

Orientierungsveranstaltung IST

Theoretische Informatik und IT-Sicherheit



TECHNISCHE
UNIVERSITÄT
DARMSTADT



Profil

Beginn Bachelor: SoSe 2015
Abschluss Bachelor: August 2019 (iST und Inf)

Thema BA: Adaptive Covert-Channel Attacks

Beginn Master: Direkt im Anschluss
Abschluss Master: April 2022 (iST, Inf, IT-Sec)

Thema MA: Bisimulationsanalyse von variablen Softwaresystemen

Seit April 2022: Fachgebiet Echtzeitsysteme (Schürr)
Sonderforschungsbereich MAKI

Aktuelles Thema: **Timed (Bi-)Simulation für TA.**



Was habe ich über mich selbst gelernt?



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Was konnte ich besser als meine Kommilitonen?

Was konnte ich schlechter als meine Kommilitonen?

Was habe ich über mich selbst gelernt?

Was konnte ich besser als meine Kommilitonen?

- **Mathematik**
 - Induktionsbeweise
 - Widerspruchsbeweise
 - ...

- **Formale Methoden**
 - Krypto
 - Automatenmodelle
 - Algorithmik
 - ...

- **Systematisch Arbeiten**

Was konnte ich schlechter als meine Kommilitonen?

Was habe ich über mich selbst gelernt?

Was konnte ich besser als meine Kommilitonen?

- **Mathematik**
 - Induktionsbeweise
 - Widerspruchsbeweise
 - ...
- **Formale Methoden**
 - Krypto
 - Automatenmodelle
 - Algorithmik
 - ...
- **Systematisch Arbeiten**

Was konnte ich schlechter als meine Kommilitonen?

- **Hürden der Praxis**
 - Unsauber definierte Libraries nutzen
 - Fehlersuche in eingebetteten Systemen
 - ...
- **Schnell mal was Umsetzen**
 - Kosten-/Nutzenoptimal
 - Zielgerichtet
 - Zeitnah gute, aber nicht sehr gute, technische Lösungen entwickeln und umsetzen

Meine Themenschwerpunkte

Automaten, formale Sprachen und
Entscheidbarkeit
Aussagen- und Prädikatenlogik
Seminar Softwaresystemtechnologie

...

Theoretische Informatik

Meine Themenschwerpunkte

Automaten, formale Sprachen und
Entscheidbarkeit
Aussagen- und Prädikatenlogik
Seminar Softwaresystemtechnologie
...
Theoretische Informatik

Einführung in die Kryptographie
Seitenkanalresistente Kryptographie
Cryptocurrencies
Blockchain Praktikum
Symmetrische Kryptographie
...
Kryptographie

Meine Themenschwerpunkte

Automaten, formale Sprachen und
Entscheidbarkeit
Aussagen- und Prädikatenlogik
Seminar Softwaresystemtechnologie
...

Theoretische Informatik

Einführung in die Kryptographie
Seitenkanalresistente Kryptographie
Cryptocurrencies
Blockchain Praktikum
Symmetrische Kryptographie
...

Kryptographie

Identische Methodik!

Meine Themenschwerpunkte

Automaten, formale Sprachen und
Entscheidbarkeit
Aussagen- und Prädikatenlogik
Seminar Softwaresystemtechnologie
...

Theoretische Informatik

Einführung in die Kryptographie
Seitenkanalresistente Kryptographie
Cryptocurrencies
Blockchain Praktikum
Symmetrische Kryptographie
...

Kryptographie

Identische Methodik!

CnuVS
TK1
TK3

Computernetzwerke

Meine Themenschwerpunkte

Automaten, formale Sprachen und
Entscheidbarkeit
Aussagen- und Prädikatenlogik
Seminar Softwaresystemtechnologie
...
Theoretische Informatik

Einführung in die Kryptographie
Seitenkanalresistente Kryptographie
Cryptocurrencies
Blockchain Praktikum
Symmetrische Kryptographie
...
Kryptographie

Oftmals die
Anwendung

Identische Methodik!

CnuVS
TK1
TK3

Computernetzwerke

„Das eine nicht ohne das andere“

Meine Themenschwerpunkte

Automaten, formale Sprachen und
Entscheidbarkeit
Aussagen- und Prädikatenlogik
Seminar Softwaresystemtechnologie
...
Theoretische Informatik

Einführung in die Kryptographie
Seitenkanalresistente Kryptographie
Cryptocurrencies
Blockchain Praktikum
Symmetrische Kryptographie
...

