Dominique Schröder

Professor of Privacy-Enhancing Technologies at TU Wien
dominique.schroeder@tuwien.ac.at

Academic appointments

Technische Universität Wien, Vienna, Austria — 2024-present
Full Professor (Univ. Prof. with tenure)

Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany — 2016-2024
Full Professor (W3, with tenure)

Saarland University, Germany — 08/2015-06/2016
Professor (W2, with tenure)

Saarland University, Germany — 08/2012-07/2015
Assistant Professor (W1, tenure-track)

University of Maryland, United States of America — 02/2011-06/2012
Postdoctoral Researcher under Jonathan Katz

Technical University of Darmstadt, Germany — 10/2006-01/2011
Doctoral Student under Marc Fischlin

Education

Technical University Darmstadt — 10/2006-11/2010
Dr. rer. nat. (with distinction) · Cryptography

Technical University Braunschweig — 10/2002-09/2006
Diplom Informatiker. (Diploma/M.Sc.) · Computer Science · Identification Schemes

Research interests

How can we compute on private data and share control of digital systems without trusting a single party?

I design cryptographic protocols that distribute trust and protect sensitive information. My research asks how their security guarantees hold up when participants are compromised or protocols become part of larger systems.

Honors and awards

Feodor Lynen Award — 2021
Humboldt Foundation

Efficient Unlinkable Sanitizable Signatures from Signatures with Re-Randomizable Keys — 2017
Distinguished Paper · Invited from PKC 2016 to IET IFS Special Issue

Delegtable Functional Signatures — 2017
Distinguished Paper · Invited from PKC 2016 to IET IFS Special Issue

(Efficient) Universally Composable Oblivious Transfer Using a Minimal Number of Stateless Tokens — 2014
Distinguished Paper · Invited from TCC 2014 to Journal of Cryptology

Intel Early Career Faculty Award — 2013
Intel · Awarded to 6 people in Europe ($35,000)

Postdoctoral Fellowship — 2013
Deutscher Akademischer Austausch Dienst (DAAD) · University of Maryland

Dissertation — 2012
TU Darmstadt · summa cum laude (with highest honors)

Research Fellow — 2010
Deutscher Akademischer Austausch Dienst (DAAD) · Research visit at the University of Maryland

Best Teaching Assistant Award — 2007
TU Darmstadt · Lecture Introduction to Modern Cryptography

Programming Contest N@tkids — 2000
Winner of the programming contest "N@tkids" · akte 2000 and ricardo.de in the third category (5000 DM). Invited to the TV show akte 2000.

Research visits

Visiting Professor · University of Maryland, USA — 07/2023-09/2023
Host: Prof. Katz

Visiting Professor · University of Berkeley, USA — 08/2016
Host: Prof. Garg

Visiting Professor · Chinese University of Hong Kong, Hong Kong — 03/2016
Host: Prof. Chow

Visiting Professor · University of Maryland, USA — 07/2015-08/2015
Host: Prof. Katz

Visiting Professor · University of Maryland, USA — 08/2013-10/2013
Host: Prof. Katz

Research Internship · University of Maryland, USA — 07/2010-10/2010
Host: Prof. Katz

Research funding and projects

Unrestricted Gift — 10/2026-12/2028
Google · sole PI · 120.000 EUR

Foundations and Applications of Resource-Restricted Cryptography — 01/2026-12/2029
WWTF · PI · 299.708 EUR

Confidential 6G — 01/2023-12/2026
EU Horizon · PI · 282.500 EUR

Post-quantum Secure Key-Exchange — 04/2022-03/2023
AUDI · Research Contract · 100.000 EUR

Password-based Cryptography — 04/2021-03/2023
DFG · sole PI · 327.000 EUR

NCT: Privacy Enhancing Technologie
State of Bavaria · PI · 351.000 EUR
10/2021-09/2025

Privacy-Preserving Blockchains
Protocol Labs · PI · 23.000 EUR
10/2023-09/2024

Postquantum Security for Automobiles
AUDI · Research Contract · 60.000 EUR
01/2021-12/2021

Cybercrime and Forensic Computing
DFG Integrated Research Training Group · PI · 645.000 EUR
08/2019-07/2028

PROMISE - Personal Medial Safe
BMBF · Leading PI · 710.000 EUR
01/2016-12/2019

Password-based Cryptography
DAAD · PI · 14.000 EUR
01/2018-12/2019

Methods and Tools for Understanding Privacy
DFG - Collaborative Research Center (SFB) · PI · 325.000 EUR
01/2016-12/2019

