Friedrich-Alexander-Universität
Technische Fakultät

FAU

Cryptography

Overview of our teaching offer

Prof. Dr. Dominique Schröder

Overview

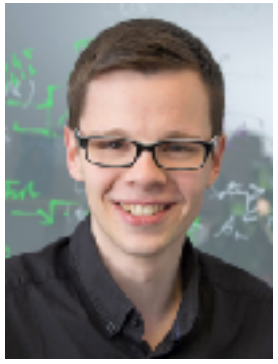
We the people

Professor
Dominique Schröder

Assistant Professor
Paul Rösler

Professors' Assistant
Yasmin Kleindienst-Heger

Technical Staff
Carina Köhler



Postdoc
Dominic Deuber

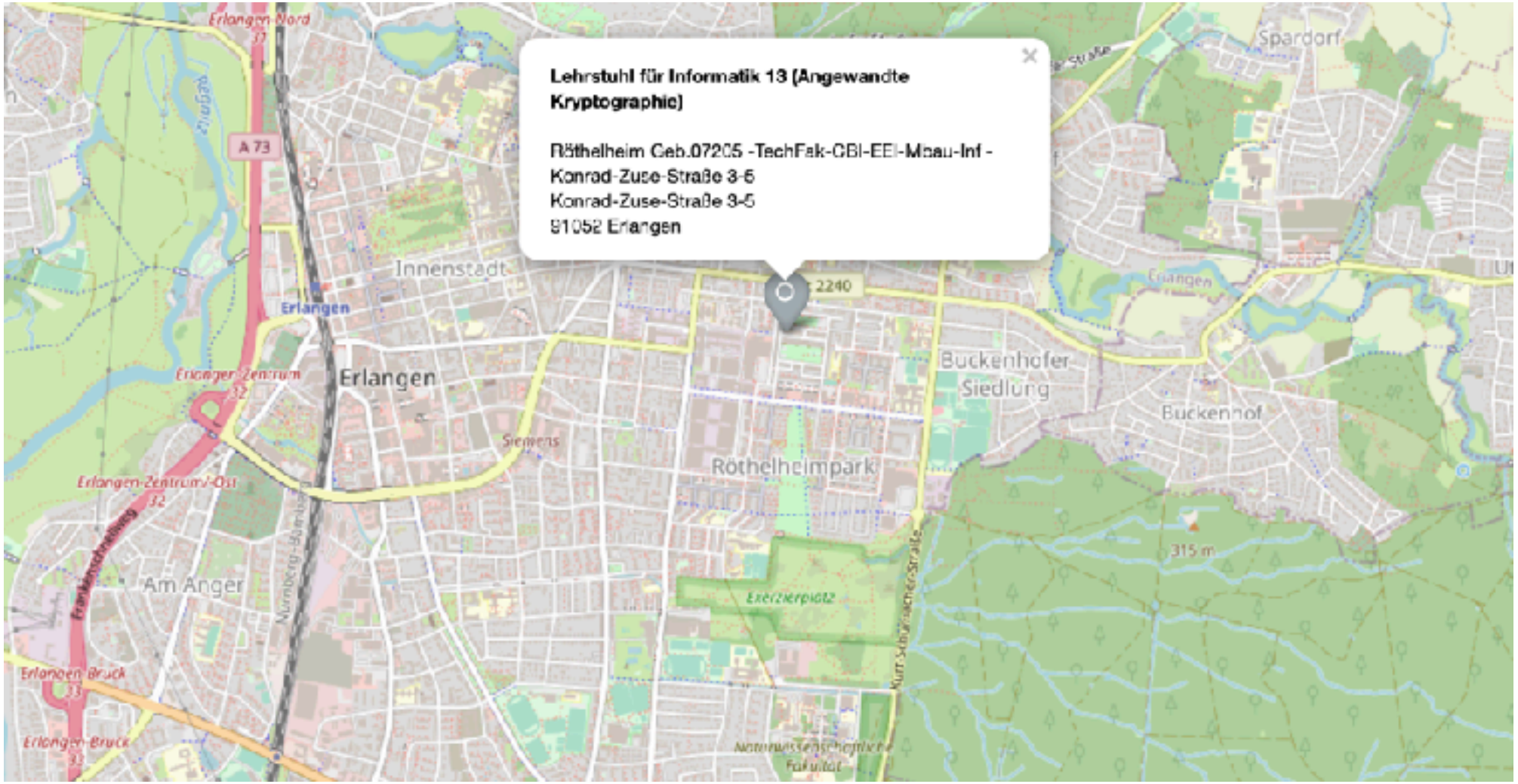
Scientific Staff (PhD)
Hien Chu

Scientific Staff (PhD)
Paul Gerhart

Scientific Staff (PhD)
Julian Kotzur

Overview

Where to find us



Overview

Where to find us

Overview

Offerings in the summer semester

Type / Branch	Summer Term	ECTS
Basic class	Introduction to Algorithms	7.5
Cryptocurrencies	Cryptocurrencies 1	5
Privacy	Data Privacy 1	5
Protocols	Cryptographic Communication Protocols	5
Seminar	Selected Topics	5
Project	Privacy and Crypto	10

All our courses are open to undergraduate students as well as master students

Overview

Offerings in the winter semester

Type / Branch	Winter Term	ECTS
Basic class	Introduction to Modern Cryptography	7.5
Cryptocurrencies	Cryptocurrencies 2	5
Privacy	Data Privacy 2	5
Seminar	Selected Topics	5
Project	Privacy and Crypto	10

All our courses are open to undergraduate students as well as master students

Friedrich-Alexander-Universität
Technische Fakultät

Einführung in die Algorithmik

Prof. Dr. Dominique Schröder

General:

- Vorlesung wird in deutscher Sprache gehalten
- 7,5 ECTS (5 ECTS VL, 2.5 ECTS Ue)
- Keine Voraussetzungen
- Voraussichtlich mit schriftlicher Klausur

Grundlagen:

- Python / Pseudocode
- Laufzeitanalyse
- Korrektheitsanalyse

Sortieren:

- Selectionsort, Bubblesort, ...
-Quicksort, Mergesort, ...
- Nicht Vergleichsbasierte Verfahren

Graphen:

- Einführung
- Kürzeste Wege
- Minimale Spannbäume
- Flussprobleme
- PageRank

Bäume:

