

Digitaltechnik

Wintersemester 2021/2022

14. Vorlesung



1. Abschluss Digitaltechnik
2. Evaluation
3. Klausurinhalt
4. Klausurorganisation
5. Ausblick
6. Fragen im Plenum

Anwendungs- software		Programme
Betriebs- systeme		Gerätetreiber
Architektur		Befehle Register
Mikro- architektur		Datenpfade Steuerung
Logik		Addierer Speicher
Digital- schaltungen		UND Gatter Inverter
Analog- schaltungen		Verstärker Filter
Bauteile		Transistoren Dioden
Physik		Elektronen

Agenda

1. Abschluss Digitaltechnik

2. Evaluation

3. Klausurinhalt

4. Klausurorganisation

5. Ausblick

6. Fragen im Plenum

Anwendungs- software		Programme
Betriebs- systeme		Gerätetreiber
Architektur		Befehle Register
Mikro- architektur		Datenpfade Steuerung
Logik		Addierer Speicher
Digital- schaltungen		UND Gatter Inverter
Analog- schaltungen		Verstärker Filter
Bauteile		Transistoren Dioden
Physik		Elektronen

Aus TUCaN / Modulhandbuch: Lehrinhalte



- ▶ *Digitaltechnik*: digitale Abstraktion und ihre technische Umsetzung, Zahlensysteme, Logikgatter, MOSFET Transistoren und CMOS Gatter
- ▶ *Kombinatorische Schaltungen*: boole'sche Gleichungen und Algebra, Abbildung auf Gatter, mehrstufige Schaltungen, vierwertige Logik (0,1,X,Z), Minimierung von Ausdrücken, kombinatorische Grundelemente, Zeitverhalten
- ▶ *Sequentielle Schaltungen*: Latches, Flip-Flops, Entwurf synchroner Schaltungen, endliche Automaten, Zeitverhalten, Parallelität
- ▶ *Hardware-Beschreibungssprachen*: Modellierung kombinatorischer und sequentieller Schaltungen, Strukturbeschreibungen, Modellierung endlicher Automaten, Datentypen, parametrisierte Module, Testrahmen
- ▶ *Grundelemente digitaler Schaltungen*: arithmetische Schaltungen, sequentielle Grundelemente, Speicherfelder, Logikfelder



- ▶ Studierende **verstehen** nach erfolgreichem Besuch der Veranstaltung die *Konzepte und Grundelemente der digitalen Logik* sowie ihre *technologische Realisierung*.
- ▶ Sie können diese Kenntnisse **selbstständig anwenden**, um zielgerichtet *kombinatorische und sequentielle Schaltungen* zu **konstruieren** und in einer *Hardware-Beschreibungssprache* zu **implementieren**.
- ▶ Sie können *digitale Schaltungen* bezüglich *funktionaler und nicht-funktionaler Eigenschaften* **analysieren**.
- ▶ vgl. didaktische Kompetenzhierarchie:
verstehen → *anwenden* → *analysieren/bewerten* → *erzeugen*

Agenda



1. Abschluss Digitaltechnik
2. Evaluation
3. Klausurinhalt
4. Klausurorganisation
5. Ausblick
6. Fragen im Plenum

Anwendungs- software		Programme
Betriebs- systeme		Gerätetreiber
Architektur		Befehle Register
Mikro- architektur		Datenpfade Steuerung
Logik		Addierer Speicher
Digital- schaltungen		UND Gatter Inverter
Analog- schaltungen		Verstärker Filter
Bauteile		Transistoren Dioden
Physik		Elektronen

- ▶ Herzlichen Dank fürs Ausfüllen der Evaluation! VL: $N = 89$, ÜB: $N = 53$
- ▶ Durch konstruktives Feedback können Lehrveranstaltungen kontinuierlich verbessert werden.
- ⇒ Bitte unterstützen Sie aktiv die Lehrevaluationen in Ihrem weiteren Studium!

Vorlesung – Inhalt + Organisation



- 3.1) Die Vorlesung war inhaltlich gut strukturiert.
- 3.2) Die Organisation der Vorlesung war gut.
- 3.3) Die Lernziele der Vorlesung sind mir klar geworden.
- 3.4) Der Stoff wurde anhand von Beispielen verdeutlicht.
- 3.5) Der Bezug zwischen Theorie und praktischen Arbeiten bzw. praktischen Anwendungen wurde hergestellt.
- 3.6) Die (Zwischen-)Fragen der Studierenden wurden angemessen beantwortet.
- 3.7) Die Vorlesungsmaterialien (Folien, Skripte, Tafelanschrieb, Lehrbücher, e-Learning, etc.) haben das Lernen wirkungsvoll unterstützt.
- 3.8) Die Vorlesung motivierte dazu, sich außerhalb der Veranstaltung selbstständig mit den behandelten Themen auseinander zu setzen.
- 3.9) Ich habe durch diese Veranstaltung viel gelernt.
- 3.10) Mein Vorwissen war ausreichend, um der Vorlesung folgen zu können.
- 3.11) Ich kann abschätzen, was in der Prüfung von mir erwartet wird.
- 3.12) Ich habe vor, in diesem Semester die Prüfung anzutreten.
- 3.13) Der Raum war für die Vorlesung geeignet.

trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu

Vorlesung – Lehrkraft

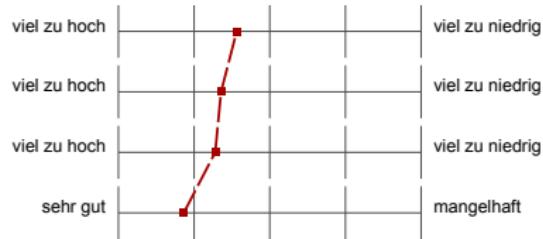
- 4.1) Die Lehrkraft hat Kompliziertes verständlich dargelegt.
- 4.2) Die Lehrkraft zeigte sich gut vorbereitet.
- 4.3) Die Lehrkraft hat die Vorlesung rhetorisch gut gestaltet.
- 4.4) Die Lehrkraft hat die Vorlesung didaktisch gut gestaltet.
- 4.5) Die Veranstalter waren auch außerhalb der Vorlesung ansprechbar.
- 4.6) Die Lehrkraft regte gezielt zum Mitdenken und zu eigener Mitarbeit in der Vorlesung an.
- 4.7) Die Lehrkraft hat elektronische Plattformen sinnvoll und hilfreich eingesetzt.
- 4.8) Die Sprachkenntnisse der Lehrkraft in der Vorlesungssprache waren gut.
- 4.9) Die Lehrkraft hielt die Vorlesung größtenteils selbst.

trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu
trifft zu					trifft nicht zu

Vorlesung – Gesamteindruck



- 7.2) Die Geschwindigkeit der Vorlesung war ...
- 7.3) Das Niveau der Vorlesung war ...
- 7.4) Der Arbeitsaufwand für die Vorlesung war ...
- 7.5) Welche Gesamtnote gibst du der Vorlesung (ohne Übungen)?



- + technische Umsetzung der digitalen Lehre (insb. Zoom Webinar mit Live Q&A)
- + Organisation und vorzeitiges Bereitstellen von Materialien
- + regelmäßige Umfragen und Pausen
- + gute Abstimmung mit Lehrbuch
- + viele Beispiele
- + “[Lehrender] ist ein cooler Dude, aber auch die Vertretung war echt gut, man hat keinen qualitativen Unterschied gemerkt.”

- ↗ Tempo zu hoch (insb. bei SystemVerilog)
- ↗ Tools zum Erstellen von Schaltplänen wünschenswert
- ↗ Aufgabenstellung in Projekten nicht repräsentativ für Klausurfragen
- ↗ scheinbar hohe Durchfallquote, keine Altklausuren verfügbar

Übung – Aufgaben



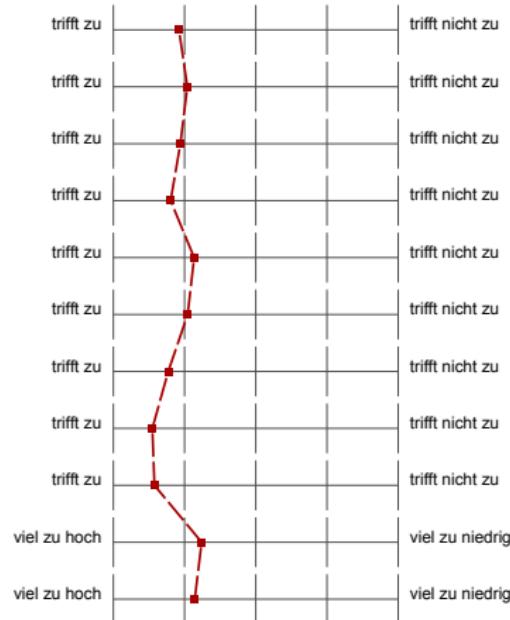
- 3.1) Durch die Aufgaben und den Übungsbetrieb habe ich viel gelernt.
- 3.2) Die Übungen haben mir geholfen, den Stoff der Vorlesung besser zu verstehen.
- 3.3) Die Aufgabenstellungen waren verständlich.
- 3.4) Die Übungsaufgaben hatten inhaltlich eine klare Struktur.
- 3.5) Die Übungsaufgaben waren motivierend.
- 3.6) Es wurden ausreichend Lösungsvorschläge bereitgestellt bzw. präsentiert.
- 3.7) Der Stoff der Vorlesung war gut auf die Übungen abgestimmt.
- 3.8) Mein Vorwissen war ausreichend, um die Übungsaufgaben bearbeiten zu können.