CISPA Center for IT-Security, Privacy, and Accountability
BMBF · PI · 690.000 EUR
01/2013-04/2018

Cryptographic Protocols for Cloud Storage
DAAD · sole PI · 12.000 EUR
01/2015-12/2016

Cryptography for Secure Digital Interaction
EU COST · PI · 135.000 EUR
11/2013-04/2018

Usable Security for Mobile Devices
BMBF · PI · 100.000 EUR
01/2014-12/2014

TWC Small: Exploring Cryptographic Models
NSF · PI, but I left to Germany · 314.000 EUR
09/2012-08/2015

Publications

BitPriv: A Privacy-Preserving Protocol for DeFi Applications on Bitcoin
Ioannis Alexopoulos, Zeta Avarikioti, Paul Gerhart, Matteo Maffei, and **Dominique Schröder**
NDSS 2027

Fully Adaptive FROST with Identifiable Aborts from AOMDL
Ruben Baecker, Paul Gerhart, Davide Li Calsi, Luigi Russo, **Dominique Schröder**, and Arkady Yerukhimovich
ASIACRYPT 2026

Fair Distributed Exchange via Threshold Adaptor Signatures
Ruben Baecker, Paul Gerhart, Jonathan Katz, and **Dominique Schröder**
ASIACRYPT 2026

Universally Composable Adaptor Signatures
Paul Gerhart, Daniel Rausch, and **Dominique Schröder**
ACM CCS 2026

Fully-Adaptive Two-Round Threshold Schnorr Signatures from DDH
Paul Gerhart, Davide Li Calsi, Luigi Russo, and **Dominique Schröder**
EUROCRYPT 2026

Password-Hardened Encryption Revisited
Ruben Baecker, Paul Gerhart, and **Dominique Schröder**
ASIACRYPT 2025

Universally Composable and Round-Optimal Password-Hardened Encryption
Behzad Abdolmaleki, Ruben Baecker, Paul Gerhart, Mike Graf, Mojtaba Khalili, Daniel Rausch, Fritz Schmidt, and **Dominique Schröder**
ASIACRYPT 2025

A Fully-Adaptive Threshold Partially-Oblivious PRF
Ruben Baecker, Paul Gerhart, Daniel Rausch, **Dominique Schröder**
CRYPTO 2025

Increasing the Resilience of Secure Multiparty Computation using Security Modules
Lamaya Omar, Felix Freiling, **Dominique Schröder**
Transactions on Dependable and Secure Computing 2025

Automated Analysis and Synthesis of Message Authentication Codes
Stefan Milius, Dominik Paulus, Julian Thomas, **Dominique Schröder**, and Lutz Schröder
CSF 2025

SoK: Descriptive Statistics Under Local Differential Privacy
René Raab, Pascal Berrang, Paul Gerhart, and **Dominique Schröder**
PETS 2025

Measuring Conditional Anonymity - A Global Study
Pascal Berrand, Paul Gerhart, and **Dominique Schröder**
PETS 2024

Foundations of Adaptor Signatures
Paul Gerhart, **Dominique Schröder**, Pratik Soni, and Sri A. K. Thyagarajan
EUROCRYPT 2024

Practical Schnorr Threshold Signatures without the Algebraic Group Model
Hien Chu, Paul Gerhart, Tim Ruffing, **Dominique Schröder**
CRYPTO 2023

ROAST: Robust Asynchronous Schnorr Threshold Signatures
Tim Ruffing, Viktoria Ronge, Elliott Jin, Jonas Schneider-Bensch, and **Dominique Schröder**
ACM CCS 2022

Verifiable Timed Linkable Ring Signatures For Scalable Payments for Monero
Sri A. K. Thyagarajan, Giulio Malavolta, Fritz Schmidt, **Dominique Schröder**
ESORICS 2022

Inner Product Functional Commitments with Constant-Size Public Parameters and Openings
Hien Chu, Dario Fiore, Dimitris Kolonelos, and **Dominique Schröder**
SCN 2022

Everlasting UC Commitments from Fully Malicious PUFs
Bernardo Magri, Giulio Malavolta, **Dominique Schröder**, and Dominique Unruh
Journal of Cryptology 2022

A Security Framework for Distributed Ledgers
Mike Graf, Daniel Rausch, Viktoria Ronge, Christoph Egger, Ralf Küsters, and **Dominique Schröder**
ACM CCS 2021