Kryptographie

Identische Methodik!

Oftmals die
Anwendung

CnuVS
TK1
TK3

Computernetzwerke

„Das eine nicht ohne das andere“

Einführung in die Kryptographie (20-00-0085-iv)

- Themen: Definitionen PRG, Sicherheit, PRF, PRP, Blockchiffren, Public Key, ...
- Zum „Reinschnuppern“ in die Krypto.
 - Noch nicht zu formell,
 - viele Beispiele,
 - praktische Beispiele allgegenwärtig.
- Prof. Faust oder Prof. Fischlin.
- Hat mir sehr (!) viel Spaß gemacht und somit motiviert, mir die Krypto stärker anzuschauen.
- Die TU Darmstadt ist in diesem Gebiet sehr gut aufgestellt.

Seminar Softwaresystemtechnologie (18-su-2080)

Es geht weniger um dieses Seminar,
als darum *überhaupt* Seminare und
Praktika zu belegen!

- Thema: Wissenschaftliche Ausarbeitung zu verschiedenen Themen.
- Es gibt in **fast jedem Fachgebiet** die Möglichkeit, Seminare zu belegen.
- In einem Seminar könnt ihr euch intensiv mit einem Thema (und einem Betreuer!) befassen.
- Das Seminar hat mir ermöglicht, in meiner Masterarbeit eine **eigene** Lösung anzubieten.
- Weitere belegte Seminare/Praktika: Seitenkanalresistente Krypto, Seminar IT für Frieden und Sicherheit, HDL Lab, C/C++ Praktikum, Sichere Mobile Netze, Projektseminar Autonomes Fahren 1, Blockchain Praktikum, ...

Warum also iST und nicht nur Informatik?

iST – Ingenieursstudium

- Welche Einschränkungen bestehen in meinem Modell?
- Welche Aspekte werden nicht berücksichtigt?

Beispiel: Seitenkanalangriffe

Informatik – Formale Betrachtung

- Was für Modelle gibt es?
- Was kann ich in diesen Modellen zeigen?
- Wie kann ich es in den Modellen zeigen?

Beispiel: Sicherheitsbeweise

Was es braucht...

- Selbstreflexion
- Kontakt zu Kommilitonen
- Ausdauer
- Sinn für Ästhetik und Idealismus
- Übersicht und Planung

- Was könnt ihr besser als euer Sitznachbar? Was nicht?
 - Ehrlich!
 - Probiert eure Thesen aus.
 - Ich habe auch ESHO1 oder „Beherrschen Moderner Prozessoren für Eingebettete Systeme“ belegt. Mit entsprechend überschaubarem Erfolg.
- Was möchtet ihr? Was möchtet ihr nicht?
 - Zielsetzung für euer Studium
- Seid ihr hier richtig?
 - Lohnt sich der Aufwand für euch? Lassen sich eure Ziele einfacher erreichen, als über dieses Studium?

Kontakt zu Kommilitonen

- Unterschiedliche Menschen, unterschiedliche Fähigkeiten.
- Lernt voneinander!
- Unterstützt euch gegenseitig.
- Verbringt auch mal so einen gemeinsamen Abend.

- (Fast) jeder zweifelt mal, ob die Studienwahl richtig ist.
 - Glaubt nicht, eure Kommilitonen würden das nicht tun.
 - Ihr seid damit nicht alleine. Ihr habt Ansprechpartner:
 - Bei stofflichen/inhaltlichen Problemen:
 - Dozent (Sprechstunden werden viel zu selten genutzt!)
 - Übungsleiter
 - Kommilitonen
 - Bei sonstigen Schwierigkeiten:
 - Studienberatung
 - Fachschaft
 - Studierendenwerk
 - uvm.
 - 1-2 Mal im Jahr für 1-2 Wochen ist vollkommen normal und im Rahmen!
 - Bevor ihr hinschmeißt: Macht euch bewusst, was ihr verpasst.
 - Vorsicht bei Phasen der Niedergeschlagenheit >2 Wochen.
- Respektiert eure Grenzen
 - Wer das Wochenende immer durcharbeitet, wird das früher oder später bezahlen.
 - Das gilt insbesondere für Abschlussarbeiten.

