Aktuelle Informatik-Richtungen und Themen für die Dissertation

Künstliche Intelligenz & Machine Learning

- Robustheit neuronaler Netze gegen adversariale Angriffe und Distribution Shift
- Effizientes Training großer Modelle durch Quantisierung, Distillation und Sparse Methods
- Interpretierbarkeit von ML-Modellen: Methoden zur Erklärung komplexer Vorhersagen
- Uncertainty Quantification: zuverlässige Unsicherheitsmaße in Deep Learning
- Fairness in ML: Bias-Erkennung, Mitigation und Bewertungskriterien
- Federated Learning: Stabilität, Sicherheit und heterogene Datenverteilungen
- Reinforcement Learning für reale Systeme: Sample Efficiency und sichere Exploration
- Multimodale Modelle: Fusion von Text, Bild und Sensordaten
- Self-Supervised Learning für domänenspezifische Anwendungen
- Evaluation von ML-Systemen: Benchmarks, Leakage und reproduzierbare Experimente

Data Science & Big Data

- Skalierbare Anomalieerkennung in Streaming-Daten
- Datenqualität und Data Validation: automatische Fehlererkennung in Pipelines
- Feature Engineering und Representation Learning für tabellarische Daten
- Causal Inference in großen Beobachtungsdaten mit robusten Annahmen
- Privacy-preserving Analytics: Differential Privacy in realen Data-Workflows
- Graph Data Science: Link Prediction und Community Detection in Netzwerken
- Zeitreihenanalyse für Industrie und IoT: Forecasting und Change Point Detection
- Entity Resolution und Deduplication in großen Datenbeständen
- Cost-aware Data Processing: Optimierung von Speicher und Rechenkosten

- Monitoring von Daten-Drift und Model Drift in Produktionssystemen

Cybersecurity & Datenschutz

- Erkennung von Angriffen in Cloud- und Container-Umgebungen
- Malware-Analyse mit statischen und dynamischen Methoden
- Zero-Trust-Architekturen: Modellierung und Sicherheitsbewertung
- Threat Intelligence: automatisierte Korrelation von Indikatoren und Ereignissen
- Privacy by Design in Web- und App-Systemen
- Sicherer Software-Supply-Chain: SBOM, Signierung und Pipeline-Absicherung
- Phishing-Detection mit NLP und Verhaltenssignalen
- Angriffserkennung in Netzwerken mit ML und Graphmethoden
- Sicherheit von IoT-Geräten: Firmware, Update-Prozesse, Angriffspfade
- Kryptografische Protokolle: formale Modelle und Sicherheitsnachweise

Software Engineering & Qualitätssicherung

- Automatisierte Tests: Generierung von Testfällen für komplexe Systeme
- Bug Prediction und Code Smells: ML-gestützte Qualitätssicherung
- Software-Architektur-Analyse: technische Schulden und Refactoring-Strategien
- DevOps-Metriken: Messbarkeit von Stabilität, Release-Zyklen und Risiko
- CI/CD-Pipelines: Zuverlässigkeit, Security und Performance-Optimierung
- Programmanalyse zur Erkennung von Fehlern und Sicherheitslücken
- Vergleich von Microservices-Architekturen unter realer Last
- Traceability zwischen Anforderungen, Code und Tests
- Dokumentationsqualität und automatische Wissensextraktion aus Repos
- Code-Review-Optimierung durch semantische Analyse

Distributed Systems & Cloud Computing

- Skalierbarkeit und Konsistenzmodelle in verteilten Datenbanken
- Fault Tolerance: Recovery-Strategien und Resilienzmetriken
- Resource Scheduling in Kubernetes: Effizienz und Kostenkontrolle
- Serverless Computing: Performance-Modelle und Cold-Start-Optimierung
- Observability in Microservices: Tracing, Logging und Root Cause Analysis
- Consensus-Protokolle: Optimierung und formale Verifikation
- Edge Computing: Latenzoptimierung und verteilte Inferenz
- Datenreplikation und Konsistenz in Multi-Cloud-Setups
- Energy-aware Computing: effiziente Rechenzentren und Green Cloud
- Performance Engineering für Hochlast-Systeme

