretischen Modelle (bspw. Vertrauensmodelle, Gültigkeitsmodelle) verstehen, erklären und anwenden. ● Public Key Infrastrukturen in der Praxis anwenden (bspw. für Email Signatur und -Verschlüsselung, Prüfung der Authentizität von Webseiten).
4	**Voraussetzung für die Teilnahme**

5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** ● J. Buchmann, E. Karatsiolis, and A. Wiesmaier. "Introduction to Public Key Infrastructures", Springer-Verlag Berlin Heidelberg, 2013. ISBN: 978-3-642-40656-0 (Print) 978-3-642-40657-7 (Online) ● J. Buchmann, "Einführung in die Kryptographie", ISBN 3-540-41283-2 ● C. Adams / S. Lloyd, "Understanding Public-Key Infrastructure", ISBN 1-57870-166-X ● Tom Austin, "PKI / A Wiley Tech Brief", ISBN 0-471-35380-9 ● R. Housley / T. Polk, "Planning for PKI", ISBN 0-471-39702-4 ● A. Nash / W. Duane / C. Joseph/ D. Brink, "PKI Implementing and Managing E-Security", ISBN 0-007-213123-3 ● Henk C.A. van Tilborg, "Encyclopedia of Cryptography and Security", ISBN-13: 978-0387234731
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Kryptoplexität</td></tr>
<tr><td>Modul Nr.
20-00-0585</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>4</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
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
B.Sc. Informatik
M.Sc. Informatik
M.Sc. IT Sicherheit
M.Sc. Wirtschaftsinformatik
B.Sc. Psychologie in IT
Joint B.A. Informatik
B.Sc. Sportwissenschaft und Informatik</td></tr>
</table>

	Kann im Rahmen fachübergreifender Angebote auch 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

Post-Quantum Kryptographie</td></tr>
<tr><td>Modul Nr.
20-00-0632</td><td>Kreditpunkte
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-Sicherheit</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>20-00-0632-iv</td><td>Post-Quantum Kryptographie</td><td>0</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Fähigkeiten und Grenzen von Quantencomputern, Hash-basierte Kryptographie, Gitter-basierte Kryptographie, multivariate Kryptographie, Code-basierte Kryptographie, kryptanalytische Methoden</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Kenntnisse über quantencomputer-resistente Verfahren, Kenntnis der modernen Kryptanalyse, Erlernen von Techniken zur Kryptanalyse und deren Anwendung in der Praxis</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Lineare Algebra, Einführung in die Kryptographie</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0632-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:
• [20-00-0632-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
B.Sc. Informatik
M.Sc. Informatik
Kann in anderen Studiengängen verwendet werden.</td></tr>
<tr><td>9</td><td colspan="6">Literatur</td></tr>
<tr><td>10</td><td colspan="6">Kommentar</td></tr>
</table>

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Forschungsorientierte Kryptographie</td></tr>
<tr><td>Modul Nr.
20-00-0680</td><td>Kreditpunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
unregelmäßig</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0680-iv</td><td>Forschungsorientierte Kryptographie</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Aktuelle Arbeiten aus dem Gebiet der Kryptographie und Komplexitätstheorie verstehen und neue Forschungsansätze herausarbeiten.</td></tr>
<tr><td>3</td><td colspan="6">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="6">Voraussetzung für die Teilnahme
Empfohlen:
Einführung in die Kryptographie
Kryptoplexität</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
B.Sc. Informatik
M.Sc. Informatik
M.Sc. IT Sicherheit
M.Sc. Wirtschaftsinformatik
B.Sc. Psychologie in IT</td></tr>
</table>

	Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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 colspan="2">Modul Nr.
20-00-0993</td><td>Kreditpunkte
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</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>0</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)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
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%)</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
B.Sc. Informatik
M.Sc. Informatik
Kann in anderen Studiengängen verwendet werden.</td></tr>
<tr><td>9</td><td colspan="6">Literatur</td></tr>
<tr><td>10</td><td colspan="6">Kommentar</td></tr>
</table>

Modulbeschreibung

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

Cryptocurrencies</td></tr>
<tr><td>Modul Nr.
20-00-1010</td><td>Kreditpunkte
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-Sicherheit</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>20-00-1010-iv</td><td>Cryptocurrencies</td><td>0</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Konzepte von Kryptowährungen:
- Kryptographische Bausteine: Kryptographische Hashfunktionen, Signaturen, Blinde Signaturen, Commitments
- Chaum’s eCash Verfahren und dessen Sicherheitseigenschaften
- Verteilte System und Fehlermodelle
- Broadcast- und Konsensusverfahren
- Einführung in Bitcoin und dessen Konsensusverfahren
- Mining Bitcoins und sicheres Speichern von Bitcoins
- Anonymität in Kryptowährungen
- Angriffe auf Kryptowährungen
- Smart Contracts und Anwendungen
- Skalierbarkeit von Kryptowährungen
- Altcoins and Blockchain ecosystem</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende verstehen nach erfolgreichem Besuch der Veranstaltung die technischen und theoretischen Grundkonzepte von kryptographischen Währungen. Insbesondere lernen sie:
• Den Umgang mit kryptographischen Bausteinen und deren formale Sicherheitsanalyse mittels Beweise
• Die Entwicklung kryptographischer Protokolle und verteilter Systeme
• Die Grundkonzepte Blockchain-basiertere Kryptowährungen insbesondere der Konsensus Mechanismen
• Mögliche Angriffe auf Bitcoin und die zugrundeliegende Technologie
• Die Grundkonzepte der Entwicklung von Smart Contracts und deren Anwendung
• Neue Lösungsansäte zur Verbesserung von Kryptowährungen hinsichtlich Anonymität, Skalierbarkeit und Sicherheit
• Eine Übersicht über verschiedene Altcoins und deren Vorteile/Nachteile</td></tr>
</table>

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)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1010-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur** Literaturempfehlungen werden kontinuierlich aktualisiert, ein Beispiel für verwendete Literatur könnte sein: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller & Steven Goldfeder
10	**Kommentar**

Modulbeschreibung

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

Kryptographische Protokolle</td></tr>
<tr><td>Modul Nr.
20-00-1032</td><td>Kreditpunkte
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-Sicherheit</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>0</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)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:
• [20-00-1032-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls</td></tr>
</table>

	B.Sc. Informatik M.Sc. Informatik M.Sc. IT-Sicherheit
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Beweisbare Sicherheit					
Modul Nr. 20-00-1051	**Kreditpunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1051-vl	Beweisbare Sicherheit	0	Vorlesung	2

2 Lerninhalt

In dieser Vorlesung wird gezeigt, wie man Sicherheitseigenschaften von kryptografischen Protokollen formal beweisen kann. Dabei konzentrieren wir uns auf starke Sicherheitsgarantien und realistische Angreifermodelle und lernen verschiedene Beweistechniken kennen. Die erlernten Techniken werden wir auf teils real eingesetzte Verschlüsselungsverfahren anwenden und so eine gute Vorstellung von deren Sicherheitseigenschaften erhalten.

(1) Einführung beweisbare Sicherheit
* Definition von Sicherheit
* Einführung Sicherheitsparameter und PPT Angreifer
* Der Begriff der Reduktion
* Kryptographische Annahmen (Faktorisieren, diskrete Logarithmen)
* IND-CPA Sicherheit und das ElGamal Verschlüsselungsverfahren
* Beweis durch Reduktion: ElGamal ist IND-CPA-sicher unter der Decisional Diffie-Hellman Annahme (DDH)

(2) IND-CCA Sicherheit
* ElGamal ist nicht IND-CCA sicher
* Das Verfahren von Naor und Yung
* Das Verfahren von Cramer und Shoup

(3) Das Random-Oracle Modell (ROM)
* Einführung ROM
* Hashfunktionen
* Ist das ROM sinnvoll?
* IND-CPA und IND-CCA Sicherheit von RSA-OAEP im ROM

(4) Simulationsbasierte Sicherheit
* Vergleich simulationsbasierte und spielbasierte Sicherheitsdefinition
* Komponierbare Sicherheitsdefinitionen
* Das Universal Composability Framework
* Programmierbare Random Oracles
* Sicherer Nachrichtentransfer im (programmierbaren) ROM

3	**Qualifikationsziele / Lernergebnisse** Nachdem die Studierenden die Vorlesung besucht haben können sie - verschiedene Sicherheitsdefinitionen von Verschlüsselungsverfahren wiedergeben und vergleichen - beschreiben, welche Voraussetzungen hinreichend sind, um starke Sicherheitseigenschaften zu erreichen - formale Sicherheitsbeweise für einige Verschlüsselungsverfahren präsentieren
4	**Voraussetzung für die Teilnahme** Empfohlen, aber nicht notwendig: "Einführung in die Kryptographie"
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1051-vl] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1051-vl] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Srudiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

Grundlagen des Symmetrischen Kryptographischen Designs</td></tr>
<tr><td colspan="2">Modul Nr.
20-00-1062</td><td>Kreditpunkte
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
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-1062-vl</td><td>Grundlagen des Symmetrischen Kryptographischen Designs</td><td>0</td><td>Vorlesung</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
In diesem Kurs werden die Studenten in die Grundlagen der symmetrischen Kryptographie eingeführt. Der Fokus wird auf dem Design verschiedener Typen von Verschlüsselungsverfahren, kollisionsresistenten Hashfunktionen und Nachrichtenauthentifizierungscodes (MACs) aus grundlegenden Primitiven wie Blockchiffren und universellen Hashfunktionen liegen.
Wir werden insbesondere die neuesten kryptographischen Verfahren wie GCM, HMAC, OCB, SHA3 und SIV untersuchen, die heute verwendet werden. Der Kurs wird unter Verwendung der Methode der beweisbaren Sicherheit mit einem Ausblick auf die kryptografische Praxis durchgeführt, wobei auch praktische Angriffe auf solche kryptografische Verfahren behandelt werden. Dieser Kurs beinhaltet jedoch nicht das Design von Blockchiffren oder deren Kryptanalyse.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Studenten lernen die notwendigen Werkzeuge und Abstraktionen, um moderne kryptografische Designs und die Hintergründe für ihr Design zu verstehen. Außerdem werden die Studierenden mit der Methode der beweisbaren Sicherheit vertraut gemacht und erfahren, wie Kryptosysteme in der Praxis scheitern können. Dieser Kurz befähigt NICHT dazu, neue kryptografische Designs zu entwerfen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen wird mindestens eine der folgenden Vorlesungen:
Einführung in die Kryptographie, Kryptographie in der Praxis und Kryptoplexität.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1062-vl] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung</td></tr>
</table>

	Bausteinbegleitende Prüfung: • [20-00-1062-vl] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Symmetrische Kryptographie						
Modul Nr. 20-00-1107	**Kreditpunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1107-iv	Symmetrische Kryptographie	0	Vorlesung	4

2 Lerninhalt

Dieser Kurs deckt die Grundlagen der symmetrischen Verschlüsselung ab, die für ein Verständnis von entsprechenden modernen kryptographischen Primitiven erforderlich sind. Wesentliche Punkte sind dabei das Design von AES und Blockchiffren im Allgemeinen, kollisionsresistente und universelle Hashfunktionen, Message Authentication Codes (MACs), Tweakable Block Ciphers, Authenticated Encryption sowie Verschlüsselungsverfahren für spezialisierte Einsatzzwecke wie beispielsweise Festplattenverschlüsselung. Insbesondere werden wir jeweils die aktuell eingesetzten Verfahren wie GCM, HMAC, OCB, SHA3 und SIV untersuchen.
In diesem Kurs geht es dabei vor allem um die beweisbare Sicherheit der Verfahren, Sicherheitsdefinitionen und entsprechende Beweise spielen eine große Rolle. Dies soll den Studenten vermitteln, welche Ideen hinter den Designs der Verfahren stehen, welche Sicherheit sie versprechen und wie man sie korrekt einsetzt. Der Kurs bildet somit eine im Wesentlichen in sich geschlossene Einheit, setzt jedoch eine solide mathematische Grundbildung voraus.
Es werden als Anwendung auch praktikable Angriffe auf echte kryptographische Systeme behandelt.

3 Qualifikationsziele / Lernergebnisse

Nach Abschluss dieser Vorlesung haben die Studierenden die notwendigen Werkzeuge und Abstraktionen kennengelernt, um moderne kryptografische Designs und die Hintergründe für ihr Design zu verstehen. Außerdem sind die Studierenden mit der Methode der beweisbaren Sicherheit vertraut und haben erfahren, wie Kryptosysteme in der Praxis scheitern können. Dieser Kurs beinhaltet nicht den Entwurf neuer kryptografischer Designs.

4 Voraussetzung für die Teilnahme

Empfohlen wird mindestens eine der folgenden Vorlesungen:
Einführung in die Kryptographie, Kryptographie in der Praxis und Kryptoplexität.

5 Prüfungsform

	Bausteinbegleitende Prüfung: • [20-00-1107-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%).
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1107-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulhandbuch
M. Sc. IT-Sicherheit

Wahlbereich
System Security

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Netzsicherheit</td></tr>
<tr><td>Modul Nr.
20-00-0512</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>4</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 unterscheiden. Sie weisen ein tiefgehendes Verständnis von Sicherheitsmechanismen auf</td></tr>
</table>

	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** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Distributed Software Systems M.Sc. Autonome Systeme M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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
Sichere Mobile Systeme</td></tr>
<tr><td>Modul Nr.
20-00-0583</td><td>Kreditpunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0583-iv</td><td>Sichere Mobile Systeme</td><td>3</td><td>integrierte Lehrveranstaltung</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die integrierte Veranstaltung Sichere Mobile Systeme befasst sich mit Fragen zur Sicherheit in drahtlosen und Mobilen Netzen und Kommunikationssystemen. Grundlagen der Thematik werden durch aktuelle Forschungsthemen ergänzt.
Lerninhalte:
- Sicherheitsbetrachtung und Modellierung von Bedrohungen bei mobilen und drahtlosen Systemen
- Ausgewählte Angriffe und Sicherheitsmechanismen spezifisch für mobile und drahtlosen Systeme
- Sicherheit in drahtlosen Sensornetzen
- Sicherheit in drahtlosen Mesh-Netzen
- Bedrohungen und Schutz der Privatsphäre in mobilen und drahtlosen Systemen
- Sicherheit in zellularen Netzen (GSM, UMTS, LTE)
- Sicherheit auf der Bitübertragungsschicht
- Ausgewählte Forschungsthemen in mobilen und drahtlosen Systemen</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung besitzen die Studierenden ein spezialiertes Wissen auf dem Gebiet der Sicherheit in mobilen, verteilten, drahtlosen Netzen mit dem Schwerpunkt auf Internetsicherheit. Sie können die wichtigsten Grundlagen der IT Sicherheit, der Kryptographie sowie der Netzsicherheit in klassischen Netzen auf mobile Systeme übertragen und anwenden.

Die Studierenden 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 zu erfassen und weisen auf dem Feld sicherer mobiler Systeme ein fundiertes Wissen in Praxis und Theorie auf.</td></tr>
</table>

4	**Voraussetzung für die Teilnahme** Empfohlen: Grundlagen der Netzsicherheit und der Mobilen Netze
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Internet- und Web-basierte Systeme M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Levente Buttyan, Jean-Pierre Hubaux: Security and Cooperation in Wireless Networks, Cambridge University Press, 2008, ISBN: 978-0-521-87371-0 (book is available online for download). Ausgewählte Buchkapitel und ausgewählte wissenschaftliche Veröffentlichungen.
10	**Kommentar**

Modulbeschreibung

Modulname Sichere Kritische Infrastrukturen						
Modul Nr. 20-00-0720	**Kreditpunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0720-iv	Sichere Kritische Infrastrukturen	0	Integrierte Veranstaltung	2

2 Lerninhalt

Kritische Infrastruktur (KRITIS) sind „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ (BMI, 2009)

In der Vorlesung sollen verschiedene kritische Infrastrukturen und deren Sicherheitsherausforderungen thematisiert werden. Hierzu werden, nach einer Einführung in die Grundlagen der Thematik, Referent*innen aus Forschungseinrichtungen, Unternehmen, Behörden oder von Betreibern kritischer Infrastrukturen eingeladen, die mit Fachvorträgen einzelne Facetten des Themas beleuchten. Ein Selbststudium ausgewählter Fachartikel ergänzt die Fachvorträge.

In den vergangenen Jahren waren u.a. Referent*innen des Deutschen Bundestags, des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK), des Bundesamts für Sicherheit in der Informationstechnik (BSI), des Technischen Hilfswerks (THW), des Hessen Cyber Competence Centers (Hessen 3C), der Siemens AG, der Deutschen Bahn, der Deutschen Börse, der Deutschen Flugsicherung, sowie aus Universitäten und Forschungseinrichtungen mit ihren Vorträgen vertreten.

3 Qualifikationsziele / Lernergebnisse

Nach dem Besuch der Veranstaltung kennen die Studierenden die wichtigsten IT-Sicherheitsprobleme im Bereich kritischer Infrastrukturen. Sie verstehen Techniken zur Absicherung kritischer Infrastrukturen und sind in der Lage diese in verschiedenen Sektoren (wie dem Smart Grid, dem Transportwesen oder der Telekommunikation) anzuwenden.

4 Voraussetzung für die Teilnahme

Empfohlen: Computersystemsicherheit

5 Prüfungsform

	Bausteinbegleitende Prüfung: • [20-00-0720-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0720-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Wird in der Veranstaltung bekanntgegeben.
10	**Kommentar**

Modulbeschreibung

Modulname Physical Layer Security in Drahtlosen Systemen					
Modul Nr. 20-00-0745	**Kreditpunkte** 5 CP	**Arbeitsaufwand** 150 h	**Selbststudium** 105 h	**Moduldauer** 1 Semester	**Angebotsturnus** i.d.R. jedes Wintersemester
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0745-iv	Physical Layer Security in Drahtlosen Systemen	5	integrierte Lehrveranstaltung	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** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Ausgewählte Buchkapitel und ausgewählte wissenschaftliche Veröffentlichungen
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Drahtlose Netze zur Krisenbewältigung: Grundlagen, Entwurf und Aufbau von Null</td></tr>
<tr><td>Modul Nr.
20-00-0780</td><td>Kreditpunkte
5 CP</td><td>Arbeitsaufwand
150 h</td><td>Selbststudium
105 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0780-iv</td><td>Drahtlose Netze zur Krisenbewältigung: Grundlagen, Entwurf und Aufbau von Null</td><td>5</td><td>integrierte Lehrveranstaltung</td><td>3</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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="6">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</td></tr>
</table>

	zu betreiben. Die Studierenden erwerben Kompetenzen im Bereich Amateurfunk und Software-Defined Radios.
4	**Voraussetzung für die Teilnahme**
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Ausgewählte Buchkapitel und ausgewählte wissenschaftliche Veröffentlichungen
10	**Kommentar**

Modulbeschreibung

Modulname Schutz in vernetzten Systemen—Vertrauen, Widerstandsfähigkeit und Privatheit					
Modul Nr. 20-00-0969	**Kreditpunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0969-iv	Schutz in vernetzten Systemen—Vertrauen, Widerstandsfähigkeit und Privatheit	0	Integrierte Veranstaltung	2

2 Lerninhalt

- Schutz in vernetzten Systemen: Hintergrund, Motivation und Herausforderungen
- Vertrauen (Computational Trust): Modelle und Mechanismen
- Vertrauen (Computational Trust): PKI-Anwendungen, Cloud Computing, Reputationssysteme und Web Services
- Vertrauen: Verwaltung von Enttäuschungen and Komfort von Geräte
- Privatheit: Definitionen, Modelle, Daten-Anonymität und Kommunikations-Anonymität
- Privatheit und Vertrauen: Privatheit-respektierende Vertrauensmodelle, Mechanismen und Anwendungen für Identitätsmanagement
- Sicherheit & Ökonomie
- Widerstandsfähigkeit: Modelle, Netzwerk-Angriffserkennungs-Systeme, kollaborative Angriffserkennung, Honeypots
- Resilient networks

3 Qualifikationsziele / Lernergebnisse

Die integrierte Veranstaltung Schutz in vernetzten Systemen—Vertrauen, Widerstandsfähigkeit und Privatheit deckt die Themenbereiche berechenbares Vertrauen (computational trust), Widerstandsfähigkeit (resilience), anonyme Netzwerke, sowie kollaborative Schutzmechanismen ab. Mit der Teilnahme an diesem Kurs wird das Verständnis von Herausforderungen und Lösungen im Kontext von vernetzten Systemen vermittelt. Dieser Kurs betrachtet das Konzept von Ende-zu-Ende Systemen mit Schwerpunkt auf Nutzer, Geräte, Netzwerke, sowie Anwendungen und Dienste.