trifft zu	<input type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu
trifft zu	<input checked="" type="checkbox"/>	trifft nicht zu

Übung – Organisation



- 4.1) Die Übung war inhaltlich gut strukturiert.
- 4.2) Die Lernziele der Übung sind mir klar geworden.
- 4.3) Die Organisation des Übungsbetriebs war gut.
- 4.4) Es wurde genug Übungsmaterial (Aufgaben, etc.) zur Verfügung gestellt.
- 4.5) Es stand genug Zeit für die Bearbeitung der Aufgaben zur Verfügung.
- 4.6) Die Abgaben waren gut vereinbar mit anderen Veranstaltungen laut Regelstudienplan.
- 4.7) Die Auswahlmöglichkeiten der Termine waren angemessen bzw. der Übungszeitpunkt war passend.
- 4.8) Die Gruppengröße war zufriedenstellend.
- 4.9) Der Raum für die Übungen war zum Arbeiten und Lernen geeignet.
- 4.10) Das Anspruchsniveau der Aufgaben war ...
- 4.11) Der Aufwand für die Bearbeitung der Aufgaben war ...



Übung – Tutoren



- 5.3) ... hat die Gruppe motiviert.
- 5.4) ... war fachlich kompetent.
- 5.5) ... zeigte sich gut vorbereitet.
- 5.6) ... hat die Übungstunde gut strukturiert.
- 5.7) ... war engagiert.
- 5.8) ... stellte wesentliche Punkte zur Bearbeitung der Aufgaben vor.
- 5.9) ... regte mich gezielt zum Mitdenken und zu eigener Mitarbeit an.
- 5.10) ... setzte verfügbare Medien (z. B. Tafel, Projektor, Beamer) sinnvoll ein.
- 5.11) ... hat elektronische Plattformen sinnvoll und hilfreich eingesetzt.
- 5.12) ... erschien pünktlich.
- 5.13) ... behandelte alle Studierenden respektvoll.
- 5.14) ... teilte die Zeit zwischen den Studierenden angemessen auf.
- 5.15) ... hat konstruktives bzw. gutes Feedback gegeben.
- 5.16) ... hat nachvollziehbar bewertet bzw. benotet.

trifft zu	trifft nicht zu

Übung – Gesamteindruck

7.2) Welche Gesamtnote gibst du dem*der Tutor*in?

7.3) Welche Gesamtnote gibst du der Übung?



Übung – Fazit (Auswertung Freitextfelder)

- + engagierte, geduldige und nette Tutoren
- + Tablet Version von Übungsblättern
- + angenehme Gruppengröße (nach einigen Wochen...)
- + Miro als Kollaborationstool
- + Angebot der Präsenzübung

- ↗ unrealistische Zeitangaben
- ↗ Bedienung von Miro mit Maus/Trackpad
- ↗ technische Ausstattung von Tutoren (Mikroqualität, etc.)
- ↗ kein ausführliches Feedback zu Projekten

Agenda



1. Abschluss Digitaltechnik
2. Evaluation
3. Klausurinhalt
4. Klausurorganisation
5. Ausblick
6. Fragen im Plenum

Anwendungs- software		Programme
Betriebs- systeme		Gerätetreiber
Architektur		Befehle Register
Mikro- architektur		Datenpfade Steuerung
Logik		Addierer Speicher
Digital- schaltungen		UND Gatter Inverter
Analog- schaltungen		Verstärker Filter
Bauteile		Transistoren Dioden
Physik		Elektronen

- ▶ Prüfungsrelevanter Stoff:
 - ▶ VL1 bis VL13
 - ▶ ÜB1 bis ÜB13 (ohne Zusatzaufgaben)
- ▶ Klausuraufbau
 - ▶ 10 Aufgaben
 - ▶ 9 Punkte pro Aufgabe
 - ⇒ $10 \times 9 = 90$ Punkte erreichbar
 - ▶ 1 Punkt entspricht etwa einer Minute der Bearbeitungszeit
 - ▶ Bestehengrenze: 45 Punkte (50 %)
- ▶ Aufbau der Aufgaben je Themenblock
 - ▶ 3× Wissens- und Verständnisfragen (3 Punkte)
 - ▶ 1× Übungsaufgabe (3 Punkte)
 - ▶ 1× Transferaufgabe (3 Punkte)



