Orientierungsveranstaltung IST

Theoretische Informatik und IT-Sicherheit

Profil

TECHNISCHE UNIVERSITÄT DARMSTADT

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?

Was konnte ich besser als meine Kommilitonen?

Was konnte ich schlechter als meine Kommilitonen?

Was habe ich über mich selbst gelernt?

TECHNISCHE UNIVERSITÄT DARMSTADT

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?

TECHNISCHE UNIVERSITÄT DARMSTADT

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

TECHNISCHE UNIVERSITÄT DARMSTADT

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

Identische Methodik!

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

Identische Methodik!

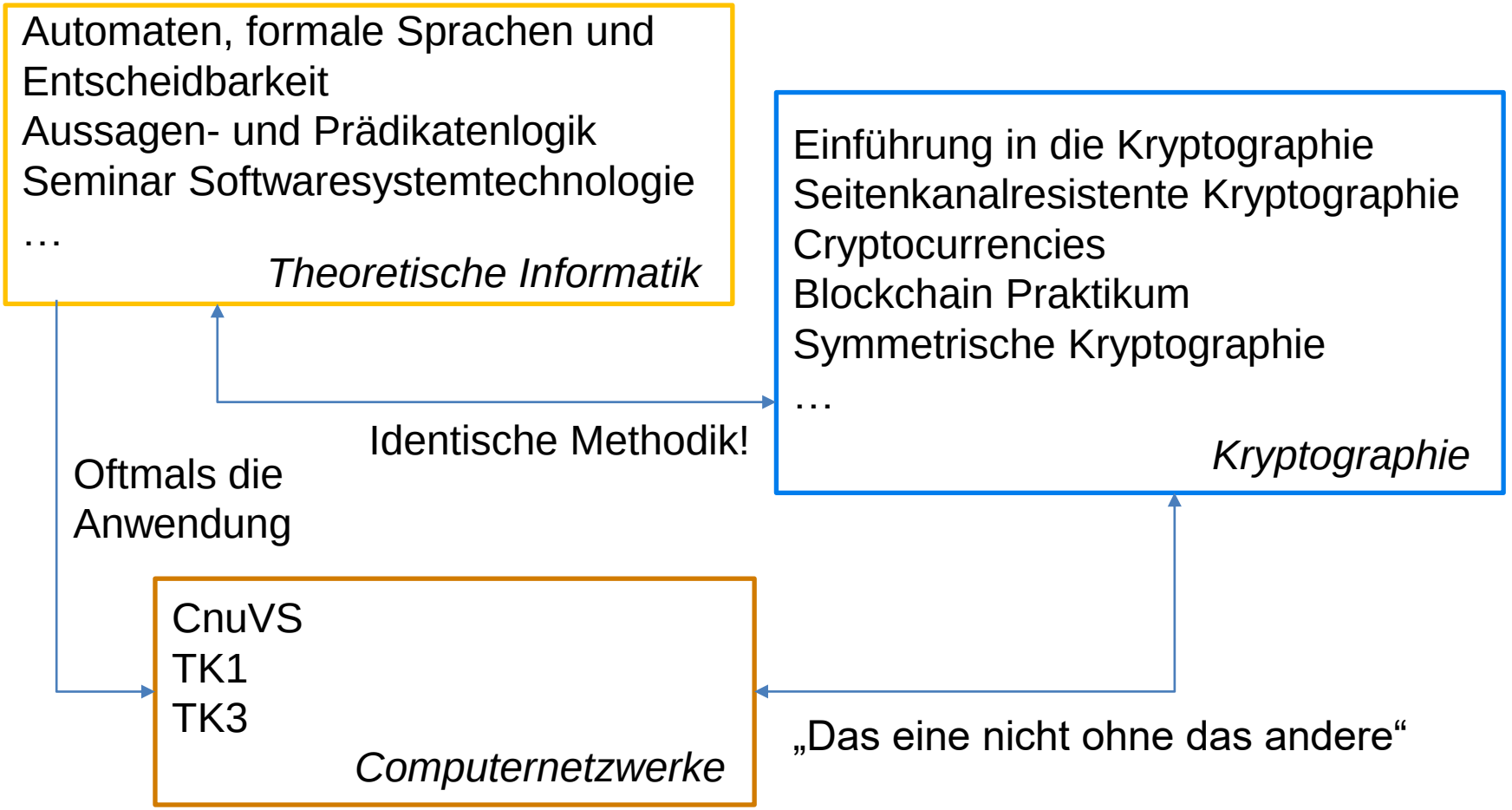
Einführung in die Kryptographie
Seitenkanalresistente Kryptographie
Cryptocurrencies
Blockchain Praktikum
Symmetrische Kryptographie
…