4 Voraussetzung für die Teilnahme

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-0969-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0969-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur** - Trust and Reputation for Service-Oriented Environments: Technologies For Building Business Intelligence And Consumer Confidence, Elizabeth Chang, Tharam Dillon, and Farookh K. Hussain, 374 pages, 2006. ISBN: 978-0-470-01547-6 - On anonymity in an electronic society: A survey of anonymous communication systems, Matthew Edman and Bülent Yener, ACM Computing Surveys, Vol. 42, Issue 1, 2009. - Taxonomy and Survey of Collaborative Intrusion Detection, Emmanouil Vasilomanolakis, Shankar Karuppayah, Max Mühlhäuser, Mathias Fischer, ACM Computing Surveys, Vol. 47 Issue 4, 2015. - Selected book chapters and scientific publications
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Hardware-orientierte Sicherheit</td></tr>
<tr><td>Modul Nr.
20-00-1082</td><td>Kreditpunkte
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</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-1082-iv</td><td>Hardware-orientierte Sicherheit</td><td>0</td><td>Integrierte Veranstaltung</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
• Zufallszahlengeneratoren
• Physically Unclonable Functions
• Hardware-Trojaner
• Seitenkanalangriffe gegen kryptographische Implementierungen
• Trusted Platform Modules und Trusted Execution Environments
• Techniken des Remote Attestation
• Covert Channels
• Effiziente Implementierung kryptographischer Verfahren</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Kenntnisse:
Die Studierenden erwerben grundlegende Kenntnisse im Bereich der hardware-orientierten Sicherheit: Mit diesen Verfahren können effektiv moderne Rechnerplattformen abgesichert werden. Sie lernen verschiedene Klassen von Verfahren der Hardware-Sicherheit kennen und können diese auf neue Problemstellungen anwenden.

Fähigkeiten:
Die Studierenden lernen Einsatzbereiche von Techniken der hardware-orientierten Sicherheit kennen. Sie erwerben die Fähigkeit, die besprochenen Techniken in der Praxis umzusetzen.

Kompetenzen:
Die Studierenden lernen die Sicherheit von Methoden der hardware-basierten Sicherheit zu beurteilen und die für einen Anwendungsfall geeigneten Methoden auszuwählen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Fortgeschrittene IT-Security</td></tr>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1082-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1082-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname
Privatheit biomedizinischer Daten

Modul Nr.	Kreditpunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-1084	3 CP	90 h	60 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Deutsch	Koordinatoren/Koordinatorinnen IT-Sicherheit

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1084-vl	Privatheit biomedizinischer Daten	0	Vorlesung	2

2 Lerninhalt
Grundlagen Genetik, Epigenetik
Grundlagen Bioinformatik in der Humanmedizin
Biomedizinische Sensorik
Das TMF-Konzept zum Datenschutz
Privacy Metriken
Secure-Multi-Party-Computations

3 Qualifikationsziele / Lernergebnisse
Die Studierenden können aktuelle Forschungsliteratur erfassen und Technologieentwicklungen hinsichtlich ihrer Datenschutzniveaus im Bereich der Biomedizin unterscheiden.
Sie können weiterhin anhand der erläuterten Grundlagen potentielle Re-Identifikationsrisiken einschätzen und Mechanismen zu deren Behebung konzeptionell vorschlagen.
Sie können weiterhin einfach Abfragen/Auswertungen/Studien-Designs hinsichtlich ihrer Privacy-Implikationen einschätzen.

4 Voraussetzung für die Teilnahme
Empfohlen: Grundlagen der Kryptographie

5 Prüfungsform
Bausteinbegleitende Prüfung:

- [20-00-1084-vl] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

6 Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)

7 Benotung
Bausteinbegleitende Prüfung:

- [20-00-1084-vl] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)

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

Modulbeschreibung

Modulname Cyber Range					
Modul Nr. 20-00-1096	**Kreditpunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1096-iv	Cyber Range	0	Integrierte Veranstaltung	2

2 Lerninhalt

Der Kurs basiert auf der Fraunhofer Cyber Range-Plattform, einer Simulationsumgebung für Sicherheitstrainings. Die Plattform kann Unternehmensnetzwerke verschiedener Größen simulieren und darin echte Malware ausführen und Sicherheitsprobleme simulieren. In verschiedenen Szenarien müssen Studenten das Netzwerk überwachen, Sicherheitsprobleme zeitnah erkennen, analysieren und geeignete Gegenmaßnahmen treffen.

Die Studenten werden alleine als auch in Gruppen mit realer SIEM-/Monitoring-Software arbeiten. Von dort ausgehend werden sie eine Reihe von Untersuchungen durchführen an einer Vielzahl von Linux- und Windows-basierten Systemen, um die Ursachen für Sicherheitsprobleme zu entdecken. Während den Untersuchungen setzen sie dabei eine Vielzahl von Standard-Systemwerkzeugen und spezielle forensische Software ein. Am Ende eines jeden Szenarios werden sie die Ursachen der Sicherheitsprobleme beheben und das Netzwerk geeignet absichern.

Ein Trainer wird die Studenten während den Szenarien unterstützen und anleiten, gefundene Schwachstellen in dem System wie in einem SOC ordnungsgemäß zu dokumentieren. Für die Dokumentation vergibt das System automatisiert Punkte.

Der Kurs wird eine ganze Woche am Fraunhofer-Institut für Sichere Informationstechnologie stattfinden und enthält sowohl Vorlesungsanteile als auch praktische Anteile. Studenten bekommen eine Einführung in die verwendete Software, aber der Fokus des Kurses ist die Anwendung von Sicherheitswissen in der Simulationsumgebung unter Anleitung eines Trainers.

Die Inhalte der Szenarien enthalten unter anderem grundlegende Netzwerkprobleme wie unerwartete Dienstausfälle, Web Defacement, SQL-Injections als auch fortgeschrittene Themen wie Malware/Ransomeware-Ausbrüche, forensische Malware-Analysen und Erkennung von Man-in-the-Middle-Angriffen. Die meisten Szenarien sind "Blue Team"-Szenarien, in denen Studenten ein Netzwerk verteidigen

	müssen. Einige "Red Team"-Szenarien runden den Kurs ab, bei denen Studenten selbst in Systeme eindringen müssen.
3	**Qualifikationsziele / Lernergebnisse** * Grundlegende Bedienung von SIEM-/Netzwerküberwachungssoftware * Verständnis für Netzwerkanalyse * Wissen über grundlegende forensische Methoden zur Analyse von Windows- und Linux-Systemen * Umgang mit grundlegender Malware-Analyse * Umgang mit netzwerkbasierten Sicherheitsproblemen
4	**Voraussetzung für die Teilnahme** Empfohlen werden: * Fortgeschrittene Netzwerkkenntnisse * Grundlegendes Wissen über Linux- und Windows-Administration, insbesondere Log-Analyse * Programmierkenntnisse in mehreren Programmier- und Skriptsprachen * Kenntnisse über relationale Datenbanksysteme * Grundlegende Assembler-Kenntnisse
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1096-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1096-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Seitenkanalangriffe gegen IT-Systeme</td></tr>
<tr><td>Modul Nr.
04-00-0218</td><td>Kreditpunkte
5 CP</td><td>Arbeitsaufwand
150 h</td><td>Selbststudium
105 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>04-00-0218-vu</td><td>Seitenkanalangriffe gegen IT-Systeme</td><td></td><td>Vorlesung und Übung</td><td>3</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Mathematik: Modellierung von Seitenkanalinformationen durch stochastische Prozesse, Anwendungen der statistischen Entscheidungstheorie und der multivariaten Statistik (Ziele: optimale Verwertung der Seitenkanalinformation etc.), elementare Zahlentheorie.

Kryptographie und IT-Sicherheit: Laufzeitangriffe, Cachebasierte Angriffe, Powerangriffe.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach dem Besuch dieses Moduls sind die Studierenden mit den behandelten Seitenkanalangriffen vertraut, haben die elementaren mathematischen Methoden durchdrungen und können diese auf verwandte Problemstellungen anwenden. Sie haben zumindest die Grundideen der fortgeschritteneren mathematischen Ansätze verstanden. Die Studierenden sollen alle mathematische Ansätze und Methoden beherrschen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
(LA und Ana) oder vergleichbare Kenntnisse, Kenntnisse in Stochastik wünschenswert, Grundkenntnisse in Kryptographie hilfreich</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
</table>

8	**Verwendbarkeit des Moduls** BSc. Math. Wahlbereich, MSc. Math. Ergänzungsbereich
9	**Literatur** H. Bauer: Wahrscheinlichkeitstheorie. 5. Auflage, de Gruyter, Berlin 2001. F.E. Beichelt, D.C. Montgomery: Teubner Taschenbuch der Stochastik - Wahrscheinlichkeitstheorie, Stochastische Prozesse, Mathematische Statistik. Teubner, Wiesbaden 2003. O.J.W.F. Kardaun: Classical Methods of Statistics. Springer, Berlin 2005. S. Mangard, E. Oswald, T. Popp: Power Analysis Attacks - Revealing the Secrets of Smart Cards. Springer, Berlin 2007. + eine Vielzahl einschlägiger Aufsätze
10	**Kommentar**

Modulhandbuch
M. Sc. IT-Sicherheit

Wahlbereich
Software 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>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Studenten 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 Studenten 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.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Grundkenntnisse in Multimedia-Formaten und IT-Sicherheit.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Visual Computing M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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
Formale Methoden der Informationssicherheit</td></tr>
<tr><td>Modul Nr.
20-00-0362</td><td>Kreditpunkte
9 CP</td><td>Arbeitsaufwand
270 h</td><td>Selbststudium
180 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</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
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
</table>

7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Distributed Software Systems M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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

Modulname Statische und dynamische Programmanalyse					
Modul Nr. 20-00-0580	**Kreditpunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0580-iv	Statische und dynamische Programmanalyse	0	Integrierte Veranstaltung	4

2 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

3 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.

4 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

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-0580-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0580-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

Automatisches Beweisen</td></tr>
<tr><td>Modul Nr.
20-00-0660</td><td>Kreditpunkte
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-Sicherheit</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>0</td><td>Integrierte Veranstaltung</td><td>4</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
Stark empfohlen wird die Teilnahme an der Vorlesung “Aussagen- und Prädikatenlogik” oder vergleichbarer Module. Ansonsten genügt eine gewisse mathematische Reife.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0660-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:
• [20-00-0660-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
B.Sc. Informatik
M.Sc. Informatik</td></tr>
</table>

	B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Robinson, Voronkov: Handbook of Automated Reasoning, 2 vols., North-Holland
10	**Kommentar**

Modulbeschreibung

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

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0794-iv	Formale Spezifikation und Verifikation von Software	0	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
Formale Grundlagen der Informatik 2 und 3
(oder vergleichbarer)

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0794-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0794-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT M.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Applied Static Analysis					
Modul Nr. 20-00-0949	**Kreditpunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0949-iv	Applied Static Analysis	0	Integrierte Veranstaltung	2

2 Lerninhalt

Foundations of (scalable) static analyses for large(r) software systems; in particular
- Basic Terminology:
- AST, SSA,
- Object-/ Field-/ Context-/ Flow-/ Path Sensitivity
- (I)CFG
- Inter-procedural analyses
- …
- stack based intermediate representations (JVM Bytecode)
- register based intermediate representations (LLVM IR)
- program transformations and native code analyses using LLVM

Concrete static analyses and algorithms:
- Call graph algorithms for libraries and applications
- Inter procedural data- and control-flow analyses
- IDE/IFDS
- Points-to analyses
- Escape analyses

Applications
- General software quality analyses
- Capability Analysis
- Security Vulnerabilities Detection
- Dead Paths/Computations
- Next generation software development tools

3 Qualifikationsziele / Lernergebnisse

Students can effectively use the basic static analyses related terminology.
Students are familiar with modern static analyses working on intermediate representations.
They are able to apply and adapt available static analysis algorithms to new scenarios.

4 Voraussetzung für die Teilnahme

Empfohlen:

The lecture is targeted towards Master students with a very high degree of interest in reading, analyzing and also writing code. Basic knowledge in compiler construction is helpful. Deep

	knowledge of object-oriented programming concepts and in particular of object-oriented programming in Java is required. Interest in learning new programming languages (in particular Scala) is required.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0949-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%) Studierende, die die Lehrveranstaltung 20-00-0732 oder 20-00-0771 besucht haben, dürfen diese Veranstaltung nicht hören, da die Inhalte sehr vergleichbar sind.
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0949-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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>Kreditpunkte
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-Sicherheit</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>0</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
Empfohlen:

Grundlagen der Informatik</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-1025-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1025-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Informationstechnologie für Frieden und Sicherheit					
Modul Nr. 20-00-1026	**Kreditpunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1026-iv	Informationstechnologie für Frieden und Sicherheit	0	Integrierte Veranstaltung	4

2 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

3 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

4 Voraussetzung für die Teilnahme

Empfohlen:

Grundlagen der Informatik

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1026-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%)

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1026-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Typsysteme</td></tr>
<tr><td>Modul Nr.
20-00-1076</td><td>Kreditpunkte
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-Sicherheit</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>20-00-1076-iv</td><td>Typsysteme</td><td>0</td><td>Integrierte Veranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Typsysteme bieten einen effizienten Weg, um die korrekte Funktionsweise von Programmen zu garantieren, bevor diese überhaupt gestartet werden. Es gibt sie in den verschiedensten Ausprägungen: als Standard-Konstrukt und Teil einer Programmiersprache oder speziell für bestimmte Anwendungen entworfen.

Wir werden uns u.A. mit den folgenden Themen beschäftigen:
- Einfach getypter lambda-Kalkül
- Statische vs. dynamische Analyse von Typen
- Operationale Semantik
- Soundness von Typsystemen
- Typ Inferenz
- Curry-Howard-Korrespondenz
- Polymorphism
- Subtyping
- Safety und Liveness Garantien durch Typsysteme
- Abhängige Typen</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Veranstaltung kennen Studierende ein Spektrum von unterschiedlichen Typsystemen und ihre Einsatzgebiete. Sie verstehen die Grundlagen und Funktionsweise statische Programmanalyse und die Unterschiede verschiedener Typsysteme. Sie können können verschieden artige Typsysteme anwenden. Darüber hinaus können sie beurteilen und formal analysieren, welche Eigenschaften ein Typsystem garantieren kann. Sie kennen die Grenzen statischer Analysen und können Varianten bekannter Typsysteme für neue Anwendungen 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>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1076-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1076-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B,Sc. Informatik M.Sc. Informatik 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>Kreditpunkte
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-Sicherheit</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>0</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>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1079-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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>Kreditpunkte
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-Sicherheit</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>0</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>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1069-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Software-Engineering - Wartung und Qualitätssicherung					
Modul Nr. 18-su-2010	**Kreditpunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** i.d.R. jedes Sommersemester
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

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

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 wird als durchgängiges Beispiel ein geeignetes "Open Source"-Projekt ausgewählt. Die Übungsteilnehmer untersuchen die Software des gewählten Projektes in einzelnen Teams, denen verschiedene Teilsysteme des betrachteten Gesamtsystems zugeordnet werden.

3 Qualifikationsziele / Lernergebnisse

Die Lehrveranstaltung vermittelt an praktischen Beispielen und einem durchgängigen Fallbeispiel grundlegende Software-Wartungs- und Qualitätssicherungs-Techniken, also eine ingenieurmäßige Vorgehensweise zur zielgerichteten Wartung und Evolution von Softwaresystemen. Nach der Lehrveranstaltung sollte ein Studierender in der Lage sein, die im Rahmen der Softwarewartung und -pflege eines größeren Systems anfallenden Tätigkeiten durchzuführen. Besonderes Augenmerk wird dabei auf Techniken zur Verwaltung von Softwareversionen und –konfigurationen sowie auf das systematische Testen von Software gelegt. 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 sowie auf die Arbeit im Team unter Einhaltung von vorher festgelegten Qualitätskriterien gelegt.

4 Voraussetzung für die Teilnahme

Empfohlen: Grundlagen der Softwaretechnik sowie gute Kenntnisse einer objektorientierten Programmiersprache.

5	**Prüfungsform** Fachprüfung
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** MSc ETiT, MSc iST, MSc Wi-ETiT, Informatik
9	**Literatur** www.es.tu-darmstadt.de/lehre/se_ii/
10	**Kommentar**

Modulhandbuch
M. Sc. IT-Sicherheit

Wahlbereich
Selected Complementary Topics

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Graphische Datenverarbeitung I</td></tr>
<tr><td>Modul Nr.
20-00-0040</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>4</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
● Grundlegende Algorithmen und Datenstrukturen
● Lineare Algebra
● Analysis
● Inhalte der Vorlesung Visual Computing</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
</table>

7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>4</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: Algorithmen und Datenstrukturen, Grundlagen aus der Höheren Mathematik, Graphische Datenverarbeitung I, C / C++</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard

In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.</td></tr>
</table>

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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>Kreditpunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
i.d.R. jedes Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>4</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 praktische 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>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Nach der erfolgreichen Absolvierung dieser Lehrveranstaltung sind die Studenten in der Lage</td></tr>
</table>

	● 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** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Autonome Systeme M.Sc. Visual Computing M.Sc. Internet- und Web-basierte Systeme M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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

Netz-, Verkehrs- und Qualitäts-Management für Internet Services</td></tr>
<tr><td>Modul Nr.
20-00-0056</td><td>Kreditpunkte
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</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0056-vl</td><td>Netz-, Verkehrs- und Qualitäts-Management für Internet Services</td><td>0</td><td>Vorlesung</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Einführung in das Management von Internet Service Provider (ISP-)Netzen zur Integration von Service Plattformen mit ihren Qualitäts- und Verkehrsprofilen</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Stoffplan:
Anforderungen und Maßnahmen zur Sicherung der Quality-of-Service (QoS)

- Kriterien aus Anwendungs- & Nutzer-Sicht (QoE: Quality of Experience)
- QoS Architektur in IP-Netzen: Differentiated & Integrated Services
- QoS Support & Auswirkung je Anwendung im IP Verkehrs-Mix
(Video-Streaming, VoIP, Web Browsing, Downloads, Social Networking etc.)

