

Ruben Baecker

Doctoral Student · Chair of Applied Cryptography · FAU Erlangen-Nürnberg

Konrad-Zuse-Strasse 3-5, 91052 Erlangen

mail@ruben-baecker.de · ruben-baecker.de · [Google Scholar](#) · [DBLP](#)

Education

since 12/2023	Friedrich-Alexander-University Erlangen-Nürnberg Main focus: Threshold Cryptography, Adaptive Security, Oblivious Pseudorandom Functions, Password-Based Cryptography Doctoral Student under Dominique Schröder, Cryptography
10/2021–09/2023	Friedrich-Alexander-University Erlangen-Nürnberg Main focus: Cryptography, Cyber Security, and IT-Forensics Master of Science with Distinction, Computer Science Thesis: Phoenix rises once again: How to defeat the (PW-)Hero Completed while caring for a child full-time (02/2022–11/2023)
10/2017–05/2022	Friedrich-Alexander-University Erlangen-Nürnberg Main focus: Cryptography Bachelor of Science with Distinction, Computer Science Thesis: Securing Passwords against Offline Dictionary Attacks

Peer-reviewed

2026	Fully Adaptive FROST in the Algebraic Group Model From Falsifiable Assumptions 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
2025	Password-Hardened Encryption Revisited Ruben Baecker, Paul Gerhart, and Dominique Schröder ASIACRYPT
2025	Universally Composable Password-Hardened Encryption Behzad Abdolmaleki, Ruben Baecker, Paul Gerhart, Mike Graf, Mojtaba Khalili, Daniel Rausch, and Dominique Schröder ASIACRYPT

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

Preprints

2026 **Adaptive Distributed Key Generation for Discrete-Log Cryptosystems**
Ruben Baecker, Paul Gerhart, Stanislaw Jarecki, Phillip Nazarian, Daniel Rausch, and
Dominique Schröder
eprint.iacr.org

Talks

2025 **Password-Hardened Encryption Revisited**
ASIACRYPT, Melbourne, AU
[Slides](#)

2025 **Universally Composable Password-Hardened Encryption**
ASIACRYPT, Melbourne, AU
[Slides](#)

2025 **A Fully-Adaptive Threshold Partially-Oblivious PRF**
CRYPTO, Santa Barbara, CA
[Slides](#) · [Video](#)

Work Experience

since 2023 **University Research Assistant**
Applied Cryptography
Friedrich-Alexander-University Erlangen-Nürnberg

2020–2021 **Student Employee**
Software Development in C#
Siemens AG - Digital Industries

2019–2020 **University Teaching Assistant**
System Programming I & II
Friedrich-Alexander-University Erlangen-Nürnberg

2018 **Student Employee**

Scholarships and Awards

2024	Jury Award at TechFak Science Slam 500€ Awarded for the slam "Password-Hardening - The Solution to the Password Problem" (in German)
2024	ASQF Best Thesis Award 500€ Awarded for the master thesis "Phoenix Rises Once Again: How to Defeat the (pw-)hero<="" span="" style="white-space: nowrap; ">"
2020–2023	German Academic Scholarship Foundation 300€ per Month Awarded for outstanding academic potential (extended in 2021 and 2022)

Parental Leave

12/2025–11/2026	Part-time parental leave, working 30 h/week Friedrich-Alexander-University Erlangen-Nürnberg
05/2025–07/2025	Full-time parental leave Friedrich-Alexander-University Erlangen-Nürnberg
08/2024–09/2024	Full-time parental leave Friedrich-Alexander-University Erlangen-Nürnberg

Research Visits

08/2025–09/2025	UC Irvine Hosted by Prof. Stanislaw Jarecki USA
-----------------	--

Supervised Students

2026	Samuel Huber <i>An Analysis of SecureDNA Continued</i> Master Thesis
------	---

2025	Tabea Stengl <i>An Analysis of SecureDNA</i> Bachelor Thesis
2025	Matthias Flosbach <i>Parameter Selection for LWR-based PRFs</i> Bachelor Thesis

Teaching Activities

Winter 26/27	Introduction to Modern Cryptography Teaching Assistant
Summer 26	Cryptography and Its Impact Organizer
Winter 25/26	Cryptography in Secure Messaging Organizer
Summer 25	Cryptography and Its Impact Organizer
Winter 24/25	Cryptography in Secure Messaging Organizer
Summer 24	Introduction to Algorithms (in German) Guest Lecturer

Community Service

	Program Committee
27	USENIX
26	ESORICS
	External Reviews (Selected)
24,25	CRYPTO
24,26	EUROCRYPT
26	ASIACRYPT
24,25	CCS
25	PKC
24,25,26	ESORICS
24,26,27	CSF