- ▶ Vorlesungsfolien, Übungsblätter und Projektaufgaben
- ▶ Referenzliteratur (hauptsächlich **Harris 2013/2016**)
- ▶ Moodle Kurs “Digital Logic Design”
- ▶ nicht bereitgestellt werden
 - ▶ Altklausuren
 - ▶ Projektlösungen
- ▶ für (System)Verilog
 - ▶ <https://www.mikrocontroller.net/articles/Verilog>
 - ▶ <http://www.chipverify.com/verilog-tutorial>
 - ▶ <http://www.chipverify.com/system-verilog/system-verilog>

Agenda



1. Abschluss Digitaltechnik
2. Evaluation
3. Klausurinhalt
4. Klausurorganisation
5. Ausblick
6. Fragen im Plenum

Anwendungs- software		Programme
Betriebs- systeme		Gerätetreiber
Architektur		Befehle Register
Mikro- architektur		Datenpfade Steuerung
Logik		Addierer Speicher
Digital- schaltungen		UND Gatter Inverter
Analog- schaltungen		Verstärker Filter
Bauteile		Transistoren Dioden
Physik		Elektronen



- ▶ Bis 20.02.2022: Korrektur Projekt Teil 3 abgeschlossen (planmäßig)
 - ▶ Eintragung der Studienleistung in TUCaN
 - ▶ Studienbüro prüft Klausurzulassung
- ▶ Bis 04.03.2022: Raumeinteilung wird in Moodle bekannt gegeben
 - ▶ S1|01 A1 (Audimax), A01, A03 (im Keller)
 - ▶ L4|02 1, 2, 201, 202 (HMZ)
 - ▶ Darmstadtium Spectrum
- ▶ Durchführung am **08.03.2022** ab 11:00 Uhr
- ▶ Ergebnisse werden in TUCaN veröffentlicht

- ▶ Die **Abmeldung** ist ohne Angabe von Gründen über TUCaN bis 7 Tage vor der jeweiligen Fachprüfung möglich
- ▶ **Sonderregelung Wintersemester 2021/2022:** Sie können bis zum Beginn der Prüfung formlos zurücktreten, eine E-Mail an das **Studienbüro** mit Angabe der Prüfungs- und Ihrer Matrikelnummer ist ausreichend, auf Vorlage eines Attestes wird ausnahmsweise verzichtet
- ▶ Sollten Sie über ein **ärztliches Attest** verfügen und **einreichen**, bitte beachten:
 - ▶ Wenn das Attest über einen Zeitraum geht, in dem Sie von mehreren Prüfungen krankheitsbedingt zurücktreten wollen, tragen Sie alle betroffenen Prüfungen ein
 - ▶ Nehmen Sie trotz Attest an einer Prüfung teil, wird das Ergebnis gewertet
 - ▶ Rückwirkend ausgestellte Atteste werden nicht unbegründet angenommen

- ▶ Wird die Fachprüfung als nicht ausreichend bewertet oder gilt sie als nicht bestanden, kann sie zweimal wiederholt werden
- ▶ Termin im Sommersemester 2022 noch nicht bekannt
- ▶ Studienleistung muss jedoch bereits vorliegen

Klausurdurchführung am 08.03.22 ab 11:00



- ▶ Unbedingt mitbringen:
 - ▶ Lichtbildausweis (Personalausweis, Führerschein, etc.)
 - ▶ Studienausweis
 - ▶ dokumentenechter Stift (Kugelschreiber oder Füller) in blau oder schwarz
 - ▶ **3G-Nachweis** (Vorraussetzung für Einlass)
 - ▶ geeignete Maske (medizinische OP- oder FFP2-Maske)
⇒ Maskenpflicht in allen Gebäuden und während der Prüfung sowie bei An- und Abreise mit ÖPNV
- ▶ **Wegführung im Darmstadium** sowie Mindestabstand beim Betreten und Verlassen der Gebäude/Prüfungsräume beachten
- ▶ Hilfsblatt und Zusatzpapier liegt der Klausur bei
- ▶ Keine Hilfsmittel (Taschenrechner, etc.) erlaubt
- ▶ Deckblatt mit Hinweisen zur Klausurdurchführung in Moodle verfügbar