Qualitätssicherung für Internet Services in ISP Netzinfrastrukturen

- Einfluss der Netz- und Transportebene:
Routing (OSPF, BGP), Multiprotocol Label Switching (MPLS), TCP mit Absicherung gegen Fehler und Ausfälle
- Messung, Monitoring, Optimierung von IP Verkehr bzgl. QoS

Qualitätssicherung in Service Overlays und auf Anwendungsebene

- Content Delivery Netze (CDN), Clouds und Peer-to-Peer Netze (P2P)
inkl. verteilter Caches, Transportpfad-Optimierung, Skalierbarkeit
- IETF Standardisierung (CDN Interconnection, ALTO: Appl. Layer Traffic Opt.)</td></tr>
</table>

4	**Voraussetzung für die Teilnahme** Empfohlen: Vorwissen: Grundlegende Kenntnisse der Informatik und Internet-Anwendungen werden vorausgesetzt. Die Vorlesungen Kommunikationsnetze I und II sind empfohlen.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0056-vl] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0056-vl] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls**
9	**Literatur** Wird in der Vorlesung angesprochen
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
TK1: Verteilte Systeme und Algorithmen</td></tr>
<tr><td>Modul Nr.
20-00-0065</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0065-iv</td><td>TK1: Verteilte Systeme und Algorithmen</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Lernziele:
● Umfassendes Überblickswissen über die grundlegenden Probleme und Ansätze
● Tiefgehendes Methodenwissen zu klassischen verteilten Algorithmen und Programmierparadigmen
● Anwendbare exemplarische Kenntnis aktueller Entwicklungen und Standards

Stoffplan:
● Einführung
● Auffrischung und Ergänzung von Kapitel 1 der Kanonik Net-Centric Computing
● Überblick über die Vorlesung
● Verteilte Algorithmen
○ Elementaralgorithmen (z.B. globaler Zustand)
○ Basisalgorithmen (z.B. Ausschluss, Konsens, Kooperation)
○ Formalisierung (Eigenschaften und deren Nachweis)
● Verteiltes Programmieren
○ Push-Paradigmen (z.B. IPC, RPC, DOC)
○ aktuelle Ansätze (z.B. Pull-Paradigmen, Objektmobilität)</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende kennen nach erfolgreichem Besuch der Veranstaltung die Grundlagen der verteilten Programmierung und verteilter Algorithmen. Sie verstehen die grundlegenden Probleme verteilter Systeme und die klassischen verteilen Algorithmen und Programmierparadigmen. Sie können klassische und aktuelle Standards verteilter Programmierung praktisch anwenden.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: „Computer-Netzwerke und verteilte Systeme“</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
</table>

7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Autonome Systeme M.Sc. Internet- und Web-basierte Systeme M.Sc. Distributed Software Systems M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Literaturempfehlungen werden kontinuierlich aktualisiert, Beispiele für verwendete Literatur könnten sein: ● George Coulouris, Jean Dollimore, Tim Kindberg: Distributed Systems. Concepts and Design (Gebundene Ausgabe) 832 Seiten, Addison Wesley; Auflage: 4th (14. Juni 2005), ISBN: 0321263545 ● M. Boger: Java in verteilten Systemen, 1999, dpunkt-Verlag, Heidelberg, ISBN: 3932588320 ● G. Tel: Introduction to Distributed Algorithms, 2nd Ed 2001, Cambridge University Press, ISBN: 0521794838 ● A. Tanenbaum, M.v.Steen, Verteilte Systeme: Grundlagen und Paradigmen, Pearson Studium 2003, ISBN: 3827370574 ● A. Tanenbaum: Computernetzwerke. 4te Auflage. Pearson Studium 2003, ISBN-10: 3827370469 ● J. Kurose, K. Ross: Computer Networking, 1. Ed. 2000, Adison-Wesley. ISBN: 0201477114 ● L. Peterson, B. Davie, Computernetze, 1. Aufl. 2000, dpunkt Heidelberg, ISBN: 393258869X ● Hammerschall, U.: Verteilte Systeme und Anwendungen. Pearson, München 2005, ISBN: 3827370965
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Konzepte der Programmiersprachen</td></tr>
<tr><td>Modul Nr.
20-00-0072</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0072-iv</td><td>Konzepte der Programmiersprachen</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die wesentlichen Konzepte von Programmiesprachen. Insbesondere werden dazu Programmiersprachen in ihre Basiskonzepte aufgespalten und diese detailliert betrachtet:
● Die Rolle von Syntax
● Funktionen
● Meta-Interpreter
● Rekursion
● Verzögerte Auswertung
● Zustand und Seiteneffekte
● Continuations
● Statische Typsysteme
● Domain-spezifische Sprachen und Makros
● Objektorientierte Programmierung</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach dem erfolgreichen Abschluss der Veranstaltung verfügen die Studierenden über die folgenden Fähigkeiten:

● Sie können die entscheidenden Merkmale von Programmiersprachen benennen und im konkreten Fall identifizieren;

● die Studierenden sind mit den wesentlichen theoretischen Konzepten von Programmiersprachen vertraut;

● sie können verschiedene Vorgehensweisen bei der Implementierung von Programmiersprachen benennen und einfache Programmiersprachen umsetzen;

● die Studierenden verstehen, wie Programmiersprachen den Lösungsraum von Problemen beeinflussen; sie können die Auswirkung der Wahl einer Programmiersprache auf die Softwareentwicklung abschätzen;</td></tr>
</table>

	● die Studierenden sind in der Lage stereotypische Kategorisierungen von Programmiersprachen zu überwinden.
4	**Voraussetzung für die Teilnahme** Empfohlen: Funktionale und Objektorientierte Programmierkonzepte
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Distributed Software Systems B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** ● S. Krishnamurthi: Programming Languages - Application and Interpretation ● M. Scott: Programming Language Pragmatics, Morgan Kaufmann ● D. Friedman et al.: Programming Language Essentials, MIT Press
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Web Mining</td></tr>
<tr><td>Modul Nr.
20-00-0101</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0101-iv</td><td>Web Mining</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Das World-Wide Web verschafft jedem Internet-User Zugang zu einer stetig wachsenden Informationsfülle, die ohne entsprechende Unterstützung nicht mehr zu überschauen ist. Web Mining ist eine Forschungsrichtung, die versucht, das Problem mit Hilfe von Techniken des Maschinellen Lernens und Data Minings in den Griff zu bekommen. In dieser Vorlesung werden sowohl Grundlagen von Information Retrieval und Text Classification vermittelt, als auch auf die Ausnutzung der Besonderheiten von Web-Dokumenten (d.h., ihre Strukturierung und ihre Vernetzung) eingegangen.
● Introduction
○ Web Mining Overview
○ The Web, HTTP, HTML, DOM, XPath
○ Data Mining Overview
○ Structured, Semi-Structured and Unstructured Data
○ Sample Web Mining Tasks
● Information Retrieval on the Web
○ search engines & web crawlers
○ document indexing
○ the vector space model
○ inverted index
○ performance measures (recall & precision)
○ relevance feedback
○ estimating the size of the web
● Text Mining
○ text classification
■ document representation
■ induction of classifiers (k-NN, Naive Bayes, SVMs, Rule Learners)
■ Overfitting Avoidance
■ Evaluation of Classifiers
■ Multi-Label Classification
○ feature engineering
■ stop words</td></tr>
</table>

	■ feature subset selection ■ n-grams ■ stemming ■ phrases ■ latent semantic indexing ○ semi- and unsupervised learning ■ clustering (k-means, bottom-up agglomerative) ■ semi-supervised learning (active learning, self-training, co-training) ● Structure mining ○ the Web as a graph ○ hyperlink-based relevance ranking (hubs and authorities, page rank) ○ hypertext classification (Naive Method, HyperClass, hyperlink ensembles) ● Information Extraction & Wrapper Induction ○ conventional information extraction (AutoSlog) ○ structured text (LR-Wrappers) ○ semi-structured text (SoftMealy, WHISK, SRV, RAPIER) ● Web Usage Mining ○ recommender systems ○ memory-based collaborative filtering ○ model-based collaborative filtering ○ web log mining
3	**Qualifikationsziele / Lernergebnisse** Nachdem Studierende die Veranstaltung besucht haben, können sie ● grundlegende Techniken des Information Retrieval und Web Mining verstehen und erklären ● praktische Information Retrieval und Web Mining Systeme selbständig einsetzen und deren Stärken und Schwächen verstehen ● neue Entwicklungen uaf diesem Gebiet kritisch beurteilen
4	**Voraussetzung für die Teilnahme**
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Internet- und Web-basierte Systeme M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** ● Soumen Chakrabarti: Mining the Web - Discovering Knowledge from Hypertext Data. Morgan Kaufmann Publishers, 2003. ● Christopher D. Manning, P. Raghavan and H. Schütze, Introduction to Information Retrieval, Cambridge University Press. 2008.
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Effiziente Graphenalgorithmen</td></tr>
<tr><td>Modul Nr.
20-00-0110</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0110-iv</td><td>Effiziente Graphenalgorithmen</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
- Effiziente Algorithmen für Graphendurchlauf und Zusammenhangsprobleme in Graphen
- Optimale Bäume und Branchings
- Netzwerk-Flussprobleme
- Matching- und Zuweisungsprobleme
- Planare Graphen
- Theorie, generische Ansätze, Verbesessrungen durch Beschleunigungstechniken und Datenstrukturen</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nachdem Studierende erfolgreich diese Veranstaltung besucht haben,

- kennen sie grundlegende Algorithmen

- kennen sie Verfahren zur Effizienzsteigerung

- können sie Graphenalgorithmen analysieren

- beherrschen sie Methoden, um spezielle Eigenschaften (Planarität, Dünnbesetztheit) auszunutzen

- können sie die Effizienz von Verfahren in der Praxis beurteilen</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
</table>

7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Internet- und Web-basierte Systeme B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Wird in der Veranstaltung bekannt gegeben
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Algorithmische Modellierung / Grundlagen des Operations Research</td></tr>
<tr><td>Modul Nr.
20-00-0113</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0113-iv</td><td>Algorithmische Modellierung / Grundlagen des Operations Research</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
- Algorithmische Optimierungssprachen wie OPL und Eclipse
- Modellierung innerhalb eines restriktiven Modellierungsrahmens (zum Beispiel lineare Optimierung oder ganzzahlige lineare Optimierung)
- Modellierung als kombinatorische Optimierungsprobleme (z.B. Netzwerkflussprobleme, Färbungsprobleme, Wegeprobleme)
- Komplexe Fallbeispiele aus der Praxis, z.B. Anwendungen in Logistik, deterministisches und stochastisches Scheduling</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nachdem Studierende erfolgreich diese Veranstaltung besucht haben,

- kennen sie Modellierungsstrategien für Entscheidungs-, Konstruktions- und Optimierungsprobleme

- können sie zwei algorithmische Modellierungssprachen anwenden

- können sie komplexe Probleme adäquat modellieren</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: „Algorithmen und Datenstrukturen“ oder vergleichbar („Modellierung, Spezifikation und Semantik“ wäre ebenfalls wünschenswert).</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
</table>

	In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Internet- und Web-basierte Systeme B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** wird in der Veranstaltung bekannt gegeben
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
TK3: Ubiquitous / Mobile Computing</td></tr>
<tr><td>Modul Nr.
20-00-0120</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0120-iv</td><td>TK3: Ubiquitous / Mobile Computing</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
● Kenntnis technischer Grundlagen der Mobilkommunikation
● Kenntnis wichtiger Herausforderungen, Thesen und Modelle des Ubiquitous Computing
● Methodenwissen über aktuelle Ansätze des Ubiquitous Computing

Stoffplan:

● Einführung in Ubiquitous Computing

○ Definitionen und Bedeutung
○ Herausforderungen und Klassifikation
○ Wichtiges zur historischen Entwicklung (Mark Weiser u.a.)
○ Von Terminologie zu Taxonomie
○ Referenzarchitekture

● Mobilkommunikation als ‘Enabling Technology’

○ Einordnung und physikalische Grundlagen
○ Elementare Mehrfachzugriffs- und Modulationsverfahren
○ Zellulare Weitverkehrsnetze: von GSM bis LTE
○ Drahtlose lokale Netze: wLAN, Bluetooth und ZigBee

● Internet-of-Things: RFID und Smart Items

○ Grundlagen von RFID-Systemen
○ EPC und Smart Items
○ NFC: Nahfeld-Kommunikation

● Service Discovery und Cloudlets</td></tr>
</table>

	○ Grundlagen der Skalierbarkeit im Ubiquitous Computing ○ Service Discovery: Grundlagen ○ Service Discovery: konkurrierende Ansätze ○ Cloudlets: Forschungsansätze für Ubiquitous Cloud Computing ● Context- und Location Aware Computing ○ Grundlagen der Adaptivität in Ubiquitous Computing ○ Kontext-Modelle und Ansätze für Context-Aware Computing ○ Technische Grundlagen der Ortsbestimmung und Location Awareness ● Mensch-Maschine-Interaktion für Ubiquitous Computing ○ Einführung: Ease-of-Use und Post-Desktop-Interaktion ○ Interaction Design und Mulitmodale Interaktion ○ Grundlagen von Multitouch-Systemen ○ Pen-and-Paper-Interaktion und Tangible Interaction ○ UI Design: Evaluationstechniken ○ Systematisches UI Engineering ● Privatsphäre und Vertrauen im Ubiquitous Computing ○ Einführung in Privacy und rechtliche Grundlagen ○ Zum Wesen personenbezogener Daten ○ Privacy-Enhancing Technologies (PETs) und Anonyme Kommunikation ○ Einführung in Vertrauen und Reputation ○ Vertrauensmodelle und Computational Trust ○ Trust-Management-Systeme
3	**Qualifikationsziele / Lernergebnisse** Studierende kennen nach erfolgreichem Besuch der Veranstaltung die technische Grundlage mobiler Kommunikation. Sie verstehen die grundlegenden Herausforderungen von Ubiquitous Computing. Sie kennen aktuelle Ansätze um diese Herausforderungen zu lösen. Sie sind außerdem in der Lage ihre Kenntnisse auf aktuelle Probleme anzuwenden.
4	**Voraussetzung für die Teilnahme** Empfohlen: „Computer-Netzwerke und verteilte Systeme“
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard

	In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Internet- und Web-basierte Systeme M.Sc. Distributed Software Systems M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Literaturempfehlungen werden kontinuierlich aktualisiert, Beispiele für verwendete Literatur könnten sein: A Primärliteratur: Handbook of Research: Ubiquitous Computing Technology for Real Time Enterprises edited by Prof. Dr. Max Mühlhäuser, Dr. Iryna Gurevych, 2008, Information Science Reference, ISBN-10: 1599048329 B Sekundärliteratur: 1. F. Adelstein, S. Gupta et al.: Fundamentals of Mobile & Pervasive Computing McGraw Hill 2004, 2. Stefan Poslad: Ubiquitous Computing, Wiley 2009, ISBN 978-0-470-03560-3 3. Kapitel Mobilkommunikation: M. Sauter: Grundkurs Mobile Kommunikationssysteme: UMTS, HSDPA und LTE, GSM, GPRS und Wireless LAN; Vieweg-Teubner Studium 2010 4. J. Krumm (Ed.): Ubiquitous Computing Fundamentals, CRC Press 2010 D. Cook, S. Das (Ed.): Smart Environments, Wiley 2005
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Ubiquitous Computing in Geschäftsprozessen</td></tr>
<tr><td>Modul Nr.
20-00-0121</td><td>Kreditpunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0121-vl</td><td>Ubiquitous Computing in Geschäftsprozessen</td><td>3</td><td>integrierte Lehrveranstaltung</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
● Nutzungsmöglichkeiten aktueller Ubiquitous Computing Technologien in Geschäftsprozessen und im Bereich von Smart Cities
● Ermittlung des ökonomischen Potentials verschiedener Ubiquitous Computing Technologien im Kontext verschiedener Geschäftsprozesse und im Bereich von Smart Cities
● Verständnis der grundlegenden Technologien und Darstellung der mit diesen verbundenen Vorteile, Herausforderungen und Anwendungsfälle
● Spezifische Technologien wie RFID, Smart Items (z.B. Smart Shelf) etc. und ihre Integration in Prozesse
● Darstellung der Integration zwischen physischer und virtueller Welt, wie sie z.B. in aktuellen Enterprise Software Systemen realisiert wird
● Sammeln praktischer Erfahrungen im Umgang mit Ubiquitous Computing Technologien im Kontext verschiedener Anwendungsfälle, z.B. mittels Live-Demonstrationen</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach der Teilnahme an dieser Lehrveranstaltungen haben sich Studierende Kenntnissen über Auswirkungen des ubiquitären Computing auf Geschäftsprozesse und Smart Cities in Verbindung mit grundlegenden Konzepten angeeignet</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
</table>

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Internet- und Web-basierte Systeme M.Sc. Distributed Software Systems M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** ● Mühlhäuser, M.; Gurevych, I. (Eds.): Ubiquitous Computing Technology for Real Time Enterprises Information Science Reference, Dezember, 2007 ● Finkenzeller, K: RFID-Handbuch. Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC. Hanser Fachbuch; Auflage: 5., aktual. u. erw. Aufl. (1. Oktober 2008) ● Fleisch, E.; Mattern, F. (Hrsg.): Das Internet der Dinge: Ubiquitous Computing und RFID in der Praxis, Springer, Berlin, Heidelberg, New York 2005 ● Österle, H.; Fleisch, E.; Alt, R.: Business Networking – Shaping Collaboration between Enterprises, Springer ● Callaway, E.H.: Wireless Sensor Networks: Architectures and Protocols, Auerbach Publications
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Geometrische Methoden des CAE/CAD</td></tr>
<tr><td>Modul Nr.
20-00-0140</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0140-iv</td><td>Geometrische Methoden des CAE/CAD</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
● parametrische Kurvenmodelle
● parametrische Flächenmodelle
● Topologie und CAD-Volumenmodelle
● CAD-Operationen auf Flächen
● Tessellierung
● Approximation von Kurven und Flächen
● Finite-Elemente-Methode und Strömungssimulation
● verschiedene Anwendungen aus dem CAD-Bereich</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende beherrschen nach erfolgreichem Besuch der Veranstaltung die Grundlagen der rechnergestützten Methoden der geometrischen Modellierung und Simulation. Sie verstehen verschiedene parametrische Kurven- und Oberflächenrepräsentationen und können diese auswerten und miteinander vergleichen. Weiter kennen Sie klassische Datenstrukturen und Algorithmen aus dem Computer Aided Design (CAD). Sie sind in der Lage, diese Techniken praktisch umzusetzen und damit 3D-Geometrie im Rechner darzustellen und zu visualisieren.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Grundwissen in Informatik</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
</table>

7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Vorlesungsfolien Lee: Principles of CAD / CAM / CAE Systems, Addison-Wesley. Piegl, Tiller: The NURBS Book, Springer Verlag. Farin: Kurven und Flächen im Computer Aided Geometric Design, vieweg Shah, Mäntylä: Parametric and Feature-based CAD/CAM, Wiley & Sons
10	**Kommentar**

Modulbeschreibung

Modulname Bildverarbeitung						
Modul Nr. 20-00-0155	**Kreditpunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** i.d.R. jedes Sommersemester	
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0155-iv	Bildverarbeitung	3	integrierte Lehrveranstaltung	2

2 Lerninhalt

Überblick über die Grundlagen der Bildverarbeitung:
- Bildeigenschaften
- Bildtransformationen
- einfache und komplexere Filterung
- Bildkompression,
- Segmentierung
- Klassifikation

3 Qualifikationsziele / Lernergebnisse

Noch erfolgreichem Besuch der Veranstaltung haben die Studierenden einen Überblick über die Funktionsweise und die Möglichkeiten der modernen Bildverarbeitung. Studierende sind dazu in der Lage, einfache bis mittlere Bildverarbeitungsaufgaben selbständig zu lösen.

4 Voraussetzung für die Teilnahme

5 Prüfungsform

Fachprüfung schriftlich/mündlich 60-120/30 min.