Kryptographie

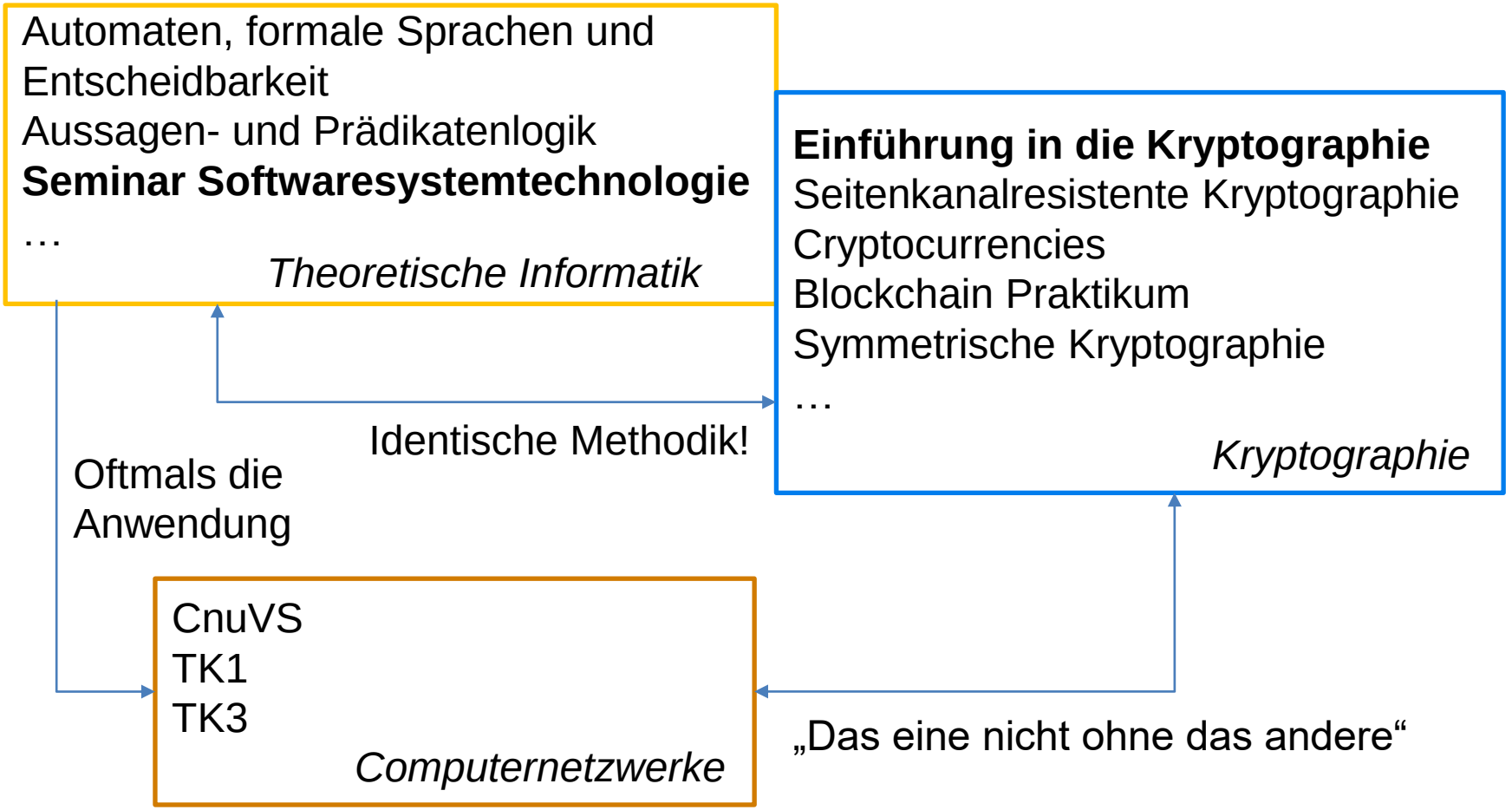
CnuVS
TK1
TK3

Computernetzwerke

Meine Themenschwerpunkte



Meine Themenschwerpunkte



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

TECHNISCHE UNIVERSITÄT DARMSTADT

- 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)

TECHNISCHE UNIVERSITÄT DARMSTADT

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, …

Untypischer iSTler

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

Selbstreflexion

TECHNISCHE UNIVERSITÄT DARMSTADT

- 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

TECHNISCHE UNIVERSITÄT DARMSTADT

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

Ausdauer

- (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.