OpenSquare: Decentralized Repeated Modular Squaring Service
Sri A. K. Thyagarajan, Adithya Bhat, Tiantian Gong, Aniket Kate, and **Dominique Schröder**.
ACM CCS 2021

CoinJoin in the Wild - An Empirical Analysis in Dash
Dominic Deuber and **Dominique Schröder**
ESORICS
2021

Foundations of Ring Sampling
Viktoria Ronge, Christoph Egger, Russell W. F. Lai, **Dominique Schröder**, Hoover H. F. Yin
PETS
2021

Controlling My Genome With My Smartphone a First Clinical Experiences Of The PROMISE-System
Ali Amr, Marc Hinderer, Lena Griebel, Dominic Deuber, Christoph Egger, Farbod Sedaghat-Hamedani, Elham Kayvanpour, Daniel Huhn, Jan Haas, Karen Frese, Marc Schweig, Ninja Marnau, Annika Krämer, Claudia Durand, Florian Battke, Hans-Ulrich Prokosch, Michael Backes, Andreas Keller, **Dominique Schröder**, Hugo A. Katus, Norbert Frey, Benjamin Meder
Clinical Research in Cardiology
2021

Threshold Password-Hardened Encryption Services
Julian Brost, Christoph Egger, Russell W. F. Lai, Fritz Schmid, **Dominique Schröder**, and Markus Zoppelt
pp. 409-424
ACM CCS
2020

Verifiable Timed Signatures Made Practical
Sri A. K. Thyagarajan, Adithya Bhat, Giulio Malavolta, Nico Döttling, Aniket Kate, and **Dominique Schröder**
pp. 1733-1750
ACM CCS
2020

The Patient as Genomic Data Manager - Evaluation of the PROMISE App.
Lena Griebel, Marc Hinderer, Ali Amr, Benjamin Meder, Marc Schweig, Dominic Deuber, Christoph Egger, Claudia Kawohl, Annika Krämer, Isabell Flade, **Dominique Schröder**, Hans-Ulrich Prokosch
pp. 1061-1065
MIE
2020

Feasibility and Infeasibility of Secure Computation with Malicious PUFs
Dana Dachman-Soled, Nils Fleischhacker, Jonathan Katz, Anna Lysyanskaya, and **Dominique Schröder**
pp. 595-617
Journal of Cryptology
2020

Omniring: Scaling Up Private Payments Without Trusted Setup - Formal Foundations and Constructions of Ring Confidential Transactions with Log-size Proofs
Russell W. F. Lai, Viktoria Ronge, Tim Ruffing, **Dominique Schröder**, Sri A. K. Thyagarajan, and J.Wang
pp. 31-48
ACM CCS
2019

Efficient Invisible and Unlinkable Sanitizable Signatures
Xavier Bultel, Pascal Lafourcade, Rusell W.F. Lai, Giulio Malavolta, **Dominique Schröder**, and Sri A. K. Thyagarajan
pp. 159-189
PKC
2019

My Genome Belongs to Me: Controlling Third Party Computation on Genomic Data
Dominic Deuber, Christoph Egger, Katharina Fech, Giulio Malavolta, Sri A. K. Thyagarajan, Florian Battke, Claudia Durand, and **Dominique Schröder**
pp. 108-132
PETS
2019

Tight Security Proofs for Schnorr Signatures
Nils Fleischhacker, Tibor Jager, and **Dominique Schröder**
pp. 566-599
Journal of Cryptology
2019

(Efficient) Universally Composable Oblivious Transfer Using a Minimal Number of Stateless Tokens
Seung Geol Choi, Jonathan Katz, **Dominique Schröder**, Arkady Yerukhimovich, Hong-Sheng Zhou
pp. 459-497
Journal of Cryptology
2019

Group ORAM for privacy and access control in outsourced personal records
Matteo Maffei, Giulio Malavolta, Manuel Reinert, **Dominique Schröder**
pp. 1-47
Journal of Computer Security
2019

Homomorphic Secret Sharing for Low Degree Polynomials
Russell W. F. Lai, Giulio Malavolta, and **Dominique Schröder**
pp. 279-309
ASIACRYPT
2018

Simple Password-Hardened Encryption Services
Russell W. F. Lai, Christoph Egger, Manuel Reinert, Sherman S. M. Chow, Matteo Maffei, and **Dominique Schröder**
pp. 1405-1421
USENIX
2018

Functional Credentials
Dominic Deuber, Matteo Maffei, Giulio Malavolta, Max Rabkin, **Dominique Schröder**, Mark Simkin.
pp. 64-84
PETS
2018