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Modulabschlussprüfung (100%)

7 Benotung

Standard

8 Verwendbarkeit des Moduls

B.Sc. Informatik
M.Sc. Informatik
M.Sc. IT Sicherheit

	M.Sc. Autonome Systeme M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** ● Gonzalez, R.C., Woods, R.E., "Digital Image Processing", Addison- Wesley Publishing Company, 1992 ● Haberaecker, P., "Praxis der Digitalen Bildverarbeitung und Mustererkennung", Carl Hanser Verlag, 1995 ● Jaehne, B., "Digitale Bildverarbeitung", Springer Verlag, 1997
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Computer Vision I</td></tr>
<tr><td>Modul Nr.
20-00-0157</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 I</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</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: Besuch von Visual Computing</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
</table>

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Autonome Systeme M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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="7">Modulname
Virtuelle und Erweiterte Realität</td></tr>
<tr><td>Modul Nr.
20-00-0160</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0160-iv</td><td>Virtuelle und Erweiterte Realität</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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="6">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="6">Voraussetzung für die Teilnahme
Empfohlen: Grundlagen der Graphischen Datenverarbeitung (GDV)</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Autonome Systeme M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Dörner, R., Broll, W., Grimm, P., Jung, B. Virtual und Augmented Reality (VR / AR)
10	**Kommentar**

Modulbeschreibung

Modulname Algorithmen für Hardware-Entwurfswerkzeuge					
Modul Nr. 20-00-0183	**Kreditpunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** unregelmäßig
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0183-vl	Algorithmen für Hardware-Entwurfswerkzeuge	3	integrierte Lehrveranstaltung	2

2 Lerninhalt

- Das VLSI-Entwurfsproblem
- Grundlegende Graphenrepräsentationen und -algorithmen
- Darstellung von hierarchischen Schaltungen
- Realisierungstechnologien für integrierte Schaltungen
- Layout-Kompaktierung
- Timing-Analyse
- Heuristische Optimierungsverfahren
- Platzierungsprobleme, -verfahren und -kostenfunktionen
- Exakte Optimierungsverfahren
- Partitionierung mit Anwendung in der Platzierung
- Floorplanningprobleme, -repräsentationen und -verfahren
- Verdrahtungsprobleme, -verfahren und -kostenfunktionen

3 Qualifikationsziele / Lernergebnisse

Studierende kennen nach erfolgreichem Besuch der Veranstaltung verschiedene Technologien für die Realisierung von integrierten Schaltungen. Sie können aus den verschiedenen Technologien die Anforderungen an Automatisierungswerkzeuge für verschiedene Teilaufgaben des Entwurfs- und Realisierungsprozesses herleiten. Sie sind vertraut mit der Modellierung technologischer Probleme durch formale Konzepte wie Graphen, Gleichungssysteme etc. Sie verstehen grundlegende Verfahren zur Lösung auch von harten Problemen und können aufbauend auf Erfahrungen mit verschiedenen Basisalgorithmen neue bzw. verfeinerte Implementierungen zur Erledigung der Entwurfsaufgaben entwickeln.

4 Voraussetzung für die Teilnahme

Empfohlen: Empfohlen wird der erfolgreiche Besuch der Veranstaltungen “Digitaltechnik” sowie “Algorithmen und Datenstrukturen” und “Funktionale und objektorientierte Programmierung”.

5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Literaturempfehlungen werden kontinuierlich aktualisiert, Beispiele für verwendete Literatur könnten sein: Gerez: Algorithms for VLSI Design Automation Wang/Chang/Cheng: Electronic Design Automation
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Optimierung statischer und dynamischer Systeme</td></tr>
<tr><td>Modul Nr.
20-00-0186</td><td>Kreditpunkte
10 CP</td><td>Arbeitsaufwand
300 h</td><td>Selbststudium
210 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0186-iv</td><td>Optimierung statischer und dynamischer Systeme</td><td>10</td><td>integrierte Lehrveranstaltung</td><td>6</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Optimierung statischer Systeme:
- nichtlineare Optimierung ohne und mit Nebenbedingungen, notwendige Bedingungen
- numerische Newton-Typ- und SQP-Verfahren
- nichtlineare kleinste Quadrate
- gradientenfreie Optimierungsverfahren
- praktische Aspekte wie Problemformulierung, Approximation von Ableitungen, Verfahrensparameter, Bewertung einer berechneten Lösung

Optimierung dynamischer Systeme:
- Parameteroptimierungs- und Schätzprobleme
- optimale Steuerungsprobleme
- Maximumprinzip und notwendige Bedingungen
- numerische Verfahren zur Berechnung optimaler Trajektorien
- optimale Rückkopplungssteuerung
- linear-quadratischer Regulator

Anwendungen und Fallstudien aus den Ingenieurwissenschaften und der Robotik
Theoretische und praktische Übungen sowie Programmieraufgaben zur Vertiefung der Fachkenntnisse und methodischen Fähigkeiten</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende besitzen nach erfolgreicher Teilnahme grundlegende Kenntnisse und methodische Fähigkeiten der Konzepte und Berechnungsverfahren der Optimierung statischer und dynamischer Systeme und deren Anwendungen bei Optimierungsaufgaben in den Ingenieurwissenschaften.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: grundlegende mathematische Kenntnisse und Fähigkeiten in Linearer Algebra, Analysis mehrerer Veränderlicher und Grundlagen gewöhnlicher Differentialgleichungen</td></tr>
</table>

5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Autonome Systeme M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** - vorlesungsbegleitende Folien zu einzelnen Themen der Lehrveranstaltung: - J. Nocedal, S.J. Wright: Numerical Optimization, Springer - C.T. Kelley: Iterative Methods for Optimization, SIAM Frontiers in Applied Mathematics - L.M. Rios, N.V. Sahinidis: Derivative-free optimization: a review of algorithms and comparison of software implementations, Journal of Global Optimization (2013) 56:1247-1293 - A.E. Bryson, Y.-C. Ho: Applied Optimal Control: Optimization, Estimation and Control, CRC Press - J.T. Betts: Practical Methods for Optimal Control and Estimation Using Nonlinear Programming, SIAM Advances in Design and Control
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Informationsvisualisierung und Visual Analytics</td></tr>
<tr><td>Modul Nr.
20-00-0294</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0294-iv</td><td>Informationsvisualisierung und Visual Analytics</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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="6">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

•Wissen über Hauptcharakteristika menschlicher visuellen Wahrnehmung in Informationsvisualisierung und Visual Analytics anwenden

•geeignete Evaluationsmethode für spezifische Situationen und Szenarien auswählen</td></tr>
</table>

4	**Voraussetzung für die Teilnahme** Empfohlen: Interesse an Methoden der Computergrafik und Visualisierung
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Visual Computing M.Sc. Internet- und Web-basierte Systeme B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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** Die Veranstaltung richtet sich an Informatiker, Wirtschaftsinformatiker, Mathematiker in Bachelor, Master und Diplomstudiengänge und weiteren interessierten Kreisen (z.B. Biologen, Psychologen)

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Software Engineering - Design and Construction</td></tr>
<tr><td>Modul Nr.
20-00-0341</td><td>Kreditpunkte
8 CP</td><td>Arbeitsaufwand
240 h</td><td>Selbststudium
180 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0341-iv</td><td>Software Engineering - Design and Construction</td><td>8</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Der primäre Inhalt der Veranstaltung ist der Entwurf modularer Software, um wartbare, wiederverwendbare und erweiterbare Sofwaresysteme zu erhalten.
Integraler Bestandteil der Veranstaltung ist die Diskussion der Beziehung zwischen den Eigenschaften fortschrittlicher Programmiersprachen und dadurch möglicher Entwurfsalternativen. Weiterhin wird die Auswirkung der Programmiersprache auf den Entwurf eines Softwaresystems als Ganzes besprochen.
Die Vorlesung behandelt insbesondere:
● Prinzipien des Klassenentwurfs unter Verwendung fortgeschrittener Entwurfsmuster und fortschrittlicher Programmiersprachen;
● Prinzipien des Entwurfs auf Paketebene;
● Architekturelle Stile;
● Dokumentation des Entwurfs;
● Refactorings existierender Software;
● Metriken zur Evaluierung von Entwürfen.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach dem erfolgreichen Abschluss der Lehrveranstaltung sind Studierende in der Lage die folgenden Aufgaben durchzuführen:

● Sie können den Entwurf existierender Systeme in Hinblick auf ihre Modularität analysieren und ggf. Refactorings vorschlagen, die der Verbesserung bzw. Wiederherstellung selbiger dienen.

● Sie verstehen die mittel- und langfristigen Auswirkung nicht-modularer Softwaresysteme.

● Sie kennen fortgeschrittene Entwurfsmuster und können diese in existierendem Code identifizieren und auch einsetzen, um neue Probleme zu lösen.

● Sie kennen etablierte architekturelle Stile und können diese einsetzen.</td></tr>
</table>

	● Sie verstehen, dass die Lösung eines Entwurfsproblems von der gewählten Programmiersprache abhängt und sind in der Lage entsprechende Entscheidungen kritisch zu hinterfragen.
4	**Voraussetzung für die Teilnahme** Empfohlen: Successful completion of the lecture Software Engineering
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Autonome Systeme M.Sc. Distributed Software Systems B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** ● Bass, L.; Clements, P.; Kazman, R. ; Software Architecture in Practice, Addison-Wesley ● Booch, G. Object-Oriented Analysis and Design with Applications. Addison-Wesley ● Budd, T. Introduction to Object-Oriented Programming. 2nd. ed., Addison-Wesley ● Buschmann, F. et al. Pattern-Oriented Software Architecture: A System of Patterns. John Wiley & Sons. ● Czarnecki, K. and Eisenecker, U. Generative Programming. Addison-Wesley. ● Garland, D. and Shaw, M. Software Architecture: Perspectives on an Emerging Discipline. Prentice Hall. ● Gamma, E. et al. Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley.

	● Martin, Robert. Agile Software Development. Principles, Patterns, and Practices. Pearson US Imports & PHIPEs. ● Riel, A. Object-Oriented Design Heuristics. Addison-Wesley.
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Statistisches Maschinelles Lernen</td></tr>
<tr><td>Modul Nr.
20-00-0358</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0358-iv</td><td>Statistisches Maschinelles Lernen</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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</td></tr>
<tr><td>3</td><td colspan="6">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.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard

In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.</td></tr>
</table>

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Autonome Systeme M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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
Serious Games</td></tr>
<tr><td>Modul Nr.
20-00-0366</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0366-iv</td><td>Serious Games</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Einführung in die Thematik „Serious Games“: wissenschaftlich-technische Grundlagen, Anwendungsgebiete und Trends. Die Einzelthemen umfassen unter anderem:
• Einführung in Serious Games
• Game Development, Game Design
• Game Technology, Tools und Engines
• Personalisierung und Adaption
• Interactive Digital Storytelling
• Authoring und Content Generation
• Multiplayer Games
• Game Interfaces und Sensor Technology
• Effects, Affects und User Experience
• Mobile Games
• Serious Games Anwendungsbereiche und Best-Practice Beispiele
Die Übungen enthalten Theorie- und Praxisanteile. Dabei wird die Verwendung einer Game Engine gelehrt.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nach erfolgreicher Teilnahme an der Vorlesung können die Studierenden das Konzept von „Serious Games“ erklären und in verschiedene Anwendungsbereiche (wie Bildung und Gesundheit) transferieren. Sie können das allgemeine Vorgehen bei der Entwicklung von Computerspielen beschreiben und können grundsätzliche Prinzipien des Game Designs, der Personalisierung / Adaption und des Interactive Digital Storytellings anwenden. Außerdem können sie weitere aktuelle Fragestellungen sowie deren Lösungen aus dem Bereich Serious Games skizzieren.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme</td></tr>
</table>

5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Autonome Systeme M.Sc. Visual Computing M.Sc. Internet- und Web-basierte Systeme B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Wird in der Vorlesung bekanntgegeben.
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Medizinische Bildverarbeitung</td></tr>
<tr><td>Modul Nr.
20-00-0379</td><td>Kreditpunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0379-vl</td><td>Medizinische Bildverarbeitung</td><td>3</td><td>integrierte Lehrveranstaltung</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Vorlesung gliedert sich in zwei Teile.
In der ersten Hälfte der Vorlesung wird die Funktionsweise von Geräten, welche medizinische Bilder liefern (CT, MRI, PET, SPECT, Ultraschall), erklärt.
In der zweiten Hälfte werden verschiedene Bildverarbeitungsmethoden erklärt, welche typischerweise für die Bearbeitung medizinischer Bilder eingesetzt werden.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Noch erfolgreichem Besuch der Veranstaltung haben die Studierenden einen Überblick über die Funktionsweise und die Möglichkeiten der modernen medizinischen Bildverarbeitung.
Studierende sind dazu in der Lage, einfache bis mittlere medizinische Bildverarbeitungsaufgaben selbständig zu lösen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Mathematische Grundlagen sind dringend empfehlenswert. Ferner wird empfohlen, die Vorlesung „Bildverarbeitung“ vorher besucht zu haben.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
B.Sc. Informatik
M.Sc. Informatik
M.Sc. IT Sicherheit
M.Sc. Visual Computing
B.Sc. Computational Engineering
M.Sc. Computational Engineering</td></tr>
</table>

	M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** 1) Heinz Handels: Medizinische Bildverarbeitung 2) 2) Gonzalez/Woods: Digital Image Processing (last edition) 3) 3) Bernd Jähne: Digitale Bildverarbeitung. 6. überarbeitete und erweiterte Auflage. Springer, Berlin u. a. 2005, ISBN 3-540-24999-0. 4) Kristian Bredies, Dirk Lorenz: Mathematische Bildverarbeitung. Einführung in Grundlagen und moderne Theorie. Vieweg+Teubner, Wiesbaden 2011, ISBN 978-3-8348-1037-3.
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Ambient Intelligence</td></tr>
<tr><td>Modul Nr.
20-00-0390</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>4</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>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Empfohlen für Studenten mit abgeschlossenem Bachelor-Studium, empfehlenswerte Vorlesung “Visual Computing“, Seminar „Multimodale Interaktion mit intelligenten Umgebungen“</td></tr>
</table>

5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Autonome Systeme M.Sc. Visual Computing M.Sc. Internet- und Web-basierte Systeme B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Wird jeweils passend zu den aktuellen Themen bekanntgegeben
10	**Kommentar**

Modulbeschreibung

Modulname Computer Vision II						
Modul Nr. 20-00-0401	**Kreditpunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** i.d.R. jedes Sommersemester	
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0401-iv	Computer Vision II	6	integrierte Lehrveranstaltung	4

2 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

3 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.

4 Voraussetzung für die Teilnahme

Empfohlen: Besuch von Visual Computing und Computer Vision I ist empfohlen.

5 Prüfungsform

Fachprüfung schriftlich/mündlich 60-120/30 min.

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Modulabschlussprüfung (100%)

7 Benotung

Standard

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Autonome Systeme M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>4</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++
Systemnahe und Parallele Programmierung</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
</table>

	In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Autonome Systeme M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>4</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>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nachdem Studierende die Veranstaltung besucht haben, können sie</td></tr>
</table>

	● 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 Algorithmen und Datenstrukturen sowie Programmierkenntnisse in Java werden erwartet
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Internet- und Web-basierte Systeme M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** ● Kai-Uwe Carstensen, Christian Ebert, Cornelia Endriss, Susanne Jekat, Ralf Klabunde: Computerlinguistik und Sprachtechnologie. Eine Einführung. 3. Auflage. Heidelberg: Spektrum, 2009. ISBN: 978-3-8274-20123-7. http://www.linguistics.rub.de/CLBuch/ ● T. Götz, O. Suhre: Design and implementation of the UIMA Common Analysis System, IBM Systems Journal 43(3): 476–489, 2004.

	● Adam Kilgarriff, Gregory Grefenstette: Introduction to the Special Issue on the Web as Corpus, Computational Linguistics 29(3): 333–347, 2003. ● Christopher D. Manning, Prabhakar Raghavan, Hinrich Schütze: Introduction to Information Retrieval, Cambridge: Cambridge University Press, 2008. ISBN: 978-0-521-86571-5. http://nlp.stanford.edu/IR-book/
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
Probabilistische Graphische Modelle</td></tr>
<tr><td>Modul Nr.
20-00-0449</td><td>Kreditpunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
i.d.R. jedes Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0449-iv</td><td>Probabilistische Graphische Modelle</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
● Auffrischung Wahrscheinlichkeits- & Bayes’sche Entscheidungstheorie
● Gerichtete und ungerichtete graphische Modelle und deren Eigenschaften
● Inferenz in Baumgraphen
● Approximative Inferenz in allgemeinen Graphen: Message Passing und Mean Field
● Lernen von gerichteten und ungerichteten Modellen
● Sampling-Methoden für Inferenz und Lernen
● Modellierung in Beispielanwendungen, inkl. Topic-Modelle
● Tiefe Netze
● Halb-überwachtes Lernen</td></tr>
<tr><td>3</td><td colspan="5">Qualifikationsziele / Lernergebnisse
Studierende haben nach erfolgreichem Besuch der Veranstaltung ein vertieftes Verständnis von probabilistischen graphischen Modellen. Sie beschreiben und analysieren die Eigenschaften graphischer Modelle und formulieren geeignete Modelle für konkrete Schätz- und Lernaufgaben. Sie verstehen Inferenzalgorithmen, beurteilen deren Eignung und gebrauchen diese für graphische Modelle in relevanten Anwendungen. Sie ermitteln weiterhin welche Lernverfahren sich eignen, um die Modellparameter anhand von Beispieldaten zu bestimmen, und wenden diese an.</td></tr>
<tr><td>4</td><td colspan="5">Voraussetzung für die Teilnahme
Empfohlen: Besuch von “Statistisches Maschinelles Lernen” ist empfohlen.</td></tr>
<tr><td>5</td><td colspan="5">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="5">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="5">Benotung
Standard</td></tr>
</table>

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Autonome Systeme M.Sc. Visual Computing M.Sc. Internet- und Web-basierte Systeme B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Literaturempfehlungen werden regelmäßig aktualisiert und beinhalten beispielsweise: ● D. Barber: “Bayesian Reasoning and Machine Learning”, Cambridge University Press 2012 ● D. Koller, N. Friedman: “Probabilistic Graphical Models: Principles and Techniques”, MIT Press 2009
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Medizinische Visualisierung</td></tr>
<tr><td>Modul Nr.
20-00-0467</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>4</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
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard

In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
B.Sc. Informatik</td></tr>
</table>

	M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Preim, Botha: Visual Computing for Medicine
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Capturing Reality</td></tr>
<tr><td>Modul Nr.
20-00-0489</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0489-iv</td><td>Capturing Reality</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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="6">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="6">Voraussetzung für die Teilnahme
Empfohlen: Der Besuch der Veranstaltung Graphische Datenverarbeitung I oder Computer Vision I sowie grundlegende Programmierkenntnisse in C/C++</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
</table>

	In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Autonome Systeme M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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>Kreditpunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
i.d.R. jedes Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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 Lehrveranstaltung</td><td>2</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

● Evaluationstechniken kennen gelernt und angewandt</td></tr>
</table>

4	**Voraussetzung für die Teilnahme**
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Visual Computing M.Sc. Distributed Software Systems M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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

<table>
<tr><td colspan="7">Modulname
Foundations of Language Technology</td></tr>
<tr><td>Modul Nr.
20-00-0546</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0546-iv</td><td>Foundations of Language Technology</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Vorlesung bietet eine Einführung in die zentralen Sichtweisen, Probleme, Methoden und Techniken der automatischen Sprachtechnologie am Beispiel der Programmiersprache Python.