- Binärbäume
-Suchbäume
- B+ Bäume
- Bruder Bäume
- AVL Bäume

Friedrich-Alexander-Universität
Technische Fakultät

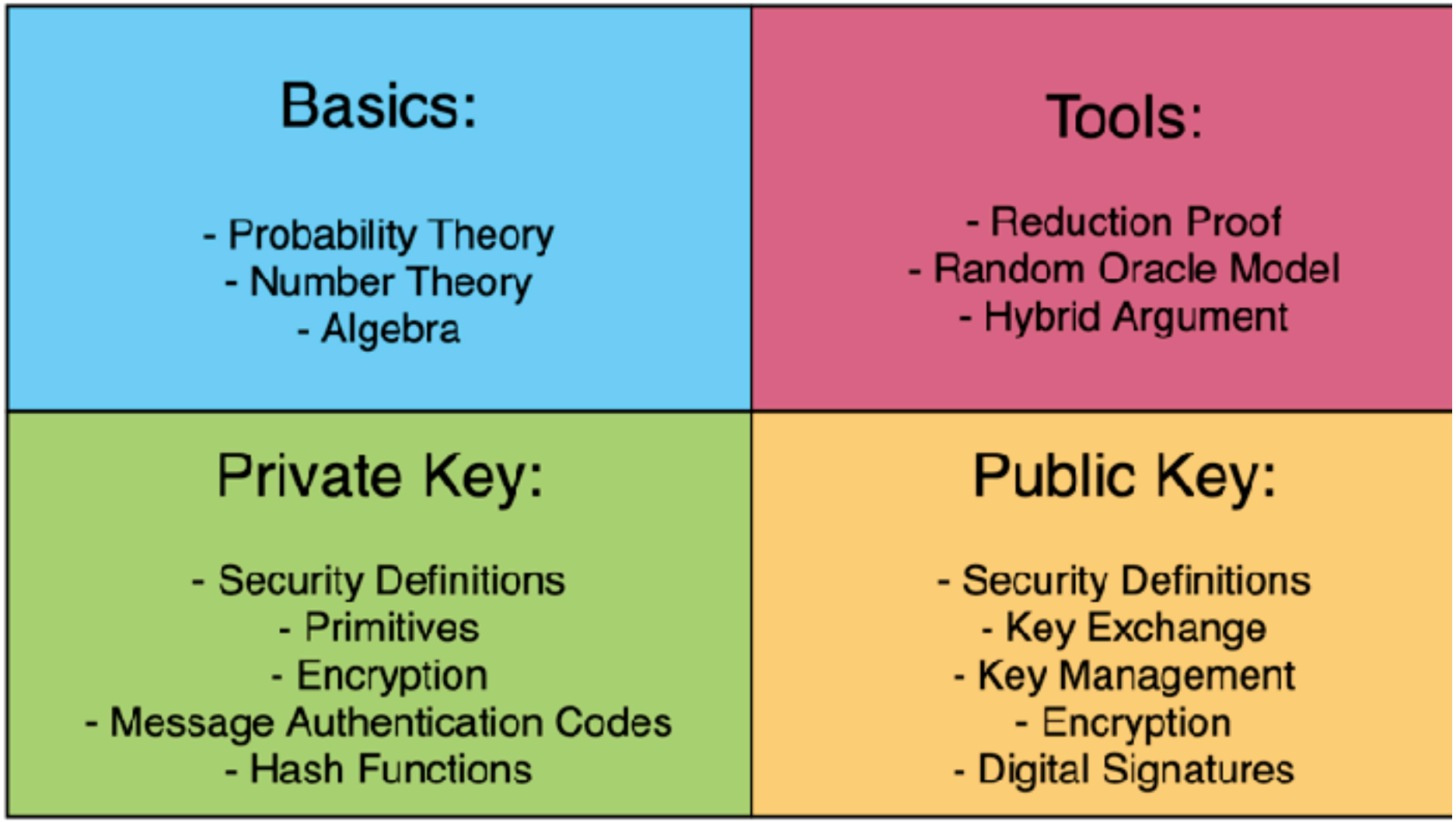
FAU

Introduction to Modern Cryptography

Prof. Dr. Dominique Schröder

General:

- Lecture is held in English
- 7.5 ECTS
- Recommended requirements: Basic knowledge in math, probability theory and computer science may be helpful.
- Probably a written exam


Basics:
- Probability Theory
- Number Theory
- Algebra
Tools:
- Reduction Proof
- Random Oracle Model
- Hybrid Argument
Private Key:
- Security Definitions
- Primitives
- Encryption
- Message Authentication Codes
- Hash Functions
Public Key:
- Security Definitions
- Key Exchange
- Key Management
- Encryption
- Digital Signatures

Friedrich-Alexander-Universität
Technische Fakultät

FAU

Cryptocurrencies

Prof. Dr. Dominique Schröder

General:

- Lecture is held in English
- 5 ECTS
- Recommended requirements: Basic knowledge in math, probability theory, cryptography, and computer security is assumed. Introduction to cryptography would be ideal.
- Probably a written exam

First Part:

- Cryptocurrencies and Bitcoin: Cryptocurrencies are digital currencies, with Bitcoin being the most well-known, based on blockchain technology.
- The Bitcoin Backbone Protocol: The blockchain is the decentralized database that contains all Bitcoin transactions and is validated through mining.
- Applications and Limitations of Bitcoin: Bitcoin can be used as a global payment system, but it has limited scalability and longer transaction times.
- Payment Channels and Anonymity: Payment channels improve scalability and reduce transaction costs. Bitcoin is pseudonymous, but techniques like CoinJoin enhance anonymity.