Burning Zerocoins for Fun and for Profit: A Cryptographic Denial-of-Spending Attack on the Zerocoin Protocol
Tim Ruffing, Sri A. K. Thyagarajan, Viktoria Ronge, **Dominique Schröder**
pp. 116-119
Crypto Valley Conference on Blockchain Technology
2018

Subset Predicate Encryption and Its Applications
Jonathan Katz, Matteo Maffei, Giulio Malavolta, and **Dominique Schröder**
CANS
2017

On the Security of Frequency-Hiding Order-Preserving Encryption
Matteo Maffei, Manuel Reinert, and **Dominique Schröder**
pp. 115-134
CANS
2017

Efficient Ring Signatures in the Standard Model
Giulio Malavolta and **Dominique Schröder**
pp. 128-157
ASIACRYPT
2017

Phoenix: Rebirth of a Cryptographic Password-Hardening Service
Russell W.F.Lai, Christoph Egger, **Dominique Schröder**, and Sherman S.M.Chow
pp. 899-916
USENIX
2017

Maliciously Secure Multi-Client ORAM
Matteo Maffei, Giulio Malavolta, Manuel Reinert, and **Dominique Schröder**
pp. 645-664
ACNS
2017

Security of Blind Signatures Revisited
Dominique Schröder and Dominique Unruh
pp. 470-494
Journal of Cryptology
2017

Efficient Cryptographic Password Hardening Services From Partially Oblivious Commitments
Jonas Schneider, Nils Fleischhacker, **Dominique Schröder**, and Michael Backes
pp. 1192-1203
ACM CCS
2016

Efficient Sanitizable Signatures without Random Oracles
Russell W. F. Lai, Tao Zhang, ShermanChow and **Dominique Schröder**
pp. 363-380
ESORICS
2016

Two Message Oblivious Evaluation of Cryptographic Functionalities
Nico Doettling, Nils Fleischhacker, Johannes Krupp, and **Dominique Schröder**
pp. 619-648
CRYPTO
2016

Delegtable Functional Signatures
Michael Backes, Sebastian Meiser, and **Dominique Schröder**
pp. 357-386
PKC
2016

Efficient Unlinkable Sanitizable Signatures from Signatures with Re-Randomizable Keys
Nils Fleischhacker, Johannes Krupp, Giulio Malavolta, Jonas Schneider, **Dominique Schröder**, and Mark Simkin
pp. 301-330
PKC
2016

Nearly Optimal Verifiable Data Streaming
Johannes Krupp, **Dominique Schröder**, Mark Simkin, Dario Fiore, Giuseppe Ateniese, and Stefan Nuernberger
pp. 417-445
PKC
2016

Efficient Unlinkable Sanitizable Signatures from Signatures with Re-Randomizable Keys
Nils Fleischhacker, Giulio Malavolta, **Dominique Schröder**, and Mark Simkin
pp. 166-183
IET IFS Special Issue
2016

Delegtable Functional Signatures
Sebastian Meiser and **Dominique Schröder**.
pp. 194-206
IET IFS Special Issue
2016

Efficient Pseudorandom Functions via On-the-Fly Adaptation
Nico Döttling and **Dominique Schröder**
pp. 329-350
CRYPTO
2015

Privacy and Access Control for Outsourced Personal Records
Matteo Maffei, Giulio Malavolta, Manuel Reinert, and **Dominique Schröder**
pp. 341-358
IEEE Symposium on Security and Privacy
2015

Liar, Liar, Coins on Fire! Penalizing Equivocation By Loss of Bitcoins
Tim Ruffing, Aniket Kate, and **Dominique Schröder**
pp. 219-230
ACM CCS
2015

Verifiably Encrypted Signatures: Security Revisited and a New Construction — ESORICS 2015
Christian Hanser, Max Rabkin, and **Dominique Schröder**

VeriStream - A Framework for Verifiable Data Streaming — FC 2015
Dominique Schröder and Mark Simkin
pp. 146-164

Foundations of Reconfigurable PUFs — ACNS 2015
Jonas Schneider and **Dominique Schröder**
pp. 579-594

Feasibility and Infeasibility of Secure Computation with Malicious PUFs — CRYPTO 2014
Dana Dachman-Soled, Nils Fleischhacker, Jonathan Katz, Anna Lysyanskaya, and **Dominique Schröder**
pp. 405-420