Zentrale Inhalte:

● Sprachtechnologie/Natural language processing (NLP)
○ Tokenisierung
○ Segmentierung
○ Wortartenerkennung
○ Korpora
○ Statistische Analyse
● Maschinelles Lernen
○ Kategorisierung und Klassifikation
○ Informationsextraktion
● Einführung in Python
○ Datenstrukturen
○ Strukturierte Programmierung
○ Arbeiten mit Dateien
○ Einsatz von Bibliotheken
○ Programmbibliothek NLTK

Die Veranstaltung basiert auf der Klassenbibliothek NLTK für Python. Diese bietet einen mächtigen Werkzeugkasten, um die theoretischen Methoden explorativ und problemlösend einzusetzen, ohne umfangreiche Programmierkenntnisse vorauszusetzen.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Nachdem Studierende die Veranstaltung besucht haben, können sie</td></tr>
</table>

	● die grundlegende Terminologie der automatischen Sprachtechnologie definieren, ● wesentliche Fragestellungen dieses Gebietes benennen und erläutern, ● einfache Pythonprogramme erklären und selbst implementieren, ● die gelernten Methoden und Techniken auf konkrete Anwendungsszenarien des Textverstehens übertragen sowie ● deren Möglichkeiten und Grenzen kritisch beurteilen.
4	**Voraussetzung für die Teilnahme** Empfohlen:
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Internet- und Web-basierte Systeme M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Steven Bird, Ewan Klein, Edward Loper: Natural Language Processing with Python, O'Reilly, 2009. ISBN: 978-0596516499. http://www.nltk.org/book/
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Lernende Roboter</td></tr>
<tr><td>Modul Nr.
20-00-0629</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0629-vl</td><td>Lernende Roboter</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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</td></tr>
<tr><td>3</td><td colspan="6">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.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Gute Programmierkenntnisse in Matlab, Machine Learning 1 - Statistical Approaches sind hilfreich aber nicht zwingend erforderlich</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
</table>

7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Autonome Systeme M.Sc. Visual Computing M.Sc. Internet- und Web-basierte Systeme B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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

IT-Lösungen durch praxiserprobtes Software Engineering</td></tr>
<tr><td>Modul Nr.
20-00-0635</td><td>Kreditpunkte
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-Sicherheit</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>20-00-0635-iv</td><td>IT-Lösungen durch praxiserprobtes Software Engineering</td><td>0</td><td>Integrierte Veranstaltung</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
- Modellierung mit UML bzw. DSL und Code-Generierung</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Teilnehmer lernen theoretisch und praktisch - anhand von Fallbeispielen aus der Praxis - wie Software-Engineering zur Erarbeitung von IT-Lösungen eingesetzt wird. Dabei werden moderne, praxiserprobte Konzepte zur Erstellung von IT-Lösungen vorgestellt, zum Beispiel Modellierung (Geschäftsprozesse, UML, DSL), Generierung und Testautomatisierung. Die Teilnehmer können die Wirtschaftlichkeit von IT-Projekten bewerten, praxiserprobte Projektmanagement-Pattern einsetzen und lernen die umgebenden Rahmenbedingungen einer IT-Organisation swoie die Rolle des CIO in einem Unternehmen als Berater der Fachbereiche kennen. Sie beherrschen das Anforderungsmanagement und den Lösungsentwurf, insbesondere für mobile Anwendungen und SAP-Lösungen. Die Veranstaltung wird durch eingeladene Vorträge von Experten aus der Praxis ergänzt.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Funktionale und objektorientierte Programmierkonzepte

Algorithmen und Datenstrukturen

Einführung in Software Engineering</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-0635-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0635-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Optimierungsalgorithmen</td></tr>
<tr><td>Modul Nr.
20-00-0667</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0667-iv</td><td>Optimierungsalgorithmen</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Algorithmische Standardansätze für komplexe diskrete Optimierungsprobleme, bspw. Evolutionsstrategien, dynamische Programmierung, Branch-and-Bound u.ä.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
In der Veranstaltung erwerben Studierende systematische Kenntnis generischer algorithmischer Ansätze in der diskreten Optimierung sowie die Fähigkeit, komplexe diskrete Optimierungsprobleme Ziel führend algorithmisch anzugehen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Funktionale und objektorientierte Programmierkonzepte, Algorithmen und Datenstrukturen oder vergleichbar.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard

In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
B.Sc. Informatik
M.Sc. Informatik
M.Sc. IT Sicherheit
M.Sc. Visual Computing
B.Sc. Computational Engineering</td></tr>
</table>

	M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Wird in der Veranstaltung bekannt gegeben
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Physikalisch-basierte Animation</td></tr>
<tr><td>Modul Nr.
20-00-0682</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0682-iv</td><td>Physikalisch-basierte Animation</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
1. Grundlagen der physikalisch-basierten Animation
- Anwendungen
- Simulationsmodelle
- Definition holonomer und nichtholonomer Zwangsbedingungen
- Bewegungsgleichungen für Partikel
- Gewöhnliche Differentialgleichungen
- Numerische Integrationsverfahren
2. Partikelsysteme
- Aufbau von Partikelsystemen
- Simulation physikalischer Effekte
3. Simulation von Haaren
- Haarmodelle
- Simulationsverfahren
- Haar-Haar Interaktion
4. Simulation von Kleidung
- Masse-Feder-Systeme
- Finite-Elemente-Methoden
- Positionsbasierte Verfahren
5. Simulation von Weichkörpern
- Generierung von Volumennetzen
- Masse-Feder-Systeme
- Finite-Elemente-Methoden
- Positionsbasierte Verfahren
- Volumenerhaltung
6. Starrkörper
- Grundlagen
- Bewegungsgleichungen für Starrkörper
- Simulation von Gelenken
7. Kollisionserkennung</td></tr>
</table>

	- Hüllkörper - Hüllkörperhierarchien - Zellrasterverfahren - Kollisionstests für Starrkörper - Kollisionstests für deformierbare Körper - Kontinuierliche Kollisionserkennung - Bildbasierte Verfahren 8. Brüche - Animation von Brüchen mit Bruchmustern - Simulation spröder Brüche - Anpassung des Simulationsnetzes
3	**Qualifikationsziele / Lernergebnisse** Studierende kennen nach einem erfolgreichen Besuch der Veranstaltung Mehrkörpersysteme und diskrete und kontinuierliche deformierbare Simulationsmodelle. Sie verstehen die numerischen Simulationsverfahren sowie deren jeweiligen Anwendungsbereiche und können diese Verfahren anwenden. Sie haben einen grundlegenden Überblick über Verfahren der Echtzeitsimulation in der Computergraphik.
4	**Voraussetzung für die Teilnahme** Empfohlen: Grundlegende Kenntnisse von Numerik, Algorithmen und Datenstrukturen, Computergraphik
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Visual Computing B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.

9	**Literatur** wird in der Vorlesung bekannt gegeben
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Fortgeschrittener Compilerbau</td></tr>
<tr><td>Modul Nr.
20-00-0701</td><td>Kreditpunkte
5 CP</td><td>Arbeitsaufwand
150 h</td><td>Selbststudium
105 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>5</td><td>integrierte Lehrveranstaltung</td><td>3</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”</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Fachprüfung schriftlich/mündlich 60-120/30 min.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
</table>

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Distributed Software Systems B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik M.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch 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
Grundlagen der Robotik</td></tr>
<tr><td>Modul Nr.
20-00-0735</td><td>Kreditpunkte
10 CP</td><td>Arbeitsaufwand
300 h</td><td>Selbststudium
210 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0735-iv</td><td>Grundlagen der Robotik</td><td>0</td><td>integrierte Lehrveranstaltung</td><td>6</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Lehrveranstaltung behandelt räumliche Darstellungen und Transformationen, Manipulatorkinematik, Fahrzeugkinematik, kinematische Geschwindigkeit, Jacobi-Matrix, Roboterdynamik, Robotersensoren und -antriebe, Roboterregelungen, Bahnplanung, Lokalisierung und Navigation mobiler Roboter, Roboterautonomie und Roboterentwicklung.

Theoretische und praktische Übungen sowie Programmieraufgaben dienen zur Vertiefung der Lehrinhalte.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende besitzen nach erfolgreicher Teilnahme die für grundlegende Untersuchungen und ingenieurwissenschaftliche Entwicklungen in der Robotik notwendigen grundlegenden Fachkenntnisse und methodischen Fähigkeiten im Bereich der Modellierung, Kinematik, Dynamik, Regelung, Bahnplanung, Navigation, Wahrnehmung und Autonomie von Robotern.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen werden mathematische Grundkenntnisse und -fähigkeiten in Linearer Algebra, Analysis mehrerer Veränderlicher und Grundlagen gewöhnlicher Differentialgleichungen.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0735-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)

In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. § 25 (2) der 5. Novelle der APB und den vom FB 20 am 30.3.2017 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0735-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik M. Sc. IT Sicherheit M. Sc. Autonome Systeme M. Sc. Visual Computing B. Sc. Computational Engineering M. Sc. Computational Engineering M. Sc. Wirtschaftsinformatik B. Sc. Psychologie in IT Joint B.A. Informatik B. Sc. Sportwissenschaft und Informatik M. Sc. Sportwissenschaft und Informatik M. Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** - vorlesungsbegleitendes Skript und Vorlesungsfolien Umfassende Übersicht der Robotik: - B. Siciliano, O. Khatib: Springer Handbook of Robotics, Springer Verlag zu einzelnen Themen der Lehrveranstaltung: - J.J. Craig: Introduction to Robotics: Mechanics and Control, 3rd edition, Prentice Hall - M.W. Spong, S. Hutchinson, M. Vidyasagar: Robot Modeling and Control, Wiley - R. Siegwart, I.R. Nourbakhsh, D. Scaramuzza: Introduction to Autonomous Mobile Robots, MIT Press - H. Choset, K.M. Lunch, S. Hutchinson, G.A. Kantor,W. Burgard, L.E. Kavraki, S. Thrun: Principles of Robot Motion: Theory, Algorithms, and Implementations, Bradford - S. Thrun,W. Burgard, D. Fox: Probabilistic Robotics, MIT Press
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="6">Modulname
Mobile Netze</td></tr>
<tr><td>Modul Nr.
20-00-0748</td><td>Kreditpunkte
6 CP</td><td>Arbeitsaufwand
180 h</td><td>Selbststudium
120 h</td><td>Moduldauer
1 Semester</td><td>Angebotsturnus
i.d.R. jedes Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="3">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0748-iv</td><td>Mobile Netze</td><td>6</td><td>integrierte Lehrveranstaltung</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="5">Lerninhalt
Mobilkommunikation und drahtlose Kommunikationstechniken haben sich in den letzten Jahren rapide weiterentwickelt. Die integrierte Lehrveranstaltung 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** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit M.Sc. Autonome Systeme M.Sc. Internet- und Web-basierte Systeme M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik B.Sc. Informationssystemtechnik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.

9	**Literatur** Ausgewählte Buchkapitel und ausgewählte wissenschaftliche Veröffentlichungen
10	**Kommentar**

Modulbeschreibung

Modulname

Deep Learning für Natural Language Processing

Modul Nr.	Kreditpunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-0947	6 CP	180 h	120 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Deutsch	Koordinatoren/Koordinatorinnen IT-Sicherheit

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0947-iv	Deep Learning für Natural Language Processing	0	Integrierte Veranstaltung	4

2 Lerninhalt

Die Veranstaltung bietet eine Einführung in die grundlegenden Konzepte des Deep Learning und ihren Einsatz für Problemstellungen im Bereich Natural Language Processing (NLP).

Zentrale Inhalte:
- grundlegende Konzepte des Deep Learning (e.g. Feed-Forward Netze, Hidden Layers, Backpropagation, Aktivierungs- und Loss-Funktionen)
- Word Embeddings: Theorie, unterschiedliche Ansätze und Modelle, Verwendung in maschinellen Lernverfahren
- neuronale Netzwerkarchitekturen (e.g. recurrent NN, recursive NN, convolutional NN) für verschiedene Gruppen von NLP-Problemen wie die Klassifikation von Dokumenten (z.B. Spamerkennung), die Bestimmung von Sequenzen (z.B. POS-Tagging, Named Entity Recognition) und komplexeren Strukturen (z.B. Chunking, Parsing, Semantic Role Labeling)

Die Veranstaltung strebt eine enge Verzahnung zwischen theoretischen Konzepten und ihrer praktischen Verwendung zur Lösung typischer Problemstellungen bei Datenanalyse auf freien Texten mit Hilfe von existierenden Programm-Bibliotheken in Python an.

3 Qualifikationsziele / Lernergebnisse

Nachdem Studierende die Veranstaltung abgeschlossen haben, können sie
- die grundlegenden Konzepte von neuronalen Netzen und Deep Learning erklären.
- Word Embeddings erklären, trainieren und für die Lösung von NLP-Problemen einsetzen.
- neuronale Netzwerkarchitekturen für NLP-Probleme wie die Klassifizierung von Dokumenten und das Bestimmen linguistischer Sequenzen (z.B. POS-Tagging) und Strukturen (z.B. Chunking) verstehen und beschreiben.
- neuronale Netzwerke für NLP-Probleme mit Hilfe existierender Bibliotheken in Python implementieren.

4 Voraussetzung für die Teilnahme

Empfohlen: Grundlegende Mathematik- und Programmierkenntnisse

5 Prüfungsform

Bausteinbegleitende Prüfung:

	• [20-00-0947-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0947-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

Concepts and Technologies for Distributed Systems and Big Data Processing</td></tr>
<tr><td>Modul Nr.
20-00-0951</td><td>Kreditpunkte
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-Sicherheit</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>20-00-0951-iv</td><td>Concepts and Technologies for Distributed Systems and Big Data Processing</td><td>0</td><td>Integrierte Veranstaltung</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
The course provides an overview of recent advances in distributed systems for Big Data processing. The course starts presenting computational models for high throughput batch processing like MapReduce. Next, we will introduce software engineering techniques for distributed systems such as REST and component-based architectures. We will then cover low latency real time stream processing and complex event processing. Finally, we will present advanced topics in distributed data-intensive systems, such as geodistribution and security.

The course focuses both on the fundamental concepts as well as on the concrete technologies and applications of the aforementioned techniques to real-world case studies.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
- The students are familiar with basic concepts and technologies on distributed systems and big data and are able to implement basic cloud based/distributed applications.

- The students are familiar with the fundamental computational models behind recent advances in distributed systems, such as models for batch processing of massive data amounts, stream processing and complex event processing.

- The students are familiar with selected advanced topics on big data, including security and geolocalization.

- The students know about real-world case studies that apply the concepts and the technologies presented during the course.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

This course is targeted at master students.</td></tr>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0951-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Pass exam (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0951-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0953-iv	Multithreading in C++	0	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)

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%)

Studierende, die die Veranstaltung 20-00-0801 abgeschlossen haben, dürfen diese Veranstaltung nicht einbringen.

7 Benotung

	Bausteinbegleitende Prüfung: • [20-00-0953-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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>Kreditpunkte
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-Sicherheit</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>0</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)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)

Diese Modul ersetzt das bisherige Modul "Fortgeschrittene parallele Programmierung 2"</td></tr>
</table>

	(FPPROG2), 20-00-0938. Studierende, die eine Prüfung in FPPROG2 absolviert haben, können keine in diesem Modul machen.
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0977-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Beherrschen Moderner Prozessoren für Eingebettete Systeme						
Modul Nr. 20-00-1004	**Kreditpunkte** 5 CP	**Arbeitsaufwand** 150 h	**Selbststudium** 105 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			
1	**Kurse des Moduls**					
	Kurs Nr.	**Kursname**	**Arbeitsaufwand (CP)**	**Lehrform**	**SWS**	
	20-00-1004-iv	Beherrschen Moderner Prozessoren für Eingebettete Systeme	0	Integrierte Veranstaltung	3	
2	**Lerninhalt** * Prozessorarchitekturen in Eingebetteten Systemen * ARM Instruktionssatz und Mikroarchitektur * ARM Compiler und Simulatoren * ARM Bootloading und (Echtzeit-)Betriebssysteme * ARM Debugging, Profiling und Tracing * ARM Ansteuerung von Peripheriekomponenten * ARM Power Management * ARM Anwendungsklassen (Cortex-M/-A/-R) * Entwicklungsperspektiven eingebetteter Prozessoren * Aktuelle Forschungsergebnisse						
3	**Qualifikationsziele / Lernergebnisse** Nach erfolgreichem Abschluss der Lehrveranstaltung können Studierende * die wesentlichen Bestandteile und Funktionsweisen von eingebetteten Prozessoren skizzieren, * die Vor- und Nachteile verschiedener Prozessorarchitekturen differenzieren, * wichtige Entwicklungswerkzeuge für eingebettete Prozessoren anwenden, * existierenden Programmcode auf Funktionalität und Effizienz untersuchen, * effizienten Programmcode für spezifische Anwendungen entwickeln, * aktuelle Forschungsarbeiten zu eingebetteten Systemen einschätzen.						
4	**Voraussetzung für die Teilnahme** Empfohlen: Erfolgreiche Teilnahme an der Veranstaltung "Rechnerorganisation" oder vergleichbare Qualifikationen						
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1004-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)						

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1004-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1017-iv	Skalierbares Datenmanagement	0	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 sollen die Studierenden einen Überblick über die wichtigsten Konzepte, Algorithmen und System-Aspekte für skalierbare Datenmanagement-Systeme erworben haben. 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
Informationsmanagement (20-00-0015-iv)

Optional:
Foundations of Distributed Systems (20-00-0998-iv)

5 Prüfungsform

Bausteinbegleitende Prüfung:

	• [20-00-1017-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1017-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M. Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1034-iv	Deep Learning: Architectures & Methods	0	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:

20-00-0358-iv Statistisches Maschinelles Ler-nen
20-00-0052-iv Data Min-ing und Maschinelles Ler-nen

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1034-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1034-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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>Modul Nr.
20-00-1047</td><td>Kreditpunkte
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-Sicherheit</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>0</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.
Vorherige Belegung der Vorlesung Statistical Machine Learning ist hilfreich aber nicht zwingend erforderlich</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1047-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1047-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname
Einführung in die Künstliche Intelligenz

Modul Nr.	Kreditpunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-1058	5 CP	150 h	105 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Deutsch	Koordinatoren/Koordinatorinnen IT-Sicherheit

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1058-iv	Einführung in die Künstliche Intelligenz	0	Integrierte Veranstaltung	3

2 Lerninhalt

Die Künstliche Intelligenz (KI) beschäftigt sich mit Algorithmen zur Lösung von Problemen, von denen man gemeinhin annimmt, dass deren Lösung Intelligenz erfordert. Orientierte man sich in den Anfangstagen der Wissenschaft primär an psychologischen Erkenntnissen über das menschliche Denken, hat sich das Gebiet seither zunehmend dahingehend entwickelt, dass in den Problemlösungsansätzen versucht wird, die Stärken des Computers auszunutzen. Im Zuge dieser Vorlesung werden wir einen kurzen Überblick über die zentralen Themen dieser Kernwissenschaft der Informatik geben, insbesondere in die Themen Suche, Planen, Lernen und Schließen. Die historischen und philosophischen Grundlagen werden ebenfalls behandelt.

- Grundlagen
- Einführung, Geschichte der AI (RN chapter 1)
- Intelligente Agenten (RN chapter 2)
- Suche
- Uninformierte Suche (RN chapters 3.1 - 3.4)
- Heuristische Suche (RN chapters 3.5, 3.6)
- Lokale Suche (RN chapter 4)
- Constraint Satisfaction Problems (RN chapter 6)
- Spiele: Suche mit Gegnern (RN chapter 5)
- Planning
- Planen im Zustandsraum (RN chapter 10)
- Planen im Planraum (RN chapter 11)
- Decisions under Uncertainty
- Unsicherheit und Wahrscheinlichkeiten (RN chapter 13)
- Bayesian Networks (RN chapter 14)
- Decision Making (RN chapter 16)
- Machine Learning
- Neural Networks (RN chapters 18.1,18.2,18.7)
- Reinforcement Learning (RN chapter 21)
- Philosophische Grundlagen

3 Qualifikationsziele / Lernergebnisse

Nach der erfolgreichen Absolvierung dieser Lehrveranstaltung sind die Studenten in der Lage
- grundlegende Techniken der Künstlichen Intelligenz zu verstehen und erklären

	- in einer Diskussion über die prinzipielle Möglichkeit der Schaffung einer Künstlichen Intelligenz fundierte Argumente vorzubringen - neue Entwicklungen auf diesem Gebiet kritisch beurteilen
4	**Voraussetzung für die Teilnahme** Keine
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1058-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1058-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname

Advanced C++modern programming

Modul Nr.	Kreditpunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-1068	3 CP	90 h	60 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Englisch	Koordinatoren/Koordinatorinnen IT-Sicherheit

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1068-iv	Advanced C++ modern programming	0	Integrierte Veranstaltung	2

2 Lerninhalt

Die Vorlesung wird die letzten Änderungen und Erweiterungen der Sprache C++ behandeln und insbesondere auf die Standards:
ISO/IEC 14882:2011, 14882:2014, and 14882:2017 eingehen.