Second Part:

- Proof-Systems: Enable transaction verification without revealing details.
- Privacy-focused cryptocurrencies: Focus on preserving users' privacy.
- Confidential transactions: Obscure transaction amounts to enhance financial privacy.
- Monero: Leading privacy-oriented cryptocurrency with Ring Signatures and Stealth Addresses.
- Zcash: Utilizes Zerocoin and zk-SNARKs to obscure transactions and allows selective transparency.

Friedrich-Alexander-Universität
Technische Fakultät

FAU

Data Privacy

Prof. Dr. Dominique Schröder

General:

- Lecture is held in English
- 5 ECTS
- Recommended requirements: Basic knowledge in math, probability theory, cryptography, and computer security is assumed. Introduction to cryptography would be ideal.
- Probably a written exam

First Part:

- Private Data Access: Control and protection of access to private data.
- Reconstruction Attacks: Attempts to reconstruct private information from publicly accessible data.
- Private-Information Retrieval: Techniques to retrieve data from a database without the server knowing the specific information being requested.
- Oblivious RAM: Memory type that keeps access patterns to data secret.
- Oblivious Group ORAM: Advanced version of Oblivious RAM, allowing simultaneous covert access by multiple users to shared storage.

Second Part:

- Basic anonymization techniques: K-Anonymity, K-Diversity, and L-Diversity protect data privacy but have some limitations.
- Differential Privacy: Minimizes the impact of individual data points on statistical results and can be securely applied to machine learning.
- Alternative approach - Homomorphic Encryption: Enables processing and analysis of encrypted data without decryption, providing high data privacy.

Friedrich-Alexander-Universität
Technische Fakultät

FAU

Cryptographic Communication Protocols

Prof. Dr.-Ing. Paul Rösler

General:

- 5 ECTS
- Recommended requirements: Basic knowledge in math, probability theory, cryptography, and computer security is assumed. Introduction to cryptography would be ideal.

Cryptographic Communication Protocols

Topics:

- Standard Tools: Public Key Encryption, Non-Interactive Key Exchange, Key Encapsulation Mechanism
- Defining Security and Modeling Real-World Attackers against Messaging Protocols
- Authenticated Key Exchange (e.g., TLS, Noise, X3DH)
- Secure Communication Channels
- Two-Party Messaging Protocols: From Theory to WhatsApp (e.g., Double Ratchet Algorithm)
- Key-Update Mechanisms
- Group Messaging Protocols: From Theory to Standardized Practice (e.g., MLS Standard)

Friedrich-Alexander-Universität
Technische Fakultät

FAU

Seminar: Cryptography in Secure Messaging

Prof. Dr.-Ing. Paul Rösler

General:

- Seminar is held in English
- 5 ECTS
- Recommended requirements: Basic knowledge in math, probability theory, cryptography, and computer security is assumed. Introduction to cryptography would be ideal.

Structure:

- Seminar purpose: Obtain an overview of modern messaging protocols used in applications like WhatsApp and Signal, with a focus on Signal's Double-Ratchet protocol and related enhancements.
- Presentation format: Each participant presents one scientific publication, explaining its core ideas and direct relations to an earlier publication.
- Summary requirement: Students must submit a 4-page summary, including core ideas of their chosen publication and its relation to another student's presentation.
- Evaluation and collaboration: Students' presentations and discussions will be evaluated based on clarity and engagement, encouraging collaboration and knowledge sharing among participants.

Friedrich-Alexander-Universität
Technische Fakultät

FAU

Seminars and Projects

Prof. Dr. Dominique Schröder

Offered seminars and projects:

- These modules provide insights into current research.
- Therefore, there are different seminars and projects offered every semester.
- Information about the current seminars can be found on the Campo portal or on the department's website.
- Especially projects can be highly individual, so please write us an email with your skills and interests!