Tight Security Proofs for Schnorr Signatures — ASIACRYPT 2014
Nils Fleischhacker, Tibor Jager, and **Dominique Schröder**
pp. 512-531

(Efficient) Universally Composable Oblivious Transfer Using a Minimal Number of Stateless Tokens — TCC 2014
Seung Geol Choi, Jonathan Katz, **Dominique Schröder**, Arkady Yerukhimovich, Hong-Sheng Zhou
pp. 638-662

Brief Announcement: Towards Security and Privacy for Outsourced Data in the Multi-Party Setting — PODC 2014
Matteo Maffei, Giulio Malavolta, Manuel Reinert, and **Dominique Schröder**
pp. 144-146

Demo: Security and Privacy with Google Glass — CCS 2014
Johannes Krupp, **Dominique Schröder**, and Mark Simkin
pp. 1445-1447

Ubic: Bridging the gap Between Digital Cryptography and the Physical World — ESORICS 2014
Mark Simkin, **Dominique Schröder**, Andreas Bulling, and Mario Fritz
pp. 56-75

WebTrust - A Comprehensive Authenticity and Integrity Framework for HTTP — ACNS 2014
Michael Backes, Reiner W. Gerling, Sebastian Gerling, Stefan Nürnberger, **Dominique Schröder**, and Mark Simkin
pp. 401-418

Verifiable Data Streaming — CCS 2012
Dominique Schröder and Heike Schröder
pp. 953-964

Uniqueness is a Different Story: Impossibility of Verifiable Random Functions from Trapdoor Permutations
Dario Fiore and **Dominique Schröder**
pp. 636-653
TCC 2012

Security of Blind Signatures Revisited
Dominique Schröder and Dominique Unruh
pp. 662-679
PKC 2012

History-Free Sequential Aggregate Signatures
Marc Fischlin, Anja Lehmann, and **Dominique Schröder**
pp. 113-130
SCN 2012

Security of Blind Signatures Under Aborts and Applications to Adaptive Oblivious Transfer
Marc Fischlin and **Dominique Schröder**.
pp. 169-204
Journal Mathematical Cryptology 2012

Round Optimal Blind Signatures
Dominique Schröder and Dominique Unruh
pp. 630-648
CRYPTO 2011

Impossibility of Blind Signatures from One-Way Permutations
Jonathan Katz, **Dominique Schröder**, Arkady Yerukhimovich
pp. 615-629
TCC 2011

How to Aggregate the CL Signature
Dominique Schröder
pp. 298-314
ESORICS 2011

Expedient Non-Malleability Notions for Hash Functions
Paul Baecher, Marc Fischlin, and **Dominique Schröder**
pp. 268-283
CT-RSA 2011

On the Impossibility of Three-Move Blind Signature Schemes
Marc Fischlin and **Dominique Schröder**
pp. 197-215
EUROCRYPT 2010

Unlinkability of Sanitizable Signatures
Christina Brzuska, Marc Fischlin, Anja Lehmann, and **Dominique Schröder**
pp. 444-461
PKC 2010

Confidential Signatures and Deterministic Signcryption
Alex W. Dent, Marc Fischlin, Mark Manulis, **Dominique Schröder**, and Martijn Stam
pp. 462-479
PKC 2010

Redactable Signatures for Tree-Structured Data: Definitions and Construction — ACNS 2010
Christina Brzuska, Heike Busch, Özgür Dagdelen, Marc Fischlin, Martin Franz, Stefan Katzenbeisser, Mark Manulis, Cristina Onete, Andreas Peters, Bertam Poettering, and **Dominique Schröder**
pp. 87-104

Generic Constructions for Verifiably Encrypted Signatures without Random Oracles or NIZKs — ACNS 2010
Markus Rückert, Michael Schneider, and **Dominique Schröder**
pp. 69-86

History-Free Aggregate Message Authentication Codes — SCN 2010
Oliver Eikemeier, Marc Fischlin, Jens-Fabian Götzmann, Anja Lehmann, **Dominique Schröder**, Peter Schröder, and Daniel Wagner
pp. 309-328

Fair Partially Blind Signatures — Africacrypt 2010
Markus Rückert and **Dominique Schröder**
pp. 34-51

Public-Key Encryption with Non-interactive Opening: New Constructions and Stronger Definitions — Africacrypt 2010
David Galindo, Benoit Libert, Marc Fischlin, Georg Fuchsbauer, Anja Lehmann, Mark Manulis, and **Dominique Schröder**
pp. 333-350