Idealismus und Ästhetik

TECHNISCHE UNIVERSITÄT DARMSTADT

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

TECHNISCHE UNIVERSITÄT DARMSTADT

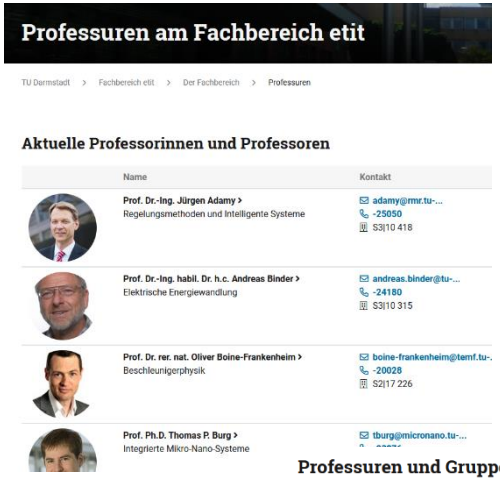
- Es gibt technisch
  - schöne Lösungen
  - unschöne Lösungen

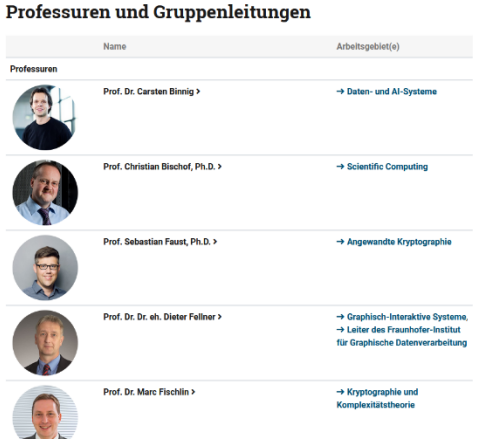
- Was ist für euch eine technisch schöne Lösung?

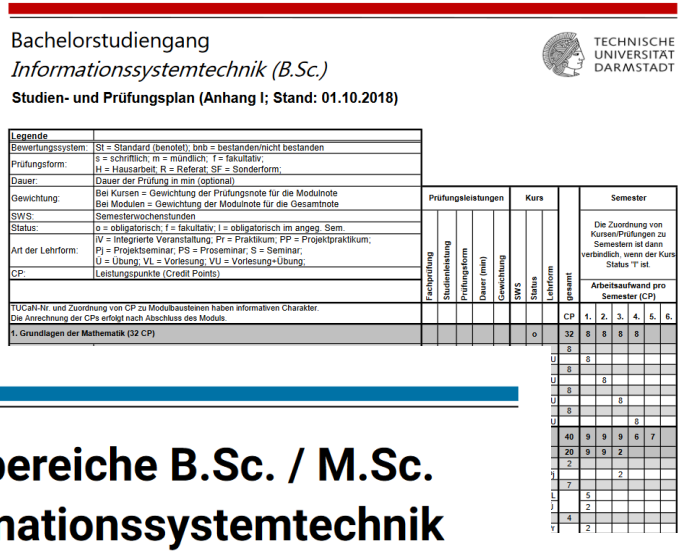
- Wenn ihr eine seht: Freut euch!

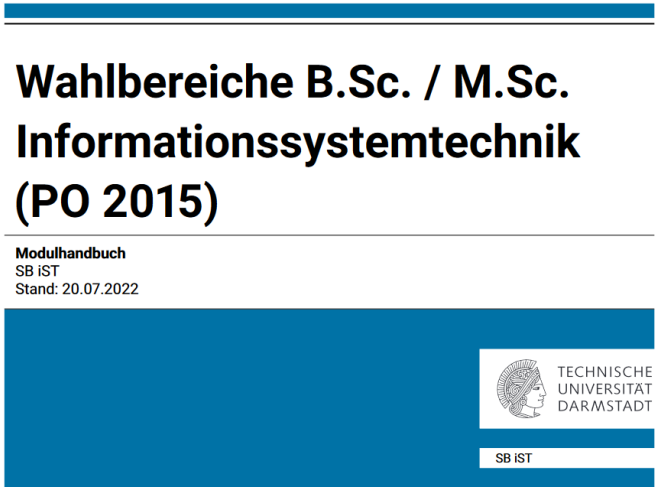
- Wie ein Kunststudierender an einem schönen Gemälde.

Übersicht und Planung









Danke für die Aufmerksamkeit.

Fragen?