Netzwerke & Kommunikation

- Traffic Engineering in Software-Defined Networks (SDN)
- Optimierung von Routing-Protokollen für dynamische Netze
- Netzwerk-Telemetrie: automatische Erkennung von Engpässen
- Sicherheit in 5G/6G-Netzen: Angriffsszenarien und Gegenmaßnahmen
- QoS-Modelle für Echtzeit-Übertragung und Video-Streaming
- Netzwerk-Simulationen und Validierung realer Messdaten
- Congestion Control: neue Verfahren für moderne Transportprotokolle
- Peer-to-Peer-Systeme: Robustheit, Skalierbarkeit und Anreizmodelle
- IoT-Kommunikation: Low-Power-Protokolle und Zuverlässigkeit
- Monitoring großer Netzwerke mit ML

Datenbanken & Information Retrieval

- Query Optimization in hybriden OLTP/OLAP-Systemen
- Vektor-Datenbanken und Retrieval für LLM-Anwendungen
- Konsistenz und Transaktionen in verteilten DB-Systemen
- Datenintegration: semantische Harmonisierung heterogener Quellen

- Suchsysteme: Ranking-Modelle und Evaluationsmethoden
- Wissensgraphen: Aufbau, Qualitätssicherung und Reasoning
- Datenschutz in Datenbanken: Zugriffskontrolle und Auditing
- Indexstrukturen für hochdimensionale Daten
- Recommender Systems: Bias, Fairness und Robustheit
- Benchmarking: realistische Workloads und Reproduzierbarkeit

Human-Computer Interaction (HCI) & UX

- Messung von Nutzerverhalten in komplexen Interfaces
- Barrierefreiheit in Web- und Mobile-Anwendungen: automatische Checks
- Explainable Interfaces: Vertrauen in KI-basierte Systeme
- User Studies: Methodik, Bias und statistische Auswertung
- Interaktionsdesign für AR/VR-Anwendungen
- Privacy UX: Wie Nutzer Datenschutz-Entscheidungen treffen
- Dark Patterns: Erkennung und Gegenmaßnahmen
- Multimodale Eingabe: Sprache, Gesten, Eye-Tracking
- Produktivitätstools: Design für kognitive Entlastung
- Usability in sicherheitskritischen Systemen

Theoretische Informatik & Algorithmen

- Untere Schranken in der Komplexitätstheorie für spezielle Problemklassen
- Approximationsalgorithmen für NP-schwere Optimierungsprobleme
- Randomisierte Algorithmen und Derandomisierungstechniken
- Parameterisierte Komplexität: Kernisierung und FPT-Algorithmen
- Graphalgorithmen für große Netze: Treewidth, Planarität und Decomposition
- Online-Algorithmen mit kompetitiven Garantien
- Streaming-Modelle: Speichergrenzen und Genauigkeit

- Algorithmische Spieltheorie: Mechanism Design mit Effizienzgarantien
- Beweisgestützte Verifikation von Algorithmen
- Codierungstheorie: neue Konstruktionen und Decoding-Methoden

Embedded Systems, IoT & Robotics

- Echtzeitfähige ML-Inferenz auf Edge-Geräten
- Energieeffiziente Algorithmen für Embedded Hardware
- Sicherheit von Firmware und Update-Prozessen
- Sensorfusion und robuste Navigation in Robotik
- Swarm Robotics: Koordination und Stabilitätsgarantien
- Digitale Zwillinge für industrielle IoT-Systeme
- Fehlerdiagnose in cyber-physischen Systemen
- Scheduling in real-time Systems unter Constraints
- Autonome Systeme: sichere Entscheidungslogik
- Edge-to-Cloud-Architekturen und Latenzoptimierung

Quanteninformatik

- Quantenalgorithmen: Ressourcenkomplexität und Vergleich zu klassischen Verfahren
- Fehlerkorrektur und Stabilität in Quanten-Schaltungen
- Post-Quantum-Kryptographie und Übergangsstrategien
- Quanten-Maschinelles Lernen: Nutzen und Grenzen
- Simulation physikalischer Systeme auf Quantenhardware
- Optimierung von Quantum Circuits für NISQ-Geräte
- Benchmarking und Evaluationsmetriken für Quantencomputer
- Hybrid Quantum-Classical Workflows
- Verifikation quantenbasierter Berechnungen
- Quantennetzwerke: Kommunikation und Protokolle