CAPTCHAs: The Good, the Bad, and the Ugly. — Sicherheit 2010
Paul Baecher, Lior Gordon, Marc Fischlin, Michael Luetzow, **Dominique Schröder**
pp. 353-365

Security of Blind Signatures Under Aborts — PKC 2009
Marc Fischlin and **Dominique Schröder**
pp. 117-128

Security of Sanitizable Signatures Revisited — PKC 2009
Christina Brzuska, Marc Fischlin, Tobias Freudenreich, Anja Lehmann, Marcus Page, Jakob Schelbert, **Dominique Schröder**, and Florian Volk
pp. 297-316

Security of Verifiably Encrypted Signatures and a Construction Without Random Oracles — Pairings 2009
Markus Rückert and **Dominique Schröder**
pp. 17-34

Aggregate and Verifiably Encrypted Signatures from Multilinear Maps without Random Oracles — ISA 2009
Markus Rückert and **Dominique Schröder**
pp. 750-759

Sanitizable Signatures: How to Partially Delegate Control for Authenticated Data
Christina Brzuska, Marc Fischlin, Anja Lehmann, and **Dominique Schröder**
pp. 117-128
BioSig
2009

Mobi: Eine Infrastruktur fuer das Internet der Dinge
Michael Döring and **Dominique Schröder**
Informatiktage
2006

Patents

Methods for threshold password-hardened encryption and decryption
Russell W.F. Lai, Dominique Schröder, Christoph Egger, Julian Brost · US · 11323248
2022

Doctoral supervision

Davide Li Calsi
Distributed Systems
Ongoing
2025 - present

Ruben Baecker
Privacy-Preserving Access Control
Ongoing
2023 - present

Julian Thomas
Formalizations of privacy-enhancing cryptographic primitives
Ongoing
2023 - present

Paul Gerhart
Fair exchange, optimized Blockchain protocols and privacy
Ongoing
2022 - present

Hien Chu
Privacy-preserving techniques, threshold cryptography
Ongoing
2021 - present

Victoria Ronge
Security and Privacy of Cryptocurrency Signatures
First position after PhD: Industry
Current position: Industry
2018 - 2023

Dominic Deuber
Cryptocurrencies Within The Conflicting Tension Between Law and IT Security
First position after PhD: Postdoc at FAU
Current position: Industry
2017 - 2023

Russel W. F. Lai
Succinct Arguments: Constructions and Applications
First position after PhD: Assistant Professor at Aalto University
Current position: Assistant Professor at Aalto University
2017 - 2022

Christoph Egger
On Abstraction and Modularization in Protocol Analysis
First position after PhD: Researcher at Institut de Recherche en Inf. Fondamentale
Current position: Assistant Professor at Chalmers University of Technology
2016 - 2022

Sri Aravinda Krishnan Thyagarajan — 2016 - 2021
Cryptographic Locks for Scriptless Cryptocurrency Payments
First position after PhD: Postdoc at Carnegie Mellon University
Current position: Assistant Professor at the University of Sydney

Guilio Malavolta — 2013 - 2019
Cryptographic Clocks and Applications
First position after PhD: UC Berkeley and Carnegie Mellon University
Current position: Assistant Professor Bocconi University

Oliver Willers — 2015 - 2019
MEMS Sensors As Physical Unclonable Functions
First position after PhD: Bosch
Current position: Bosch

Tim Ruffing — 2014 - 2019
Cryptography for Bitcoin and Friends
First position after PhD: Blockstream
Current position: Blockstream

Nils Fleischhacker — 2012 - 2016
Minimal Assumptions in Cryptography
First position after PhD: Postdoc at Carnegie Mellon University and Johns Hopkins University
Current position: Assistant Professor at Ruhr University Bochum

Postdoctoral mentoring

Luigi Russo — 07/2025 - present

Dominic Deuber — 03/2023 - 06/2024
Subsequent position: IT security expert at the German Accreditation Body

Mojtaba Khalili — 09/2022 - 09/2023
Subsequent position: Assistant Professor, Isfahan University of Technology

Albrecht Petzoldt — 09/2019 - 08/2022
Subsequent position: Dagstuhl

Bernardo Magri — 11/2016 - 11/2018
Subsequent position: Associate Professor at the University of Manchester, UK.