- ▶ 3G-Nachweis bedeutet **einer** der folgenden Nachweise:
 - ▶ **2G-Bändchen** der TU Darmstadt
 - ▶ Digitaler Impf-/Genesenennachweis (CovPass oder Corona Warn-App)
 - ▶ Impfpass, Impfzertifikat, EU–COVID-Zertifikat oder Genesenenzertifikat (**im Original!**) oder offizielles Ersatzformular
 - ▶ Testnachweis aus einem **Testzentrum** (digital oder in Papierform)
 - ⇒ Antigen-Schnelltest max. 24h alt, PCR-Test max. 48h alt
 - ⇒ Selbsttests werden **nicht** anerkannt!
- ▶ Personen **ohne Nachweis** nach §3 CoSchV haben den Veranstaltungsraum und das Gebäude unverzüglich zu verlassen – andernfalls können sie wegen Hausfriedensbruch belangt werden

Klausurdurchführung am 08.03.22 ab 11:00



TECHNISCHE
UNIVERSITÄT
DARMSTADT

- Ideal: **2G-Bändchen** (<https://www.tu-darmstadt.de/baendchen>)

2G-Bändchen für Klausuren

Wenn Sie geimpft oder genesen sind, besorgen Sie sich bitte spätestens einen Tag vor der Klausur das 2G-Bändchen und unterstützen damit den reibungslosen Einlass in die Prüfungsräume.

www.tu-darmstadt.de/baendchen

The slide features a large blue arrow pointing from left to right, containing the main text. In the background, there is a photograph of a lecture hall with rows of wooden desks and chairs. On the right side of the slide, there is a vertical banner with the university's logo and the text "TECHNISCHE UNIVERSITÄT DARMSTADT" and "Computer Science".

Klausurdurchführung am 08.03.22 ab 11:00



1. Der Einlass erfolgt erst auf unsere Aufforderung und geordnet unter Einhaltung des Mindestabstands
2. Beim Einlass wird das 2G-Bändchen oder der 3G-Nachweis kontrolliert
3. Die Klausuren befinden sich bereits an den Sitzplätzen, keiner blättert oder schreibt
4. Die allgemeinen Hinweise des Deckblatts werden verlesen
5. Das Deckblatt wird ausgefüllt
6. Auf Kommando beginnt die Bearbeitungszeit
7. Nach Ende der Bearbeitungszeit werden *sofort* alle Stifte weggelegt
8. Die Klausuren verbleiben am Platz, verlassen Sie den Saal unter Einhaltung des Mindestabstands

Allgemeine Hinweise zur Klausurdurchführung

- ▶ Schalten Sie alle elektronischen Geräte (Smartphones, Smartwatches, etc.) aus.
- ▶ Packen Sie alles bis auf Ihr Schreibwerkzeug weg und verschließen Sie Ihre Taschen. Es sind *keine* Hilfsmittel (Taschenrechner, etc.) erlaubt. Wird während der Klausur ein unerlaubtes Hilfsmittel gefunden, wird dies als Täuschungsversuch gewertet und gemäß §38 APB sanktioniert. In schweren Fällen behalten wir uns weitere Schritte bis hin zur Exmatrikulation vor.
- ▶ Legen Sie Ihren Studienausweis und einen Lichtbildausweis (Personalausweis, Führerschein, etc.) zur Kontrolle rechts neben sich bereit.
- ▶ Nur mit dokumentenechten Stiften (Kugelschreiber oder Füller) in blau oder schwarz erstellte Lösungen werden gewertet.
- ▶ Tragen Sie Ihre persönlichen Informationen auf dem Deckblatt ein und unterschreiben Sie dieses.
- ▶ Die Heftung der Klausur darf nicht gelöst werden. Ausnahme ist das angehängte Hilfsblatt.

Allgemeine Hinweise zur Klausurdurchführung

- ▶ Essen und Trinken ist erlaubt, nehmen Sie jedoch Rücksicht auf Ihre Kommiliton*innen.
- ▶ Bewertet wird insbesondere der Lösungsweg, nicht nur das Ergebnis. Geben Sie daher alle nötigen Zwischenschritte an.
- ▶ Sollten Sie mehr als eine Lösung zu einer Aufgabe abgeben, wird diese mit Null Punkten bewertet.
- ▶ Aufgrund der aktuellen Situation ist die Beantwortung individueller Nachfragen zur Aufgabenstellung durch einzelne Prüflinge während der Klausur leider nicht möglich.
- ▶ Eigenes Papier ist *nicht* gestattet. Für den Fall, dass Sie zusätzliches Papier benötigen, befinden sich am Ende der Klausur drei leere Seiten für Notizen und Lösungen. Beschriften Sie diese Seiten eindeutig mit den Aufgabenummern, für welche die Lösungen gewertet werden sollen.