Die Liste der Themen:
1. Einführung in modernes C++
2. Verbessertes Typsystem
3. Uniforme Initialisierung
4. Moderner Ansatz in Hinblick auf den Entwurf und Implementierung von Klassen
5. Verbesserungen für die Entwicklung von Bibliotheken
6. Moderne "generische Programmierung"
7. Einführung in die Metaprogrammierung
8. Vereinfachung von Code durch den Einsatz von Standardkomponenten
9. STL: Containers, Algorithmen und Iteratoren
10. Neueste Entwicklungen: C++17
11. Die Zukunft von C++: C++20

3 Qualifikationsziele / Lernergebnisse

+ Die Studierenden werden in der Lage sein die Hauptunterschiede zwischen den modernen C++ Standards zu benennen
+ Die Studierenden haben ein vertieftes Verständnis moderner "generischer Programmierung"
+ Die Studierenden sind in der Lage die neuen Hauptkomponenten der C++ Standardbibliothek zu verwenden
+ Die Studierenden können Abwägungen zwischen Flexibilität und Performance in modernen C++ nachvollziehen
+ Die Studierenden haben ein Überblick über die Wahrscheinlichsten Entwicklungsschritte

4 Voraussetzung für die Teilnahme

Empfohlen:
+ Grundlagenwissen von C und C++
+ Vertrautheit mit den Grundlagen object-orientierter und generischer Programmierung
+ Grundlagenwissen im Bereich funktionale Programmierung

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1068-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1068-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Software-Engineering für Künstliche Intelligenz</td></tr>
<tr><td>Modul Nr.
20-00-1097</td><td>Kreditpunkte
4 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-Sicherheit</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>20-00-1097-se</td><td>Software-Engineering für Künstliche Intelligenz</td><td>0</td><td>Seminar</td><td>3</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Künstliche Intelligenz (KI) ist mittlerweile Bestandteil vieler datengetriebenen Anwendungen; zum Beispiel in der Finanzindustrie, Medizin, Kognitionswissenschaft oder Biologie. Derartige Ansätze des maschinellen Lernens (ML) erfordern eine genaue Domänen- und Anforderungsanalyse, angemessenes Softwaredesign und -Entwicklung, besonderes Testen und Debugging sowie spezielle Techniken, um Skalierbarkeit und Wartbarkeit sicherzustellen. Während KI-Systeme zunehmend größeren Einfluss in vielen Bereichen besitzen, verwenden Entwickler und Data-Scientists weiterhin Methoden (Scripting, informelle/nicht-verschriftlichte Spezifikationen, trial-and-error Testing), die nicht dem aktuellen Stand der Technik in den Ingenieursdisziplinen entsprechen. Vor diesem Hintergrund ist es von entscheidender Bedeutung die Jahrzehnte lange Entwicklung im Software-Engineering (SE) zur Systematisierung von Entwicklungsprozessen für diesen Bereich zu nutzen.

In diesem Kurs wird Studierenden ein Thema im Bereich SE für KI zugewiesen. Ausgehend von vorgegebenen Quellen und persönlicher erweiternder Literaturrecherche bereiten Studierende eine Präsentation mit anschließender Diskussion vor. Diese werden an regelmäßigen Terminen gehalten. Alle Studierenden, die an einem Termin nicht präsentieren, bereiten sich auf die jeweilige Diskussion mit einführendem Lesematerial vor. Die Benotung basiert auf der Vorbereitung und der Präsentation der zugewiesenen Themenschwerpunkte sowie auf der Teilnahme an allen Diskussionen.

Beachten Sie bitte die Kursseite für mehr Informationen und Ankündigungen:
https://allprojects.github.io/SE4AI/</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Studenten entwickeln ein tieferes Verständnis zu SE für KI. Dies umfasst die Schwerpunkte Requirements Engineering, Qualitätssicherung, Entwicklungsprozesse sowie Softwarearchitektur und -Design für Modularität, Wiederverwendbarkeit, Effizienz, Skalierbarkeit, Fairness und Privatsphäre.

Die Studierenden lernen die Vorbereitung und Präsentation von wissenschaftlichen Inhalten für ein Publikum mit unterschiedlichem Hintergrundwissen. Außerdem üben die Studierenden die</td></tr>
</table>

	effiziente Vorbereitung von und aktive Teilnahme an wissenschaftlichen Diskussionen sowie deren Moderation.
4	**Voraussetzung für die Teilnahme** Empfohlen: Basiswissen zu Software-Engineering. Interesse an Künstlicher Intelligenz.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1097-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%).
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1097-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Grundlagen der Bioinformatik						
Modul Nr. 10-30-0036	**Kreditpunkte** 4 CP	**Arbeitsaufwand** 120 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** i.d.R. jedes Sommersemester	
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
10-01-0036-vl	Bioinformatik-Vorlesung	2	Vorlesung	2
10-01-0036-se	Bioinformatik-Übung	2	Übung	2

2 Lerninhalt

Algorithmen für die Sequence Analyse und Alignments
Molekulare Visualisierung
Algorithmen für Strukturvorhersage und Homologiemodellierung
Molecular Dynamics als Simulationstechnik in HPC

3 Qualifikationsziele / Lernergebnisse

Die Studenten erwerben Grundlagenwissen in der sequenz-basierten Bioinformatik (Sequence Alignment, Scoring Schemata, Datenbanken, Mustererkennung) und der

Strukturmodellierung und Simulation (Strukturvorhersage, Molekulardynamik).

Die Studenten werden in die Lage versetzt, eigenständig Standard-Werkzeuge der

Bioinformatik einzusetzen und deren grundlegende Algorithmen in diversen

Implementierungen zu identifizieren. Notwendige statistische und mathematische Grundlagen werden vermittelt und in Übungen und Seminarstunden vertieft.

4 Voraussetzung für die Teilnahme

5 Prüfungsform

Fachprüfung schriftlich/mündlich 60-120/30 min.

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Modulabschlussprüfung (100%)

7 Benotung

	Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 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 Sicherheit B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** ● Deonier, Tavare, Waterman Computational Genome Analysis, Springer, 2005 ● Durbin, Eddy, Krogh, Mitchison, Biological Sequence Analysis, Cambridge University Press, ● 1998 ● MacKay, Information Theory, Inference, and Learning Algorithms, Cambridge University ● Press, 2003 ● Schlick, Molecular Modeling and Simulation, Springer, 2002
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Kommunikationsnetze I</td></tr>
<tr><td>Modul Nr.
18-sm-1010</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>18-sm-1010-vl</td><td>Kommunikationsnetze I</td><td></td><td>Vorlesung</td><td>3</td></tr>
<tr><td>18-sm-1010-ue</td><td>Kommunikationsnetze I</td><td></td><td>Übung</td><td>1</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
In dieser Veranstaltung werden die Technologien, die Grundlage heutiger Kommunkationsnetze sind, vorgestellt und analysiert.
Die Vorlesung deckt grundlegendes Wissen über Kommunikationssysteme ab und betrachtet im Detail die 4 unteren Schichten des ISO-OSI-Modells: Bitübertragungsschicht, Sicherungsschicht, Vermittlungsschicht und Teile der Transportschicht.
Die Bitübertragungsschicht, die zuständig ist für eine adäquate Übertragung über einen Kanal, wird kurz betrachtet. Danach werden fehlertolerante Kodierung, Flusskontrolle und Zugangskontrollverfahren (Medium access control) der Sicherungsschicht betrachtet. Anschließend wird die Netzwerkschicht behandelt. Der Fokus liegt hier auf Wegefindungs- und Überlastkontrollverfahren. Abschließend werden grundlegende Funktionen der Transportschicht betrachtet. Dies beinhaltet UDP und TCP- Das Internet und dessen Funktionsweise wird im Laufe der Vorlesung detailliert betrachtet.
Themen sind:

- ISO-OSI und TCP/IP Schichtenmodelle
- Aufgaben und Eigenschaften des Bitübertragungsschicht
- Kodierungsverfahren der Bitübertragungsschicht
- Dienste und Protokolle der Sicherungsschicht
- Flußkontrolle (sliding window)
- Anwendungen: LAN, MAN, High-Speed LAN, WAN
- Dienste der Vermittlungsschicht
- Wegefindungsalgorithmen
- Broadcast- und Multicastwegefindung
- Überlastbehandlung
- Adressierung
- Internet Protokoll (IP)</td></tr>
</table>

	- Netzbrücken - Mobile Netze - Services und Protokolle der Transportschicht - TCP, UDP
3	**Qualifikationsziele / Lernergebnisse** Diese Vorlesung betrachet Grundfunktionalitäten, Serives, Protokolle, Algorithmen und Standards von Kommunikationssystemen. Vermitteltet Kompetenzen sind grundlegedes Wissen über die vier unteren Schichten des ISO-OSI-Modells: Bitübertragungsschicht, Sicherungsschicht, Vermittlungsschicht und Transportschicht. Desweiteren wird Grundwissen über Kommunikationssysteme vermittelt. Besucher der Vorlesung werden Funktionen heutiger Netzwerketechnologien und des Internets erlernen.
4	**Voraussetzung für die Teilnahme**
5	**Prüfungsform** Fachprüfung schriftlich/mündlich 60-120/30 min.
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard In dieser Vorlesung findet eine Anrechnung von vorlesungsbegleitenden Leistungen statt, die lt. §25(2) der 4. Novelle der APB und den vom FB 20 am 02.10.2012 beschlossenen Anrechnungsregeln zu einer Notenverbesserung um bis zu 1.0 führen kann.
8	**Verwendbarkeit des Moduls** Wi-CS, Wi-ETiT, BSc CS, BSc ETiT, BSc iST
9	**Literatur** Ausgewählte Kapitel aus folgenden Büchern: - Andrew S. Tanenbaum: Computer Networks, 5th Edition, Prentice Hall, 2010 - Andrew S. Tanenbaum: Computernetzwerke, 3. Auflage, Prentice Hall, 1998 - Larry L. Peterson, Bruce S. Davie: Computer Networks: A System Approach, 2nd Edition, Morgan Kaufmann Publishers, 1999 - Larry L. Peterson, Bruce S. Davie: Computernetze, Ein modernes Lehrbuch, 2. Auflage, Dpunkt Verlag, 2000 - James F. Kurose, Keith W. Ross: Computer Networking: A Top-Down Approach Featuring the Internet, 2nd Edition, Addison Wesley-Longman, 2002 - Jean Walrand: Communication Networks: A First Course, 2nd Edition, McGraw-Hill, 1998
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Kommunikationsnetze II</td></tr>
<tr><td>Modul Nr.
18-sm-2010</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>18-sm-2010-vl</td><td>Kommunikationsnetze II</td><td></td><td>Vorlesung</td><td>3</td></tr>
<tr><td>18-sm-2010-ue</td><td>Kommunikationsnetze II</td><td></td><td>Übung</td><td>1</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Vorlesung Kommunikationsnetze II umfasst die Konzepte der Computervernetzung und -telekommunikation mit dem Fokus auf dem Internet. Beginnend mit der Geschichte werden in der Vorlesung vergangene, aktuelle und zukünftige Aspekte von Kommunikationsnetzen behandelt. Zusätzlich zu bekannten Protokollen und Technologien wird eine Einführung in Neuentwicklungen im Bereich von Multimedia Kommunikation (u.a. Video Streaming, P2P, IP-Telefonie, Cloud Computing und Service-orientierte Architekturen) gegeben. Die Vorlesung ist als Anschlussvorlesung zu Kommunikationsnetze I geeignet.
Themen sind:

- Grundlagen und Geschichte von Kommunikationsnetzen (Telegrafie vs. Telefonie, Referenzmodelle, ...)
- Transportschicht (Adressierung, Flusskontrolle, Verbindungsmanagement, Fehlererkennung, Überlastkontrolle, ...)
- Transportprotokolle (TCP, SCTP)
- Interaktive Protokolle (Telnet, SSH, FTP, ...)
- Elektronische Mail (SMTP, POP3, IMAP, MIME, ...)
- World Wide Web (HTML, URL, HTTP, DNS, ...)
- Verteilte Programmierung (RPC, Web Services, ereignisbasierte Kommunikation)
- SOA (WSDL, SOAP, REST, UDDI, ...)
- Cloud Computing (SaaS, PaaS, IaaS, Virtualisierung, ...)
- Overlay-Netzwerke (unstrukturierte P2P-Systeme, DHT-Systeme, Application Layer Multicast, ...)
- Video Streaming (HTTP Streaming, Flash Streaming, RTP/RTSP, P2P Streaming, ...)
- VoIP und Instant Messaging (SIP, H.323)</td></tr>
</table>

3	**Qualifikationsziele / Lernergebnisse** Die Vorlesung Kommunikationsnetze II umfasst die Konzepte der Computervernetzung und -telekommunikation mit dem Fokus auf dem Internet. Beginnend mit der Geschichte werden in der Vorlesung vergangene, aktuelle und zukünftige Aspekte von Kommunikationsnetzen behandelt. Zusätzlich zu bekannten Protokollen und Technologien wird eine Einführung in Neuentwicklungen im Bereich von Multimedia Kommunikation (u.a. Video Streaming, P2P, IP-Telefonie, Cloud Computing und Service-orientierte Architekturen) gegeben. Die Vorlesung ist als Anschlussvorlesung zu Kommunikationsnetze I geeignet.
4	**Voraussetzung für die Teilnahme** Empfohlen: Grundlegende Kurse der ersten 4 Semester werden benötigt. Die Vorlesung Kommunikationsnetze I wird empfohlen. Das Theoriewissen aus der Vorlesung Kommunikationsnetze II wird in praktischen Programmierübungen vertieft. Gundlegende Programmierkenntnisse sind daher hilfreich.
5	**Prüfungsform** Fachprüfung
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** MSc ETiT, MSc iST, Wi-ETiT, CS, Wi-CS
9	**Literatur** Ausgewählte Kapitel aus folgenden Büchern: - Andrew S. Tanenbaum: Computer Networks, 5th Edition, Prentice Hall, 2010 - James F. Kurose, Keith Ross: Computer Networking: A Top-Down Approach, 6th Edition, Addison-Wesley, 2009 - Larry Peterson, Bruce Davie: Computer Networks, 5th Edition, Elsevier Science, 2011
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Kommunikationsnetze IV</td></tr>
<tr><td>Modul Nr.
18-sm-2030</td><td>Kreditpunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>18-sm2030-vl</td><td>Kommunikationsnetze IV</td><td>3</td><td>Vorlesung</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Kommunikationsnetze IV behandelt die Modellierung und Leistungsbewertung von Computernetzwerken und Kommunikationssystemen. Der Schwerpunkt liegt auf aktuellen Analysemethoden mit denen ein grundlegendes Verständnis der Leistungsfähigkeit sowie eine Basis zur Planung, Optimierung und Weiterentwicklung von Kommunikationsnetzen vermittelt wird. Bedeutung und Implikationen der einzelnen Theorien werden an Beispielen mit Schwerpunkt auf dem Internet erläutert. Neben den analytischen Methoden gibt die Vorlesung eine Einführung in die Simulation von Kommunikationsnetzen sowie in die Messung in realen oder prototypischen Systemen und Testumgebungen. Über die gängigen Verfahren und ihre Anwendungen hinaus werden in der Vorlesung ausgesuchte Aspekte aktueller Forschungsfragen vertieft.
Themen der Vorlesung sind:

- Einführung in die Leistungsbewertung und ihre Anwendungen
- Leaky-bucket-Verkehrsregulatoren, deterministische Verkehrsmodelle, deterministische und empirische Einhüllende
- Scheduling, Generalized Processor SharingNetzwerkkalkül, min-plus Systemtheorie, deterministische Leistungsschranken
- Poisson-Prozesse, Markov-Ketten , klassische Warteschlangentheorie, M|M|1 und M|G|1 Modelle
- Modellierung von Paketdatenverkehr, Selbstähnlichkeit
- Effektive Bandbreiten, Momente erzeugende Funktionen, statistisches Multiplexen
- Statistisches Netzwerkkalkül, effektive Einhüllende, effektive Leistungsschranken
- Simulation, Generierung von Zufallszahlen, Verteilungen, Konfidenzintervalle
- Instrumentierung, Messung, Bandbreitenabschätzung im Internet</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Die Studierenden erhalten einen Überblick über die Bedeutung, grundlegende Methoden und wichtige Anwendungen der Leistungsbewertung von Kommunikationsnetzen. Sie kennen die typischen Mechanismen und Schedulingverfahren in Dienste integrierenden Netzen und können deren Wirkungsweise mit dem Netzwerkkalkül in der min-plus</td></tr>
</table>

	Systemtheorie erklären. Neben den Grundlagen der Warteschlangentheorie erlangen die Studenten detailliertes Wissen über die Theorie der effektiven Bandbreiten und weisen somit ein theoretisch fundiertes Verständnis des statistischen Multiplexens auf. Über die Analyse hinaus erhalten die Studenten Einblick in die Simulation und in ausgewählte Methoden und Werkzeuge zur Messung in realen Netzwerken. Sie sind in der Lage die erarbeiteten Verfahren gegeneinander abzugrenzen, problemspezifisch geeignete Methoden auszuwählen, auf typische Fragestellungen anzuwenden und relevante Schlussfolgerungen zu ziehen.
4	**Voraussetzung für die Teilnahme** Empfohlen: Grundlegende Kurse der ersten 4 Semester werden benötigt. Die Vorlesungen in Kommunikationsnetze I und II werden empfohlen.
5	**Prüfungsform** Fachprüfung
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** Wi-CS, Wi-ETiT, BSc/MSc CS, MSc ETiT, MSc iST
9	**Literatur** Ausgewählte Kapitel aus folgenden Büchern: - J.-Y. Le Boudec, P. Thiran: "Network Calculus: A Theory of Deterministic Queuing Systems for the Internet", Springer LNCS 2050, [url]http://ica1www.epfl.ch/PS_files/netCalBookv4.pdf[/url], 2004. - A. Kumar, D. Manjunath, J. Kuri: "Communication Networking: An Analytical Approach", Morgan Kaufmann, 2004. - A. M. Law, W. D. Kelton: "Simulation, Modeling and Analysis", McGraw Hill, 3rd Ed., 2000. - Selected Journal Articles and Conference Papers
10	**Kommentar**

Modulbeschreibung

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

Software Defined Networking</td></tr>
<tr><td>Modul Nr.
18-sm-2280</td><td>Kreditpunkte
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
Prof. Dr.-Ing. Ralf Steinmetz</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>18-sm-2280-ue</td><td>Software Defined Networking</td><td>0</td><td>Übung</td><td>2</td></tr>
<tr><td>18-sm-2280-vl</td><td>Software Defined Networking</td><td>0</td><td>Vorlesung</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Der Kurs behandelt Themen aus dem Bereich Software Defined Networking:
SDN Data Plane
SDN Control Plane
SDN Application Plane
Network Function Virtualization
Network Virtualization and Slicing
QoS and QoE in Software Defined Networks</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende erhalten einen vertieften Einblick in Software Defined Networking, sowie grundlegende Technologien und Anwendungen.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Grundlegende Kurse der ersten 4 Semester werden benötigt. Die Vorlesungen in Kommunikationsnetze I und II werden empfohlen.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Modulabschlussprüfung:
Modulprüfung (Fachprüfung, fakultativ, Standard)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten</td></tr>
</table>