Teaching

Advanced Privacy Enhancing Technologies — 2025
TUW · BSC/MSC

Data Privacy — 2025
FAU · BSC

IT Security & Law — 2025, 2024, 2023
FAU · Master

Privacy Enhancing Technologies — 2025
TUW · BSC

Blockchain und Kryptowährungen — 2024, 2022, 2020
FAU · BSC

Data Privacy — 2024, 2023, 2022
FAU · BSC/MSC

Introduction to Algorithms — 2024, 2023
FAU · BSC

Introduction to Data Privacy — 2023, 2021
FAU · BSC/MSC

Introduction to Modern Cryptography — 2023, 2022, 2021, 2020, 2018, 2017, 2016
FAU · BSC/MSC

Privacy and Legal Aspects and Their Realizations — 2022, 2021
FAU · BSC/MSC

Privacy-Preserving Cryptocurrencies — 2022, 2021, 2020
FAU · BSC/MSC

Secure Multi-Party Computation — 2021, 2017
FAU · BSC/MSC

Foundations of Privacy — 2020
FAU · BSC/MSC

Password-based Cryptography — 2020, 2019, 2018
FAU · BSC/MSC

Research Oriented Cryptography — 2020, 2014
UdS · BSC/MSC

Cryptocurrencies — 2019, 2018, 2016
FAU · BSC/MSC

Sabbatical — 2019
FAU · -

Algorithms and Data Structures — 2018
FAU · BSC

Foundations of Cryptocurrencies — 2017
FAU · BSC/MSC

Public-Key Encryption — 2017, 2015, 2014, 2013, 2012
UdS · BSC/MSC

Cryptocurrencies — 2016
UdS · BSC/MSC

Secure Multi-Party Computation — 2016, 2013
UdS · BSC/MSC

Introduction to Modern Cryptography — 2015, 2014
UdS · BSC/MSC

Recent Advances in Secure Multi-Party Computations — 2015
UdS · BSC/MSC

Conference leadership

ACM CCS Area Chair Applied Cryptography — 2025, 2026

Chair of IEEE International Conference on Blockchain	2023
Co-Chair of IEEE TEMS on Blockchain and Distributed Ledger Technologies.	2021
General Chair of IACR Theory of Cryptography Conference (TCC).	2019
Poster Session Chair of ACM Conference on Computer and Communications Security (CCS)	2016

Editorial boards

IACR Communications in Cryptology	2024-2026
ACM Transactions on Privacy and Security	2024

Program committees (selected)

USENIX Security	2026
ACM Conference on Computer and Communications Security	2019, 2023, 2024-2026
Advances in Cryptology (CRYPTO)	2016, 2019, 2020, 2023
Advances in Cryptology (EUROCRYPT)	2015, 2023, 2027
IEEE Computer Security Foundations Symposium	2020-2024
Advances in Cryptology (ASIACRYPT)	2022
Privacy Enhancing Technologies Symposium (PETS)	2021, 2022, 2024-2027
Public-Key Cryptography (PKC)	2023-2025
The Cryptographers' Track at RSA Conference (CT-RSA)	2025
European Symp. on Research in Computer Security (ESORICS)	2021-2026
Conf. on Cryptology and Network Security (CANS)	2016-2019, 2021-2023
IEEE Security and Privacy (Oakland)	2020, 2021
Advances in Cryptology (INDOCRYPT)	2021
CODASPY	2024
IEEE European Symposium on Security and Privacy (EuroSP)	2018
Asia Conference on Computer and Comm. Security (ASIACCS)	2017, 2018
Conference on Security and Cryptography for Networks (SCN)	2018, 2022
Conference on Applied Cryptography and Network Security (ACNS)	2024
International Conference on Provable Security (PROVSEC)	2016
ACM Conference on Pervasive and Ubiquitous Computing (UbiComp)	2016

Grant reviewing

European Research Council (ERC)

Deutsche Forschungsgemeinschaft (DFG)

Deutscher Akademischer Austauschdienst (DAAD)

Studienstiftung des Deutschen Volkes

Schloss Dagstuhl

Österreichische Forschungsföderungsgesellschaft (FFG)

Natural Sciences and Engineering Research Council of Canada (NSERC)

Dutch Research Council (NWO)

Journal reviewing

Journal of Cryptology

Journal of Computer Security

IET Journal for Information Security

Journal of Mathematical Cryptology

ACM Transactions on Privacy and Security (formerly TISSEC)

IEEE Transactions on Security and Dependable Computing

Doctoral committees

Jenny Ottmann — 2024
3rd reviewer · Friedrich-Alexander Universität Erlangen-Nürnberg