- ▶ Falls Sie auf Toilette müssen, zeigen Sie dies dem Aufsichtspersonal an. Während des Toilettengangs verbleibt die Klausur am Platz. Es kann zu jedem Zeitpunkt nur eine Person den Raum verlassen.
- ▶ Die späteste Möglichkeit zum Toilettengang ist 15 min vor Ende der Bearbeitungszeit, eine vorzeitige Abgabe ist nicht erlaubt.
- ▶ Klausuren dürfen keinesfalls mitgenommen werden, auch wenn sie nicht bewertet werden sollen.



Pause

Agenda



1. Abschluss Digitaltechnik
2. Evaluation
3. Klausurinhalt
4. Klausurorganisation
5. Ausblick
6. Fragen im Plenum

Anwendungs- software		Programme
Betriebs- systeme		Gerätetreiber
Architektur		Befehle Register
Mikro- architektur		Datenpfade Steuerung
Logik		Addierer Speicher
Digital- schaltungen		UND Gatter Inverter
Analog- schaltungen		Verstärker Filter
Bauteile		Transistoren Dioden
Physik		Elektronen

Wie geht es weiter? Vertiefung Hardware-naher Themen in



- ▶ Rechnerorganisation
 - ⇒ Prozessorarchitekturen, Befehlssätze, Assemblerprogramme, Mikroarchitekturen, Speicherhierarchie, virtuelle Speicher, Leistungsbewertung
- ▶ Architekturen und Entwurf von Rechnersystemen
 - ⇒ Technologische Trends der Mikroelektronik, Hardware-Entwurfstechniken (mit Bluespec-Verilog), Architekturen für parallele Ausführung, Heterogene Systems-on-Chip, On-Chip und Off-Chip Kommunikationsstrukturen
- ▶ (Fortgeschritten) Compilerbau
 - ⇒ Hochsprachen-Programme (z.B. C, Java) nach Assembler übersetzen, ISA-spezifische Optimierungen (z.B. Registerallokation, Schleifenoptimierung)
- ▶ Embedded-Systems Hands-On
 - ⇒ Praxis-nahe Einsatz von Mikroprozessoren / FPGAs in kleinen Projekten
- ▶ Kryptographische Protokolle, <https://crypto.de/CRYPTO>
 - ⇒ Sichere Auswertung von Schaltkreisen zum Rechnen unter Verschlüsselung

Cryptography and Privacy Engineering Group (ENCRYPTO)



ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

crypto.de



Our Research Topics (Examples)

In our research, we try to bridge the gap between theory and practice by building automated tools and prototypes, many of which are available as open source at <https://github.com/encryptogroup>.

Cryptography Engineering

- Secure Multi-Party Computation (MPC)
- Private Function Evaluation (PFE)
- Private Set Intersection (PSI)
- Private Information Retrieval (PIR)



Privacy Engineering

- Privacy-Preserving Biometric Identification
- Privacy-Preserving Genomic Computation
- Privacy-Preserving Machine Learning
- Privacy-Preserving Speech Processing



Multi-Party Computation (MPC)

How can multiple parties compute a public function on private data?



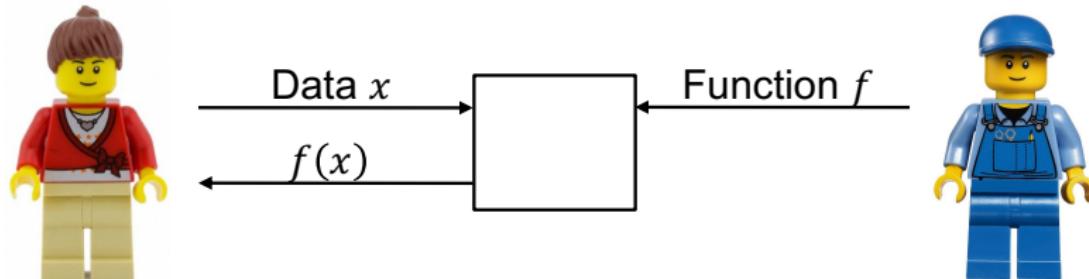
Auctions



Data
Outsourcing

Private Function Evaluation (PFE)

How to evaluate private functions on private data?

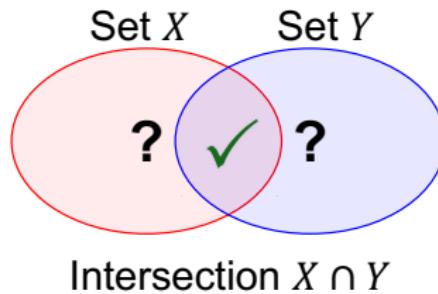


Individual
Insurances



Medical
Diagnostics

How to privately compute set intersection or variants thereof?