7	**Benotung** Modulabschlussprüfung: • Modulprüfung (Fachprüfung, fakultativ, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** MSc ETiT, BSc/MSc iST, MSc Wi-ETiT, CS, Wi-CS
9	**Literatur** Lehrbücher gemäß Ankündigung. Folienskript der Vorlesung und Artikelkopien nach Bedarf.
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Echtzeitsysteme</td></tr>
<tr><td>Modul Nr.
18-su-2020</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>18-su-2020-vl</td><td>Echtzeitsysteme</td><td></td><td>Vorlesung</td><td>3</td></tr>
<tr><td>18-su-2020-ue</td><td>Echtzeitsysteme</td><td></td><td>Übung</td><td>1</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Vorlesung Echtzeitsysteme befasst sich mit einem Softwareentwicklungsprozess, der speziell auf die Spezifika von Echtzeitsystemen zugeschnitten ist. Dieser Softwareentwicklungsprozess wird im weiteren Verlauf während der Übungen in Ausschnitten durchlebt und vertieft. Der Schwerpunkt liegt dabei auf dem Einsatz objektorientierter Techniken. In diesem Zusammenhang wird das echtzeitspezifische CASE Tool Rhapsody vorgestellt und eingesetzt. Des weiteren werden grundlegende Charakteristika von Echtzeitsystemen und Systemarchitekturen eingeführt. Auf Basis der Einführung von Schedulingalgorithmen werden Einblicke in Echtzeitbetriebssysteme gewährt. Die Veranstaltung wird durch eine Gegenüberstellung der Programmiersprache Java und deren Erweiterung für Echtzeitsysteme (RT-Java) abgerundet.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studenten, die erfolgreich an dieser Veranstaltung teilgenommen haben, sollen in der Lage sein, modellbasierte (objektorientierte) Techniken zur Entwicklung eingebetteter Echtzeitsysteme zu verwenden und zu bewerten. Dazu gehören folgende Fähigkeiten:
• Systemarchitekturen zu bewerten und Echtzeitsysteme zu klassifizieren
• selbständig ausführbare Modelle zu erstellen und zu analysieren
• Prozesseinplanungen anhand üblicher Schedulingalgorithmen durchzuführen
• Echtzeitprogrammiersprachen und -Betriebssysteme zu unterscheiden, zu bewerten und einzusetzen.</td></tr>
</table>

4	**Voraussetzung für die Teilnahme** Empfohlen: Grundkennntisse des Software-Engineerings sowie Kenntnisse einer objektorientierten Programmiersprache
5	**Prüfungsform** Fachprüfung
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** MSc ETiT, BSc iST, MSc Wi-ETiT, Informatik
9	**Literatur** www.es.tu-darmstadt.de/lehre/es/
10	**Kommentar**

Modulbeschreibung

Modulname Konzepte der Programmiersprachen					
Modul Nr. 20-00-1117	**Kreditpunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen Software-Systeme und formale Grundlagen		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1117-iv	Konzepte der Programmiersprachen	0	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

Der Student wird am Ende des Kurses in der Lage sein, die zugrundeliegenden Mechanismen der wichtigsten Konzepte hinter Programmiersprachen zu verstehen. Der Student wird 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)

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%).

7 Benotung

Bausteinbegleitende Prüfung:

- [20-00-1117-iv] (Fachprüfung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)

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

Modulhandbuch
M. Sc. IT-Sicherheit

Studienbegleitende Leistungen

Praktika, Projektpraktika und ähnliche Veranstaltungen

Modulbeschreibung

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

Hacker Contest</td></tr>
<tr><td>Modul Nr.
20-00-0114</td><td>Kreditpunkte
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-Sicherheit</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>20-00-0114-pr</td><td>Hacker Contest</td><td>0</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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</td></tr>
<tr><td>3</td><td colspan="6">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</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:
Grundkenntnisse in IT-Sicherheit, Administration von Netzen und Rechnern</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0114-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0114-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Implementierung von Programmiersprachen						
Modul Nr. 20-00-0306	**Kreditpunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0306-pr	Implementierung von Programmiersprachen	0	Praktikum	4

2 Lerninhalt

Es werden Konzepte der Implementierung von Programmiersprachen vermittelt. Ferner werden diese Konzepte angewendet, um Erweiterungen für Programmiersprachen zu implementieren.

3 Qualifikationsziele / Lernergebnisse

Die Fähigkeit, eine professionelle Aufgabe aus der Informatik selbstständig und erfolgreich nach den anerkannten Grundsätzen der Profession zu bearbeiten.

4 Voraussetzung für die Teilnahme

Es wird kein Vorwissen vorausgesetzt. Jedoch sind gute Programmiererfahrungen sowie Kenntnisse über Kompilerbau und virtuelle Maschinen von Vorteil.

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-0306-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%)

7 Benotung

Bausteinbegleitende Prüfung:

- [20-00-0306-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)

8 Verwendbarkeit des Moduls

B.Sc. Informatik
M.Sc. Informatik
M.Sc. Internet- und Web-basierte Systeme
M.Sc. Distributed Software Systems

	M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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>Kreditpunkte
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 Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>
</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</td></tr>
</table>

	Empfohlen: Erfolgreiche Teilnahme an einer Integrierten Veranstaltung des Fachgebiets SEEMOO
5	**Prüfungsform** Studienleistung schriftlich/mündlich (Präsentation, Dokumentation, technische Umsetzung oder vergleichbare Leistungen)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Internet- und Web-basierte Systeme M.Sc. Distributed Software Systems M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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>Kreditpunkte
9 CP</td><td>Arbeitsaufwand
270 h</td><td>Selbststudium
180 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>
</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 Projektplanung und -verwaltung sowie die erstellten Softwareartefakte verständlich zu</td></tr>
</table>

	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** Studienleistung schriftlich/mündlich (Präsentation, Dokumentation, technische Umsetzung oder vergleichbare Leistungen)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Internet- und Web-basierte Systeme M.Sc. Distributed Software Systems M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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>Kreditpunkte
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 Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>
</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 Studenten 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 Studenten 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
Studienleistung schriftlich/mündlich (Präsentation, Dokumentation, technische Umsetzung oder vergleichbare Leistungen)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
B.Sc. Informatik
M.Sc. Informatik
M.Sc. IT Sicherheit</td></tr>
</table>

	M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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="7">Modulname
Praktikum Smartphone Security</td></tr>
<tr><td>Modul Nr.
20-00-0615</td><td>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0615-pr</td><td>Praktikum Smartphone Security</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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="6">Qualifikationsziele / Lernergebnisse
Durch die erfolgreiche Teilnahme an dieser Veranstaltung erlangen Studenten Kenntnissen und praktischer Erfahrungen mit Sicherheitsmechanismen in moderne Smartphone Betriebssystemen. Außerdem erwerben sie generelle Erfahrung in Systemprogrammierung.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:
● Grundlagen Betriebssysteme
● Programmierkenntnisse in C++ und Java</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Studienleistung schriftlich/mündlich (Präsentation, Dokumentation, technische Umsetzung oder vergleichbare Leistungen)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
</table>

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Wird in der Veranstaltung bekannt gegeben
10	**Kommentar**

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Praktikum: Zuverlässige Softwaresicherheit für mobile Endgeräte</td></tr>
<tr><td>Modul Nr.
20-00-0640</td><td>Kreditpunkte
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 Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0640-pr</td><td>Praktikum: Zuverlässige Softwaresicherheit für mobile Endgeräte</td><td>6</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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="6">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="6">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="6">Prüfungsform
Studienleistung schriftlich/mündlich (Präsentation, Dokumentation, technische Umsetzung oder vergleichbare Leistungen)</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Distributed Software Systems M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** ausgewählte Konferenz- und Zeitschriftenartikel
10	**Kommentar**

Modulbeschreibung

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

Softwaresecurity durch Laufzeitüberwachung</td></tr>
<tr><td>Modul Nr.
20-00-0719</td><td>Kreditpunkte
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-Sicherheit</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>20-00-0719-pr</td><td>Softwaresecurity durch Laufzeitüberwachung</td><td>0</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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.</td></tr>
<tr><td>3</td><td colspan="6">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</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Programmiererfahrung in Java; Informatikkenntnisse entsprechend dem 4. Semester des Bachelorstudiengangs</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-0719-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0719-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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>Kreditpunkte
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 Wintersemester</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>
</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
Studienleistung schriftlich/mündlich (Präsentation, Dokumentation, technische Umsetzung oder vergleichbare Leistungen)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Standard</td></tr>
</table>

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. Distributed Software Systems B.Sc. Computational Engineering M.Sc. Computational Engineering M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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

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

Dynamische Kontrolle von Systemanforderungen</td></tr>
<tr><td>Modul Nr.
20-00-0797</td><td>Kreditpunkte
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-Sicherheit</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>20-00-0797-pp</td><td>Dynamische Kontrolle von Systemanforderungen</td><td>0</td><td>Praktikum</td><td>6</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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</td></tr>
<tr><td>3</td><td colspan="6">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.</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 Programmierkenntnisse in Java und die Fähigkeit, mit formalen Sprachen umzugehen</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:</td></tr>
</table>

	• [20-00-0797-pp] (Studienleistung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%) Module Exclusions: 20-00-0719 - Dynamic Enforcement of Software Security
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0797-pp] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT M.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

Zuverlässige Softwaresicherheit für mobile Endgeräte</td></tr>
<tr><td>Modul Nr.
20-00-0799</td><td>Kreditpunkte
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-Sicherheit</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>20-00-0799-pr</td><td>Zuverlässige Softwaresicherheit für mobile Endgeräte</td><td>0</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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="6">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="6">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="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-0799-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%) Module Exclusions: 20-00-0640 - Software Security for Mobile Devices
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0799-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT M.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

Distributed Systems Programming: Praktikum</td></tr>
<tr><td>Modul Nr.
20-00-0985</td><td>Kreditpunkte
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-Sicherheit</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>20-00-0985-pr</td><td>Distributed Systems Programming: Praktikum</td><td>0</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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 dem Betreuer 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-Praktikum" können Studierende technische und wissenschaftliche Probleme im Bereich DS lösen.

Je nach ausgewähltem Thema erlernen Studierende folgende Kompetenzen:</td></tr>
</table>

	Entwurf komplexer DS Methodische Analyse und Auswertung von: • 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 in der ersten Vorlesung präsentiert.
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-0985-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0985-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Cybersecurity Lab						
Modul Nr. 20-00-1018	**Kreditpunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			
1	**Kurse des Moduls**					
	Kurs Nr.	**Kursname**	**Arbeitsaufwand (CP)**	**Lehrform**	**SWS**	
	20-00-1018-pr	Cybersecurity Lab	0	Praktikum	4	
2	**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.					
3	**Qualifikationsziele / Lernergebnisse** Am Ende des Kurses werden die Studierenden gute Kenntnisse in Netzwerksicherheit, und speziell auf den Gebieten der durch sie bearbeitenden Projekte, erlangen. Die Note berechnet sich auf Grundlage der eingereichten Projekte.					
4	**Voraussetzung für die Teilnahme** Empfohlen: Die Studierenden sollten einen Background in Netzwerk- und Operating Systems haben – diese sind vorausgesetzte Kurse.					
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1018-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)					
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)					
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1018-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)					

8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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>Kreditpunkte
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-Sicherheit</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>0</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)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:</td></tr>
</table>

	• [20-00-1020-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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	**Kreditpunkte** 9 CP	**Arbeitsaufwand** 270 h	**Selbststudium** 180 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1027-pp	Projektpraktikum Friedens- und Kriseninformatik	0	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)

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%)

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1027-pp] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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

Praktikum zur Vorlesung Cryptocurrencies</td></tr>
<tr><td>Modul Nr.
20-00-1031</td><td>Kreditpunkte
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-Sicherheit</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>20-00-1031-pr</td><td>Praktikum zur Vorlesung Cryptocurrencies</td><td>0</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Diese Veranstaltung richtet sich an Studierende, die die Vorlesung Cryptocurrencies besucht 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.
Komplexe kryptografische Systeme und Bausteine aus der Vorlesung Cryptocurrencies sollen dabei in Teamarbeit verstanden und in einem dezentralen System implementiert werden. Dabei wird die eigenständige Konzeption eines Projektes gefordert, was im Verlauf der Veranstaltung von den Studierenden geplant und umgesetzt werden soll.
Die Studierenden erhalten dabei erste Erfahrungen mit der Umsetzung eines komplexeren Entwicklungsprojektes.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Studierende verstehen nach erfolgreichem Besuch der Veranstaltung die technischen und praktischen Implikaitonen 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 Benutzung kryptographischer Bausteine
• Sicherheit und Anonymität von Nutzern von kryptographischen Währungen
• Mögliche Angriffe auf Smart Contracts und Cryptocurrencies</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Dieser Kurs richtet sich an Studenten, die die Vorlesung Cryptocurrencies mit guten Noten abgeschlossen haben. Weiterhin sollten Programmierkenntnisse und ein Interesse an den Themen der Vorlesung vorhanden sein.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-1031-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1031-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname

Projektpraktikum Softwareentwicklung zum Schutz der Privatsphäre

Modul Nr.	Kreditpunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-1053	9 CP	270 h	180 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Englisch	Koordinatoren/Koordinatorinnen IT-Sicherheit

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1053-pp	Projektpraktikum Softwareentwicklung zum Schutz der Privatsphäre	0	Projekt	6

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 ist erforderlich, 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: • [20-00-1053-pp] (Studienleistung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1053-pp] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

Praktikum Softwareentwicklung zum Schutz der Privatsphäre</td></tr>
<tr><td colspan="2">Modul Nr.
20-00-1054</td><td>Kreditpunkte
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="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-1054-pr</td><td>Praktikum Softwareentwicklung zum Schutz der Privatsphäre</td><td>0</td><td>Praktikum</td><td>4</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 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.</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 Enwicklung 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 ist erforderlich, 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.</td></tr>
</table>

5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1054-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1054-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Security Engineering Lab						
Modul Nr. 20-00-1056	**Kreditpunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1056-pr	Security Engineering Lab	0	Praktikum	4

2 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

3 Qualifikationsziele / Lernergebnisse

Ziel dieses Praktikums ist die Ausweitung von Programmierkentnissen sowie die Partizipation in Forschungsprojekten. Zusätzlich werden die Teilnehmer Wissen in den genannten Bereichen erlangen und erfahren den jeweils aktuellen Forschungsstand.

4 Voraussetzung für die Teilnahme

5 Prüfungsform

Bausteinbegleitende Prüfung:

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

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%)

7 Benotung

Bausteinbegleitende Prüfung:

- [20-00-1056-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)

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

Modulbeschreibung

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

IoT- und Funkprotokolle in eingebetteten Systemen</td></tr>
<tr><td>Modul Nr.
20-00-1064</td><td>Kreditpunkte
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-Sicherheit</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>20-00-1064-pr</td><td>IoT- und Funkprotokolle in eingebetteten Systemen</td><td>0</td><td>Praktikum</td><td>4</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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="6">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="6">Voraussetzung für die Teilnahme
Empfohlen sind Vorkenntnisse in Computernetzwerken (Pflichtvorlesung "Computer-Netzwerke und Verteilte Systeme) und in Eingebetteten Systemen (Pflichtvorlesungen Rechnerorganisation und/oder Datentechnik). Kenntnis der Programmiersprache C und Grundkenntnisse. der Elektrotechnik sind hilfreich, ebenso Kenntnisse aus einschlägigen Vorlesungen des Bereichs "Netze und Verteilte Systeme" wie TK3, Mobile Netze oder KN1.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1064-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

Bestehen der Prüfung (100%)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1064-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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>Kreditpunkte
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-Sicherheit</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>0</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.

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 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>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1072-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B. Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname
Projektpraktikum Interaktive resiliente Informationstechnik

Modul Nr.	Kreditpunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-1073	9 CP	270 h	180 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Deutsch	Koordinatoren/Koordinatorinnen IT-Sicherheit

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1073-pp	Projektpraktikum Interaktive resiliente Informationstechnik	0	Projekt	6

2 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.

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 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

4 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

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1073-pp] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

6 Voraussetzung für die Vergabe von Kreditpunkten

	Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1073-pp] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Bug Hunting Praktikum					
Modul Nr. 20-00-1083	**Kreditpunkte** 6 CP	**Arbeitsaufwand** 180 h	**Selbststudium** 120 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1083-pr	Bug Hunting Praktikum	0	Praktikum	4

2 Lerninhalt

In diesem Praktikum beschäftigen sich die Studenten mit dem automatischen oder manuellen Aufdecken von Schwachstellen und Verwundbarkeiten in realen Open Source Softwareprojekten. Die Studenten 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 Studenten 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

Weitere Informationen zum Ablauf:
https://team-sik.org/bug-hunting-praktikum/

3 Qualifikationsziele / Lernergebnisse

Ein theoretischer Teil vermittelt den Studenten Methoden zur Schwachstellenidentifikation und Bedrohungsmodellierung von Softwareprojekten. In einem praktischen Teil sammeln die Studenten selbstständig Erfahrungen im Identifizieren von Schwachstellen. Die Studenten sind nach erfolgreichem Absolvieren des Praktikums in der Lage, selbstständig und strukturiert Sicherheitslücken in Softwareprojekten zu finden und zu dokumentieren. Die Studenten können nach dem Praktikum die Schwere und die Folgen von Sicherheitslücken einschätzen, sowie Gegenmaßnahmen benennen.

4 Voraussetzung für die Teilnahme

Empfohlen:

- Gute Teamfähigkeit
- Interesse an Schwachstellenidentifikation, Programmanalyse und Exploitation
- Gute Programmierkenntnisse

	- Linux Kenntnisse - Vollständige und korrekte Abgabe der Anmeldeaufgabe
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1083-pr] (Studienleistung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1083-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname
Praktikum Seitenkanalanalyse

Modul Nr.	Kreditpunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-1090	6 CP	180 h	120 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Englisch	Koordinatoren/Koordinatorinnen IT-Sicherheit

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1090-pr	Praktikum Seitenkanalanalyse	0	Praktikum	4

2 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

3 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.