Swaroop Ready — 2024
2nd reviewer · Indian Institute of Technology, Hyderabad

Victoria Ronge — 2023
advisor · Friedrich-Alexander Universität Erlangen-Nürnberg

Dominic Deuber — 2023
advisor · Friedrich-Alexander Universität Erlangen-Nürnberg

Franz-Josef Streit — 2022
chair of the commission · Friedrich-Alexander Universität Erlangen-Nürnberg

Christoph Egger — 2022
advisor · Friedrich-Alexander Universität Erlangen-Nürnberg

Russell W. F. Lai — 2022
advisor · Friedrich-Alexander Universität Erlangen-Nürnberg

Sri Aravinda Krishnan Thyagarajan — 2021
advisor · Friedrich-Alexander Universität Erlangen-Nürnberg

Markus Zoppelt — 2021
1st reviewer · Friedrich-Alexander Universität Erlangen-Nürnberg

Katja Auernhammer — 2021
3rd reviewer · Friedrich-Alexander Universität Erlangen-Nürnberg

Kristof Teichel — 2021
2nd reviewer · Friedrich-Alexander Universität Erlangen-Nürnberg

Daniel Rausch — 2020
2nd Reviewer · Universität Stuttgart

Guilio Malavolta — 2019
advisor · Friedrich-Alexander Universität Erlangen-Nürnberg

Oliver Willers — 2019
1st reviewer, co-advisor · Saarland University

Tim Ruffing — 2019
co-advisor · Saarland University

Andrea Zimmermann — 2018
external examiner · Friedrich-Alexander Universität Erlangen-Nürnberg

Nils Fleischhacker — 2017
advisor · Saarland University

Yan Zhuang — 2017
chair of the commission · Friedrich-Alexander Universität Erlangen-Nürnberg

Mykolai Protsenko — 2017
chair of the commission · Friedrich-Alexander Universität Erlangen-Nürnberg

Thomas P. Jakobsen — 2015
2nd reviewer · Aarhus University, Denmark

Esfandiar Mohammadi — 2014
2nd reviewer · Saarland University

Administrative service

Head of 6 and member of 11 hiring committees — Since 2017

FAU Study commission B. Sc. computer/IT-security — since 2017

Department of computer science board of management FAU — 2016-2024

FAU Faculty council of the faculty of engineering (re-elected in 2021) — 2019-2024

FAU Department Informatik | speaker — 2023-2024

FAU Department Informatik | Deputy speaker — 2021-2023

Study commission computer science — 2018-2021

Scientific steering committee of the NCT — 2016-2017

Master admission committee (Saarland University) — 2012-2016

evelopment of the Bachelor “Cybersicherheit” (Saarland University) — 2014

Expert contributions and public service

Deutscher Bundestag · Health Committee — 2023
Independent expert contribution: Privacy and the use of health data

Deutscher Bundestag · Health Committee — 2020
Independent expert contribution: Patient Data Protection Act (PDSG)

Deutscher Bundestag · Health Committee — 2019
Independent expert contribution: Digital Healthcare Act (DVG)

Selected talks and appearances

Privacy of Medical Data — 2023
Humboldt Foundation, Network Meeting, Mainz

Welchen Beitrag leistet die Digitalisierung für eine gerechte Gesundheitsversorgung in Deutschland? — 2021
Leopoldina, Berlin, DE.

Data Privacy for Medical Records — 2019
TU Graz, Austria.

Privacy and Access Control for Outsourced Personal Records. — 2016
Leopoldina, Saarbrücken, DE.

Efficient Pseudorandom Functions via On-the-Fly Adaptation. — 2015
Chinese University of Hong Kong (CUHK), Hong Kong.

Bridging the Gap Between Digital Cryptography and the Physical World. — 2014
ATM Security, London, UK.

Ubicrypt - Die Unterschrift der Zukunft. — 2014
Future Talk, CeBiT, Hannover, Germany.

Security and Privacy in the Internet. — 2013
SR Television. Interview with Joachim Weyand

Verifiable Data Streaming — 2013
Intel Collaborative Research Institute for Secure Computing, Darmstadt, Germany.

Verifiable Data Streaming — 2013
University of Maryland, USA.

Verifiable Data Streaming — 2013
Brown University, USA.

Verifiable Data Streaming — 2013
IMDEA, Madrid Institute of Advanced Studies, Madrid, Spain.

Provable Security and Beyond. — 2012
Florida State University, Tallahassee, USA.

History-Free Aggregate Message Authentication Codes. — 2010
Universite de Rennes, Rennes, France.