Ihr werdet mit einem iST-Master gut verdienen, aber

um mit möglichst **geringem** Aufwand
an möglichst **viel** Geld zu kommen

seid ihr hier nicht richtig.

Ihr braucht eine gewisse Begeisterung für das Studium.

Idealismus und Ästhetik

- Es gibt technisch
 - schöne Lösungen
 - unschöne Lösungen
- Was ist für euch eine technisch schöne Lösung?
- Wenn ihr eine seht: Freut euch!
- Wie ein Kunststudierender an einem schönen Gemälde.

Übersicht und Planung

Professuren am Fachbereich etit

TU Darmstadt > Fachbereich etit > Der Fachbereich > Professuren

Aktuelle Professorinnen und Professoren

Name	Kontakt
 <p>Prof. Dr.-Ing. Jürgen Adamy > Regelungsmethoden und Intelligente Systeme</p>	<p>✉ adamy@mr.tu-... ☎ -25050 📠 5310 418</p>
 <p>Prof. Dr.-Ing. habil. Dr. h.c. Andreas Binder > Elektrische Energiewandlung</p>	<p>✉ andreas.binder@tu-... ☎ -24180 📠 5310 315</p>
 <p>Prof. Dr. rer. nat. Oliver Boine-Frankenheim > Beschleunigerphysik</p>	<p>✉ boine-frankenheim@temf.tu-... ☎ -20026 📠 5217 226</p>
 <p>Prof. Ph.D. Thomas R. Burg > Integrierte Micro-Nano-Systeme</p>	<p>✉ tburg@micronano.tu-...</p>

Professuren und Gruppenleitungen

Name	Arbeitsgebiet(e)
Professuren	
 <p>Prof. Dr. Carsten Binnig ></p>	→ Daten- und AI-Systeme
 <p>Prof. Christian Bischof, Ph.D. ></p>	→ Scientific Computing
 <p>Prof. Sebastian Faust, Ph.D. ></p>	→ Angewandte Kryptographie
 <p>Prof. Dr. Dr. eh. Dieter Fellner ></p>	→ Graphisch-Interaktive Systeme, → Leiter des Fraunhofer-Instituts für Graphische Datenverarbeitung
 <p>Prof. Dr. Marc Fischlin ></p>	→ Kryptographie und Komplexitätstheorie

Bachelorstudiengang

Informationssystemtechnik (B.Sc.)

Studien- und Prüfungsplan (Anhang I; Stand: 01.10.2018)

Legende		Prüfungsleistungen				Kurs		Semester															
Bewertungssystem:		Fachprüfung	Studienleistung	Prüfungsform	Dauer (min)	Gewichtung	SWS	Status	Lernform	Semester	Die Zuordnung von Kursen/Prüfungen zu Semestern ist dann verbindlich, wenn der Kurs Status "I" ist.												
Prüfungsform:											Arbeitsaufwand pro Semester (CP)												
Dauer:		Semesterwochenstunden		CP																			
Gewichtung:		Bei Kursen = Gewichtung der Prüfungsnote für die Modulnote		Bei Modulen = Gewichtung der Modulnote für die Gesamtnote																			
Status:		o = obligatorisch, f = fakultativ, l = obligatorisch im angeg. Sem.																					
Art der Lehrform:		W = integrierte Veranstaltung, Pr = Praktikum, PP = Projektpraktikum,																					
CP:		Leistungspunkte (Credit Points)																					
TU-CM-Nr. und Zuordnung von CP zu Modulausscheiden haben informativen Charakter. Die Anrechnung der CPs erfolgt nach Abschluss des Moduls.												1.		2.		3.		4.		5.		6.	
1. Grundlagen der Mathematik (12 CP)												32		8		8		8		8		8	
												8		8		8		8		8		8	
												8		8		8		8		8		8	
												8		8		8		8		8		8	
												40		9		9		9		6		7	
												20		9		9		2					
												2		2		2							
												7		5									
												4		2									
												1		2									

Wahlbereiche B.Sc. / M.Sc. Informationssystemtechnik (PO 2015)

Modulhandbuch
SB IST
Stand: 20.07.2022



Danke für die Aufmerksamkeit.

Fragen?