4 Voraussetzung für die Teilnahme

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)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1090-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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>Kreditpunkte
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-Sicherheit</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>0</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)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%).</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:
• [20-00-1104-pr] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)</td></tr>
</table>

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

Modulbeschreibung

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

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1119-pp	Blockchain Projektpraktikum	0	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** 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)
6	**Voraussetzung für die Vergabe von Kreditpunkten** 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 Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulhandbuch
M. Sc. IT-Sicherheit

Studienbegleitende Leistungen

Seminare

Modulbeschreibung

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

Design und Implementierung moderner Programmiersprachen</td></tr>
<tr><td>Modul Nr.
20-00-0182</td><td>Kreditpunkte
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</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0182-se</td><td>Design und Implementierung moderner Programmiersprachen</td><td>0</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse
Fähigkeit zur selbständigen Erarbeitung wissenschaftlicher Fragestellungen im Bereich „Design und Implementierung moderner Programmiersprachen“

Erwerb von Kenntnissen über ausgewählte aktuelle Themen

Aneignung von Präsentationstechniken</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen:

Vordiplom oder gleichwertige Qualifikation (d.h. fachlicher Kenntnisstand nach den ersten vier Semestern des Bachelor-Studiengangs Informatik). Das Seminar kann auch zur Einarbeitung z.B. für Studien-, Semester-, Bachelor-, Master- oder Diplomarbeiten dienen.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-0182-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:

• [20-00-0182-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls</td></tr>
</table>

	B. Sc. Informatik M. Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

Sicherheitskonzepte im Eisenbahnbetrieb</td></tr>
<tr><td>Modul Nr.
20-00-0461</td><td>Kreditpunkte
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</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-0461-se</td><td>Sicherheitskonzepte im Eisenbahnbetrieb</td><td>0</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Grundwissen über Eisenbahnsicherungsanlagen und sicheren Eisenbahnbetrieb. Umsetzung von Sicherheitskonzepten in modernen Eisenbahnsicherungsanlagen.</td></tr>
<tr><td>3</td><td colspan="6">Qualifikationsziele / Lernergebnisse</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Grundkenntnisse über zuverlässige Systeme (z.B. Besuch der VL Computersystemsicherheit) und Interesse am Eisenbahnbetrieb.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-0461-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:
• [20-00-0461-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
B.Sc. Informatik
M.Sc. Informatik
Kann in anderen Studiengängen verwendet werden.</td></tr>
<tr><td>9</td><td colspan="6">Literatur</td></tr>
<tr><td>10</td><td colspan="6">Kommentar</td></tr>
</table>

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>Kreditpunkte
4 CP</td><td>Arbeitsaufwand
120 h</td><td>Selbststudium
75 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>
</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 bearbeiteten Themenfeld erworben. Arbeitstechniken wie ausführliche Literaturrecherche, kritische Diskussion und Analyse wissenschaftlicher Artikel und die Presentation der</td></tr>
</table>

	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** Studienleistung schriftlich/mündlich (Präsentation, Dokumentation, technische Umsetzung oder vergleichbare Leistungen)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Internet- und Web-basierte Systeme M.Sc. Distributed Software Systems M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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>Kreditpunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Semester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>
</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 Wissen einem heterogenen Publikum verständlich präsentieren und die technischen Details des bearbeiteten Themas erläutern.</td></tr>
</table>

4	**Voraussetzung für die Teilnahme** Empfohlen: Erfolgreiche Teilnahme an einer Integrierten Veranstaltung des Fachgebiets SEEMOO
5	**Prüfungsform** Studienleistung schriftlich/mündlich (Präsentation, Dokumentation, technische Umsetzung oder vergleichbare Leistungen)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Distributed Software Systems M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur** Themenspezifisch ausgewählte, aktuelle wissenschaftliche Veröffentlichungen
10	**Kommentar**

Modulbeschreibung

Modulname Seminar - Softwaresicherheit für mobile Endgeräte						
Modul Nr. 20-00-0641	**Kreditpunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0641-se	Seminar - Softwaresicherheit für mobile Endgeräte	0	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)

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%)

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0641-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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>Kreditpunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
i.d.R. jedes Sommersemester</td></tr>
<tr><td colspan="3">Sprache
Deutsch und Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>
</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 Studenten 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
Empfohlen: Grundlagen der Informatik</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Studienleistung schriftlich/mündlich (Präsentation, Dokumentation, technische Umsetzung oder vergleichbare Leistungen)</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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>Kreditpunkte
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-Sicherheit</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>0</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>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%) Kann nicht gemeinsam mit 20-00-0584-se eingebracht werden.
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0712-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann im Rahmen fachübergreifender Angebote auch 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>Kreditpunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
unregelmäßig</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>
</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
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</td></tr>
</table>

	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** Studienleistung schriftlich/mündlich (Präsentation, Dokumentation, technische Umsetzung oder vergleichbare Leistungen)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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>Kreditpunkte
3 CP</td><td>Arbeitsaufwand
90 h</td><td>Selbststudium
60 h</td><td>Moduldauer
1 Semester</td><td colspan="2">Angebotsturnus
unregelmäßig</td></tr>
<tr><td colspan="3">Sprache
Englisch</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>
</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>
<tr><td>5</td><td colspan="6">Prüfungsform
Studienleistung schriftlich/mündlich (Präsentation, Dokumentation, technische Umsetzung oder vergleichbare Leistungen)</td></tr>
</table>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Modulabschlussprüfung (100%)
7	**Benotung** Standard
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. IT Sicherheit M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch 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	**Kreditpunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0798-se	Seitenkanalangriffe gegen Software	0	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)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0798-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT M.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0807-se	Privatheit & Anonymität in einer vernetzten Welt	0	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)

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%)

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0807-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik M.Sc. Wirtschaftsinformatik B.Sc. Psychologie in IT M.Sc. Psychologie in IT Joint B.A. Informatik B.Sc. Sportwissenschaft und Informatik M.Sc. Sportwissenschaft und Informatik Kann im Rahmen fachübergreifender Angebote auch in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0925-se	Grundlagen der Computersicherheit	0	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)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0925-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0935-se	Privatsphäre-schützende Technologien	0	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)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0935-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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>Kreditpunkte
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-Sicherheit</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>0</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>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0960-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

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)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0961-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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>Kreditpunkte
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-Sicherheit</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>0</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>

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1009-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

Seminar Krisen-, Sicherheits- und Friedenstechnologien</td></tr>
<tr><td>Modul Nr.
20-00-1019</td><td>Kreditpunkte
4 CP</td><td>Arbeitsaufwand
120 h</td><td>Selbststudium
90 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-Sicherheit</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>20-00-1019-se</td><td>Seminar Krisen-, Sicherheits- und Friedenstechnologien</td><td>0</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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</td></tr>
<tr><td>3</td><td colspan="6">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</td></tr>
</table>

	- 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)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1019-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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

Modulname Schutz von verteilten Infrastrukturen und Netzwerken						
Modul Nr. 20-00-1022	**Kreditpunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch und Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			
1	**Kurse des Moduls**					
	Kurs Nr.	**Kursname**	**Arbeitsaufwand (CP)**	**Lehrform**	**SWS**	
	20-00-1022-se	Schutz von verteilten Infrastrukturen und Netzwerken	0	Seminar	2	
2	**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.					
3	**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.					
4	**Voraussetzung für die Teilnahme** Empfohlen: Grundlegendes Verständnis von IT-Sicherheit und verteilten Systemen. Veranstaltungen: Computersystemsicherheit (CSS) Computer-Netzwerke und verteilte Systeme (CNuvS)					
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1022-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)					

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1022-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1024-se	Seminar Cyber-Sicherheit, -Krieg, und -Frieden	0	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)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1024-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Grundlagen statischer Analysen					
Modul Nr. 20-00-1028	**Kreditpunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1028-se	Grundlagen statischer Analysen	0	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)

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%)

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1028-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik 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>Kreditpunkte
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-Sicherheit</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>0</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>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
</table>

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1030-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1052-se	Zero Knowledge Beweissysteme	0	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)

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%)

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1052-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1063-se	Binary Analysis Seminar	0	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 Studenten ein Grundverständnis der Analyse von nativem Code. Zusätzlich wird durch den Vergleich der Werkzeuge die Fähigkeit des wissenschaftlichen Arbeitens gefördert. Außerdem sammeln die Studenten praktische Erfahrungen im Umgang mit gängigen Analysewerkzeugen. Die Studenten 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) Bestehen der Prüfung (100%)
6	**Voraussetzung für die Vergabe von Kreditpunkten**
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1063-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Aktor-basierte Programmiersprachen						
Modul Nr. 20-00-1074	**Kreditpunkte** 3 CP	**Arbeitsaufwand** 90 h	**Selbststudium** 60 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			
1	**Kurse des Moduls**					
	Kurs Nr.	**Kursname**	**Arbeitsaufwand (CP)**	**Lehrform**	**SWS**	
	20-00-1074-se	Aktor-basierte Programmiersprachen	0	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** Interesse in Programmiersprachen und verteilten Systemen					
5	**Prüfungsform** Bausteinbegleitende Prüfung: • [20-00-1074-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)					
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)					
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1074-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)					
8	**Verwendbarkeit des Moduls**					

	B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname
Aktuelle Themen zu Modular Verification

Modul Nr.	Kreditpunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-1077	3 CP	90 h	60 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Englisch	Koordinatoren/Koordinatorinnen IT-Sicherheit

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1077-se	Aktuelle Themen zu Modular Verification	0	Seminar	2

2 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.

3 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.

4 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.

5 Prüfungsform

Bausteinbegleitende Prüfung:

	• [20-00-1077-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1077-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname
Fortgeschrittene Techniken der Softwareverifikation

Modul Nr.	Kreditpunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-1078	3 CP	90 h	60 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Englisch	Koordinatoren/Koordinatorinnen IT-Sicherheit

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1078-se	Fortgeschrittene Techniken der Softwareverifikation	0	Seminar	2

2 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. Die Themen des aktuellen Semesters entnehmen Sie bitte der Webseite der Lehrveranstaltung (https://www.informatik.tu-darmstadt.de/svpsys/semantik_und_verifikation_paralleler_systeme_svpsys/lehre_svpsys/seminar_ftsv_svpsys/index.de.jsp).

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.

3 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.

4 Voraussetzung für die Teilnahme

	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)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1078-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1088-se	Seitenkanalresistente Kryptographie	0	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

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)
6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1088-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname
Angreifermodelle in der IT-Sicherheit

Modul Nr.	Kreditpunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-1091	3 CP	90 h	60 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Englisch	Koordinatoren/Koordinatorinnen IT-Sicherheit

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1091-se	Angreifermodelle in der IT-Sicherheit	0	Seminar	2

2 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.

3 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.

4 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.

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1091-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

6	**Voraussetzung für die Vergabe von Kreditpunkten** Bestehen der Prüfung (100%)
7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-1091-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname CORONA-CON					
Modul Nr. 20-00-1099	**Kreditpunkte** 4 CP	**Arbeitsaufwand** 120 h	**Selbststudium** 90 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester
Sprache Englisch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit		

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-1099-se	CORONA-CON	0	Seminar	2

2 Lerninhalt

Das Thema dieses Seminars ist es, einen allgemeinen Überblick über mögliche Einsatzmöglichkeiten digitaler Technologien bei der Bewältigung von Ausnahmesituationen, wie der aktuellen COVID 19-Pandemie zu geben und konkrete Handlungsvorschläge zu entwickeln.

3 Qualifikationsziele / Lernergebnisse

Die Studenten werden sich am Beispiel der Risikoeinschätzung und Kontrollstrategien die folgenden Fertigkeiten aneignen:
- Einarbeitung in komplexe Fragestellungen
- Durchführung von Literaturrecherchen
- Teamarbeit
- Erarbeitung eigener Lösungen

4 Voraussetzung für die Teilnahme

Empfohlene Vorkenntnisse: Konzepte der Computersicherheit und des Datenschutzes

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-1099-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%).

7 Benotung

Bausteinbegleitende Prüfung:

- [20-00-1099-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)

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

Modulbeschreibung

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

Seminar Informatik, Ethik und Gesellschaft</td></tr>
<tr><td>Modul Nr.
20-00-1102</td><td>Kreditpunkte
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</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-1102-se</td><td>Seminar Informatik, Ethik und Gesellschaft</td><td>0</td><td>Seminar</td><td>3</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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</td></tr>
<tr><td>3</td><td colspan="6">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</td></tr>
</table>

	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)
6	**Voraussetzung für die Vergabe von Kreditpunkten** 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 Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

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

Seminar Kryptographie</td></tr>
<tr><td>Modul Nr.
20-00-1103</td><td>Kreditpunkte
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-Sicherheit</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>20-00-1103-se</td><td>Seminar Kryptographie</td><td>0</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Im Seminar werden aktuelle Forschungsresultate aus dem Gebiet der Kryptographie von den Studierenden vorgestellt.</td></tr>
<tr><td>3</td><td colspan="6">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.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen werden: Einführung in die Kryptographie,
andere weiterführende Veranstaltungen im Bereich Kryptographie</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1103-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%).</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:
• [20-00-1103-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)</td></tr>
</table>

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

Modulbeschreibung

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

Verfassen und Beurteilen Wissenschaftlicher Veröffentlichungen in der IT-Sicherheit</td></tr>
<tr><td>Modul Nr.
20-00-1105</td><td>Kreditpunkte
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-Sicherheit</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>20-00-1105-se</td><td>Verfassen und Beurteilen Wissenschaftlicher Veröffentlichungen in der IT-Sicherheit</td><td>0</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Die Studierenden verfassen eine kurze wissenschaftliche Arbeit im Bereich IT-Sicherheit und beurteilen die Arbeiten der anderen in einer konferenz-ähnlichen Umgebung.</td></tr>
<tr><td>3</td><td colspan="6">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.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Empfohlen: Kenntnisse in IT-Sicherheit, erste Erfahrungen im Verfassen von wissenschaftlichen Arbeiten, z.B. Bachelor-Arbeit</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
[20-00-1105-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%).</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:
[20-00-1105-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)</td></tr>
</table>

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

Modulbeschreibung

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

Sicherheit und Privatheit in vernetzten Systemen</td></tr>
<tr><td>Modul Nr.
20-00-1106</td><td>Kreditpunkte
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</td><td colspan="4">Modulverantwortliche Person
Koordinatoren/Koordinatorinnen IT-Sicherheit</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>20-00-1106-se</td><td>Sicherheit und Privatheit in vernetzten Systemen</td><td>0</td><td>Seminar</td><td>2</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">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</td></tr>
<tr><td>3</td><td colspan="6">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.</td></tr>
<tr><td>4</td><td colspan="6">Voraussetzung für die Teilnahme
Vorwissen im Bereich IT-Sicherheit, beispielsweise durch Besuch entsprechender Lehrveranstaltungen, wird empfohlen.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:

• [20-00-1106-se] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%).</td></tr>
<tr><td>7</td><td colspan="6">Benotung</td></tr>
</table>

	Bausteinbegleitende Prüfung: • [20-00-1106-se] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%, Standard)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulhandbuch
M. Sc. IT-Sicherheit

Studienbegleitende Leistungen

Praktikum in der Lehre

Modulbeschreibung

Modulname

Praktikum in der Lehre - Internetsicherheit und Sicherheit in Mobilen Netzen

Modul Nr.	Kreditpunkte	Arbeitsaufwand	Selbststudium	Moduldauer	Angebotsturnus
20-00-0957	5 CP	150 h	105 h	1 Semester	Jedes 2. Semester

Sprache	Modulverantwortliche Person
Deutsch und Englisch	Koordinatoren/Koordinatorinnen IT-Sicherheit

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0957-pl	Praktikum in der Lehre - Internetsicherheit und Sicherheit in Mobilen Netzen	0	Praktikum in der Lehre	3

2 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.

3 Qualifikationsziele / Lernergebnisse

Die Studenten können nach erfolgreicher Durchführung der Veranstaltung:
- Lehrinhalte aus der Vorlesung für Haus- und Präsenzübungen aufbereiten
- Praxisnahe Übungsformen konzipieren und erstellen
- Übungen mit Studentengruppen aller Leistungsniveaus konzipieren und durchführen
- Ein Konzept für aufeinander aufbauende praktische Übungen entwickeln
- Methoden der Lernkontrolle für die Lerninhalte der Vorlesung anwenden

4 Voraussetzung für die Teilnahme

Empfohlen:

Erfolgreicher Besuch der SEEMOO Veranstaltung für die das PIDL durchgeführt wird.

5 Prüfungsform

Bausteinbegleitende Prüfung:

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

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%)

7	**Benotung** Bausteinbegleitende Prüfung: • [20-00-0957-pl] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)
8	**Verwendbarkeit des Moduls** B.Sc. Informatik M.Sc. Informatik Kann in anderen Studiengängen verwendet werden.
9	**Literatur**
10	**Kommentar**

Modulbeschreibung

Modulname Praktikum in der Lehre - Computersystemsicherheit						
Modul Nr. 20-00-0986	**Kreditpunkte** 5 CP	**Arbeitsaufwand** 150 h	**Selbststudium** 105 h	**Moduldauer** 1 Semester	**Angebotsturnus** Jedes 2. Semester	
Sprache Deutsch			**Modulverantwortliche Person** Koordinatoren/Koordinatorinnen IT-Sicherheit			

1 Kurse des Moduls

Kurs Nr.	Kursname	Arbeitsaufwand (CP)	Lehrform	SWS
20-00-0986-pl	Praktikum in der Lehre - Computersystemsicherheit	0	Praktikum in der Lehre	3

2 Lerninhalt

- Ausarbeitung neuer Übungs- und Programmieraufgaben
- Konzeption von Übungsblättern

3 Qualifikationsziele / Lernergebnisse

Nachdem Studierende die Veranstaltung besucht haben, können sie Lerninhalte als Übungs- und Programmieraufgaben aufbereiten.

4 Voraussetzung für die Teilnahme

Empfohlen: erfolgreiche Teilnahme an der Lehrveranstaltung "Computersystemsicherheit"

5 Prüfungsform

Bausteinbegleitende Prüfung:

- [20-00-0986-pl] (Studienleistung, mündliche / schriftliche Prüfung, Standard)

6 Voraussetzung für die Vergabe von Kreditpunkten

Bestehen der Prüfung (100%)

7 Benotung

Bausteinbegleitende Prüfung:

- [20-00-0986-pl] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)

8 Verwendbarkeit des Moduls

B.Sc. Informatik
M.Sc. Informatik
Kann in anderen Studiengängen verwendet werden.

9 Literatur

10 Kommentar

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Praktikum in der Lehre - SIT</td></tr>
<tr><td>Modul Nr.
20-00-1045</td><td>Kreditpunkte
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-Sicherheit</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>20-00-1045-pl</td><td>Praktikum in der Lehre - SIT</td><td>0</td><td>Praktikum in der Lehre</td><td>3</td></tr>
</table></td></tr>
<tr><td>2</td><td colspan="6">Lerninhalt
Unterstützung der Lehre wie z.B., Betreuung von Übungsgruppen, Sprechstunden, o.ä.</td></tr>
<tr><td>3</td><td colspan="6">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.</td></tr>
<tr><td>4</td><td colspan="6">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.</td></tr>
<tr><td>5</td><td colspan="6">Prüfungsform
Bausteinbegleitende Prüfung:
• [20-00-1045-pl] (Studienleistung, mündliche / schriftliche Prüfung, Standard)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:
• [20-00-1045-pl] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
B.Sc. Informatik
M.Sc. Informatik
Kann in anderen Studiengängen verwendet werden.</td></tr>
<tr><td>9</td><td colspan="6">Literatur</td></tr>
<tr><td>10</td><td colspan="6">Kommentar</td></tr>
</table>

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>Kreditpunkte
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-Sicherheit</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>0</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
Studenten 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
• Studenten 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)</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Prüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Bausteinbegleitende Prüfung:
• [20-00-1059-pl] (Studienleistung, mündliche / schriftliche Prüfung, Gewichtung: 100%)</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
B.Sc. Informatik
M.Sc. Informatik
Kann in anderen Studiengängen verwendet werden.</td></tr>
<tr><td>9</td><td colspan="6">Literatur</td></tr>
<tr><td>10</td><td colspan="6">Kommentar</td></tr>
</table>

Modulhandbuch
M. Sc. IT-Sicherheit

Masterarbeit

Modulbeschreibung

<table>
<tr><td colspan="7">Modulname
Masterarbeit IT-Sicherheit</td></tr>
<tr><td>Modul Nr.
20-AM-5400</td><td>Kreditpunkte
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>
</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 nach wissenschaftlichen Grundsätzen selbstständig zu bearbeiten,
• die im Studium erworbenen Kenntnisse, Methoden und Kompetenzen zu verknüpfen und anzuwenden,
• 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
schriftliche Arbeit und ein mündliches Kolloquium</td></tr>
<tr><td>6</td><td colspan="6">Voraussetzung für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussprüfung (100%)</td></tr>
<tr><td>7</td><td colspan="6">Benotung
Die schriftliche Arbeit geht mit 85% und das Kolloquium mit 15% in die Note für die Masterarbeit ein.</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls
M. Sc. IT-Sicherheit</td></tr>
</table>

9	**Literatur** - Balzert, Helmut; Schäfer, Christian; Schröder, Marion: Wissenschaftliches Arbeiten - Wissenschaft, Quellen, Artefakte, Organisation, Präsentation. W3L-Verlag; Auflage: 2, 2011 - Sandberg, Berit: Wissenschaftlich Arbeiten von Abbildung bis Zitat: Lehr- und Übungsbuch für Bachelor, Master und Promotion. De Gruyter Oldenbourg; Auflage: 2, 2013
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 Wintersemester bzw. Anfang August bei Studienbeginn zum Sommersemester begonnen werden muss.