Alexander Kulpe

Mathematician & Engineer for IT-Security
Born: 1999-08-02 in Wolfenbüttel, Germany | firstname.lastname(at)ruhr-uni-bochum.de
last updated: June 2024

Education

Ruhr-University Bochum

PhD in Quantum Information and Cryptography — 2024 – present

M.Sc. IT-Security / Information Technology (Grade: excellent (99 %)) — 2022 – 2024

- Valedictorian
- Thesis: Time-Memory Tradeoffs for Subset Sum and Decoding (Grade: excellent (99 %))
- Advisors: Prof. Dr. Alexander May, Dr. André Esser (TII Abu Dhabi)

M.Sc. Mathematics (Grade: excellent (0.7)) — 2022 – present

- Thesis: Time-Memory Tradeoffs for Subset Sum and Decoding (Grade: very good (0.7))
- Advisors: Prof. Dr. Alexander May, Dr. André Esser (TII Abu Dhabi)

B.Sc. IT-Security / Information Technology (Grade: very good (91 %)) — 2018 – 2022

- Thesis: Cryptanalysis of McEliece (Grade: excellent (95 %))
- Advisors: Prof. Dr. Alexander May, Timo Glaser

B.Sc. Mathematics (Grade: very good (1.4)) — 2018 – 2022

- Thesis: Cryptanalysis of McEliece (Grade: very good (1.0))
- Advisors: Prof. Dr. Alexander May, Timo Glaser

Priv. Martin-Butzer-Gymnasium Dierdorf

Abitur (A-Levels) (Grade: very good (1.3)) — 2010 – 2018

Experience

PhD Student — 2024 – present

Quantum Information, Ruhr-University Bochum

CASA: Cybersecurity in the Age of Large-Scale Adversaries

- Advisors: Prof. Dr. Michael Walter, Asst. Prof. Dr. Giulio Malavolta
- working on the DFG-funded CASA Fundamental Research Project "Robust Certification of Quantum Devices"

Teaching Assistant — 2019 – 2024

Ruhr-University Bochum

- Algorithm Paradigms, Cryptography, Discrete Mathematics I, Discrete Mathematics II / Introduction to Theoretical Computer Science, Higher Mathematics I, Mathematics I for Computer Science and IT-Security, Public Key Cryptanalysis

Internship — 2021

secunet Security Networks AG

Division Homeland Security, Team Cryptographic Systems and Applications

- Analysis of general concepts in the field of Post-Quantum Cryptography
- Analysis and technical preparation of the consequences of Post-Quantum Cryptography on TLS
- Presentation of the work results in a webinar

Awards & Scholarships

Valedictorian IT-Security — 2024

500 € sponsored by Edgeless Systems

Deutschlandstipendium (Germany Scholarship) — 2018 – 2024

≈ 20,000 € (300 € per month)

sponsored by Horst Görtz Foundation — 2019 – 2024

sponsored by Dr. Hans-Paul Bürkner — 2018 – 2019

DPG-Abiturprize (German Physical Society Award) — 2018

for very good performances in Physics

DPG-Bookprize (German Physical Society Award) — 2018

for excellent performances in Physics

Talks

(Classical) Time-Memory Tradeoffs for Subset Sum and Decoding
@ QI Colloquium, Ruhr-University Bochum 2024
@ Master Thesis Defence, Ruhr-University Bochum & TII Abu Dhabi 2024

Chebychev Polynomials
@ Selected Chapters of Analysis Seminar, Ruhr-University Bochum 2019

Conditional lower bounds based on SAT
@ Satisfiabilty Seminar, Ruhr-University Bochum 2023

Consequences of Post-Quantum Cryptography on TLS
@ secunet Security Networks AG 2021

Cryptanalysis of McEliece
@ Bachelor Thesis Defence, Ruhr-University Bochum 2022

Overview of Mahadev's protocol for verification of quantum computations
@ Ruhr-University Bochum & Max Planck Institute for Security & Privacy 2023

McTiny: Fast High-Confidence Post-Quantum Key Erasure for Tiny Network Server
@ Real-World Cryptography Seminar, Ruhr-University Bochum 2020

Universality and Solovay-Kitaev Theorem
@ Quantum Algorithms Seminar, Ruhr-University Bochum & University of Cologne 2023

Academic Referees

Asst. Prof. Dr. Giulio Malavolta
Assistant Professor (tenure track) at Bocconi University
Department of Computing Sciences

Prof. Dr. Alexander May
Professor / Head of Chair at Ruhr-University Bochum
Chair for Cryptanalysis
Faculty of Computer Science

Prof. Dr. Michael Walter
Professor / Head of Chair at Ruhr-University Bochum
Chair for Quantum Information
Faculty of Computer Science

Social Engagement

Board Member & Treasurer 2019 – 2023
Student Home Council Studentenhaus Laerholzstraße e.V. Bochum

Umpire 2014 – 2019
Table-Tennis Federation Rhineland (TTVR) Germany

Skills

Expertise: Cryptography, Cryptanalysis, Theoretical Computer Science, Quantum Information
Language: German (native language), English (good), Latin Proficiency Certificate
Programming: ARM Assembly, C, Python, Sage

Selected Coursework (click here for more information)

Cryptography: ARM Processors for Embedded Cryptography, Authentic Key Agreement: Formal Models and Applications, Boolean Functions with Applications in Cryptography, Cryptographic Protocols, Cryptography, Cryptography on Hardware-based Platforms, Human Aspects of Cryptography Adoption and Use, Implementation of Cryptographic Schemes, Introduction to Asymmetric Cryptanalysis, Introduction to Cryptography I & II, Introduction to Usable Security & Privacy, Practical Cryptanalysis of Symmetric Ciphers, Public Key Encryption, Quantum Cryptography, Real World Cryptography Seminar, Software Implementation of Cryptographic Schemes, Symmetric Cryptanalysis, Zero-Knowledge Proof Systems

Mathematics: Algebra, Analysis I - IV, Discrete Mathematics I & II, Linear Algebra & Geometry I & II, Ordinary Differential Equations, Selected Chapters of Analysis Seminar
Quantum: Advanced Quantum Information and Computation, Quantum Algorithms Seminar, Quantum Circuits, Quantum Cryptography, Quantum Information & Computation
Theoretical Computer Science: Computational Complexity Theory, Information Theory, Introduction to Theoretical Computer Science, Satisfiability Seminar, Theoretical Computer Science

Miscellaneous

Hobbies: Table Tennis, Cinema