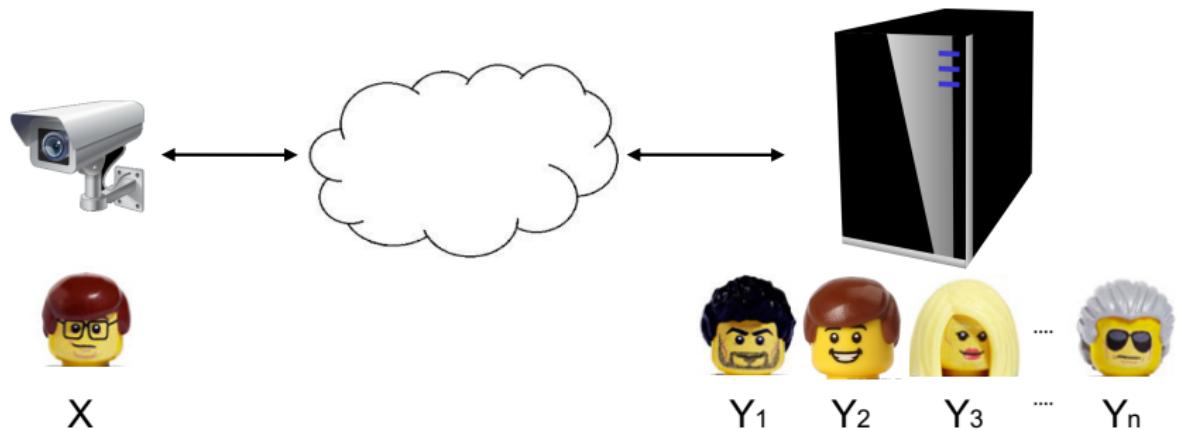
Contact
Discovery



Measuring Ad
Conversion Rates

Check if query is *similar* to an entry in the DB.

- without revealing the query to the server
- without revealing the DB to the client



How to do machine learning under encryption to protect data and models?

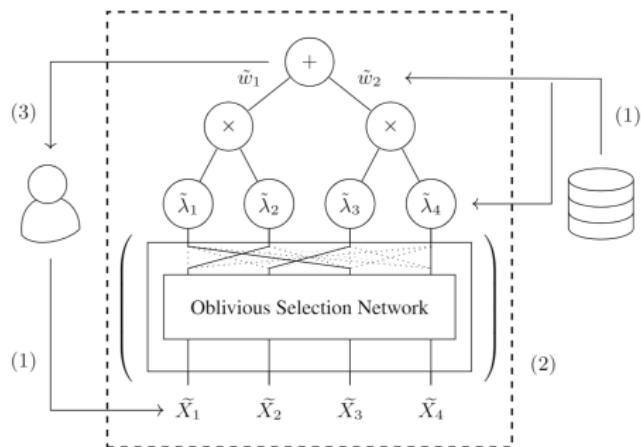
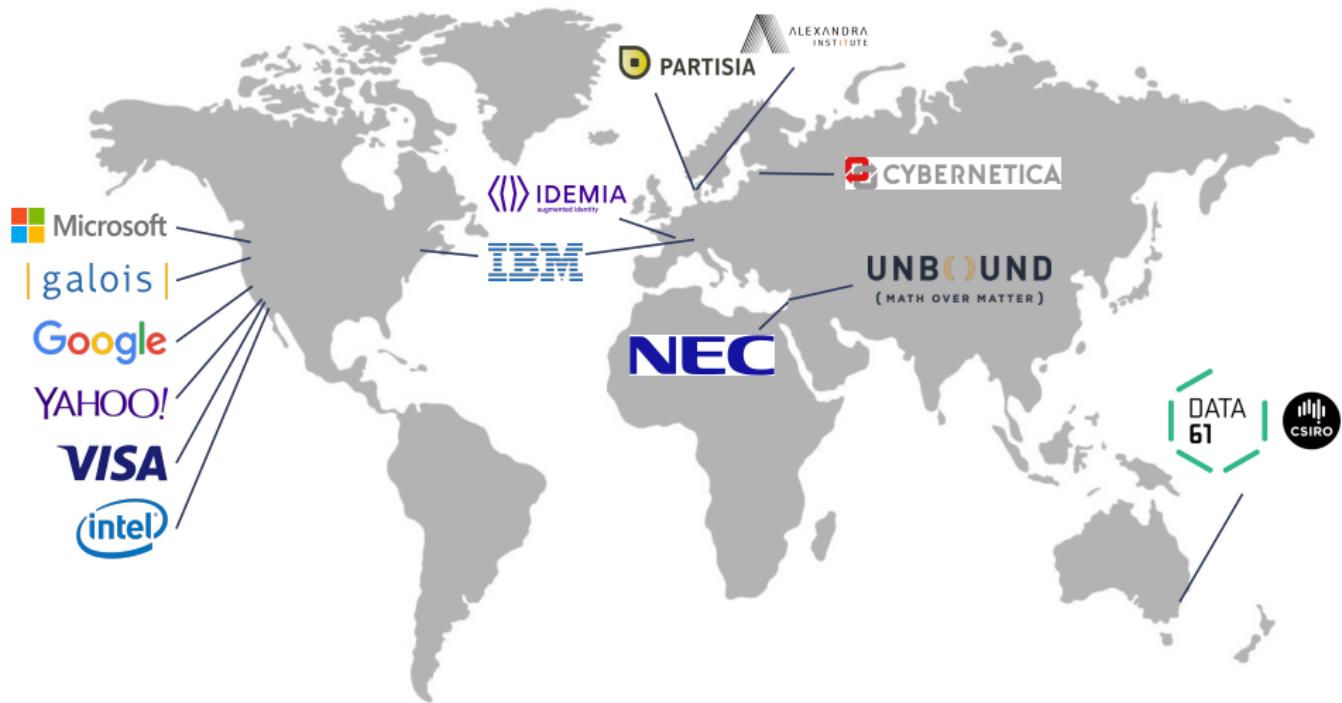


Figure 3. CryptoSPN protocol flow for an exemplary miniature SPN with Poisson leaves: (1) client and server have private inputs $X_1, \dots, 4$ and $w_{1,2}, \lambda_{1, \dots, 4}$, respectively; (2) private evaluation of leaf-, sum- and product nodes using SMPC; (3) client receives SPN inference result.

Companies & Research Labs working on Crypto Protocols





ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

encrypto.de

Bleiben Sie gerne mit uns in Kontakt!



TECHNISCHE
UNIVERSITÄT
DARMSTADT

- ▶ Weitere ENCRYPTO Lehrveranstaltungen
 - ▶ Vorlesung (CRYPROT), Seminar (PRIVTECH) und Praktikum (PRIVDEV) zu Privatsphäre-schützenden Technologien und Kryptographischen Protokollen
 - ▶ <https://crypto.de/teaching>
- ▶ Exzellente und motivierte Studierende sind herzlich willkommen
 - ▶ als Tutoren für Digitaltechnik in kommenden Wintersemestern
 - ▶ Hiwivertrag (Betreuung von 1 oder 2 Gruppen möglich)
 - ▶ Praktikum in der Lehre (5CP)
 - ▶ <https://crypto.de/DT>
 - ▶ als Hiwis für unsere Forschung
 - ▶ Grundkenntnisse in Kryptographie und Programmiererfahrung in C/C++ erforderlich
 - ▶ <https://crypto.de/jobs>
 - ▶ für Bachelor- und Masterarbeiten
 - ▶ Spannende Themen mit Bezug zur IT-Sicherheit / angewandten Kryptographie
 - ▶ <https://crypto.de/theses>



ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

Agenda

1. Abschluss Digitaltechnik
2. Evaluation
3. Klausurinhalt
4. Klausurorganisation
5. Ausblick
6. Fragen im Plenum

Anwendungs- software		Programme
Betriebs- systeme		Gerätetreiber
Architektur		Befehle Register
Mikro- architektur		Datenpfade Steuerung
Logik		Addierer Speicher
Digital- schaltungen		UND Gatter Inverter
Analog- schaltungen		Verstärker Filter
Bauteile		Transistoren Dioden
Physik		Elektronen

Haben Sie konkrete Fragen zur Lehrveranstaltung Digitaltechnik,
die wir jetzt in großer Runde besprechen sollten?

(Alles andere gerne in Moodle)

Herzlichen Dank an

- ▶ Daniel Günther, Amos Treiber und Christian Weinert (ENCRYPTO)
- ▶ Tutor*innen und PidL Studierende
- ▶ Abdulhadi Shoufan (Khalifa University, VAE), Wolfgang Heenes (FB20),
Sabine Haschka (FB20)
- ▶ Sie alle, für rege Teilnahme an der Vorlesung und spannende Fragen!



Vielen Dank und alles Gute!

Nächste Woche am 16.02.2022 entfällt die Vorlesung;
Sie können die Zeit zur Klausurvorbereitung nutzen.