Curriculum Vitae

October 5, 2023

Paul Christoph Rösler

Department Informatik
FAU Erlangen-Nürnberg
Room 11.2.14
Fürther Strasse 246c / Entrance 5
90429 Nürnberg, Germany

E-Mail: paul.roesler@fau.de
Web page: roesler-paul.de
ORCID: 0000-0002-2324-5671
DOB: August 19, 1992
Citizenship: German

Overview

Topics, questions, and concepts that I am (currently) interested in as part of my research on real-world cryptography and provable security include:

- Secure Messaging Protocols, (Authenticated) Key Exchange, and Confidential Channels
- Security Guarantees under (temporary) Corruption of User Secrets
- Systematization of Definitions and Models for Real-World Applications

Major Research Contributions Four of my important results that I want to highlight, can be summarized as follows:

- I developed a *systematic framework for strongly secure messaging protocols* [12]. This was one of few starting (and reference) points for the new, quickly evolving field of *continuous and ratcheted key exchange*. Many follow-up works on secure messaging protocols, including my own publications [10],[9],[7],[6],[5],[3], are based on this framework.
- My *analysis of widely deployed group messaging apps* (WhatsApp and Signal) *revealed novel weaknesses* in the underlying protocols and triggered the development of substantially improved mechanisms [13].
- My publications on secure interoperable messaging [1],[18] as well as my active participation in the public discussion may strengthen privacy and security for the implementation of the European DMA.
- With theoretic *performance analyses of group messaging protocols*, I obtained *lower and upper bounds* for the (necessary and sufficient) *communication overhead* of these protocols [9],[6].

Education

01/2022 – 11/2022 **Postdoc** at Cryptography Group, **New York University**, USA
Host: Yevgeniy Dodis

03/2021 – 09/2021 **Postdoc** at Chair for Cryptography and Complexity Theory, **TU Darmstadt**, Germany
Host: Marc Fischlin

10/2016 – 02/2021 **Ph.D.** at Chair for Network and Data Security, **Ruhr University Bochum**, Germany
Grade: 1.0 with distinction (Summa cum laude)
Thesis: Cryptographic Foundations of Modern Stateful and Continuous Key Exchange Primitives
Advisor & 1st Referee: Jörg Schwenk, 2nd Referee: Marc Fischlin, 2nd Advisor: Eike Kiltz

10/2019 – 03/2022 Studied B.A. Philosophy, Ruhr University Bochum without pursuing graduation

10/2015 – 12/2018 **M.Sc.** IT Security/Information Technology, **Ruhr University Bochum**
Grade: 98%=1.0 with distinction, best out of 33 graduates in 2018 (ECTS grading scale: A=96-100%)
Thesis: On the End-to-End Security of Group Chats in Instant Messaging Protocols
1st Referee: Jörg Schwenk, 2nd Referee: Tibor Jager

10/2012 – 09/2015 **B.Sc.** IT Security/Information Technology, **Ruhr University Bochum**
Grade: 94%=1.1 (ECTS grading scale: A=89-100%)
Thesis: Security Analysis of Tresorit and Tresorit's DRM Architecture (translated)
1st Referee: Jörg Schwenk, 2nd Referee: Christian Mainka

Scholarships and Awards

01/2019 **Faculty Price for Best Master's Degree** in IT Security/Information Technology in 2018 out of 33 graduates (500€)

10/2016 – 09/2017 **Scholarship** from the Federal Ministry of Education and Research (Deutschlandstipendium), partially funded by Airbus Defense and Space (3000€; donated Airbus's share to anti-war NGOs)

12/2015 – 05/2017 **Member of KMPG** AG WGP's **highQ program** (non-monetary support)

Funding

02/2023 Joint application for second funding phase of DFG Research Training Group *Cybercrime and Forensic Computing* led by Felix Freiling (funding for 1 Ph.D. student for 3.5 years)

10/2022 Study for German Federal Network Agency on Interoperability in Secure Messengers in cooperation with Jörg Schwenk and Hackmanit GmbH (>60,000€)

02/2018 STSM funding by COST CryptoAction for visiting Bertram Poettering at Royal Holloway, University of London (900€)

01/2018 Assistance for successful funding application from European Regional Development Fund in cooperation with FH Münster, G Data Advanced Analytics GmbH, MedEcon Ruhr GmbH, and radprax GmbH (>645,000€)

Professional Experience

Since 12/2022 **Assistant Professor** (Jun.-Prof.) for Real-World Cryptography at **Friedrich-Alexander-Universität Erlangen-Nürnberg**

Since 2019 **Freelance Consultant**
Security analyses of, as well as technical training and consulting on modern secure messaging protocols

01/2022 **Post-Doctoral Associate** at Cryptography Group, **New York University**

– 11/2022 Host: Yevgeniy Dodis

09/2021 **Offer** for Tenure-Track **Assistant Professorship** for Cryptography at **University of Innsbruck**
Declined in favor of Post-Doctoral Associate at Cryptography Group, New York University

03/2021 – 09/2021 **Post-Doctoral Research Assistant** at Chair for Cryptography and Comlexity Theory, **TU Darmstadt**
Host: Marc Fischlin

10/2016 – 02/2021 **Research Assistant** at Chair for Network and Data Security, **Ruhr University Bochum**
Advisor: Jörg Schwenk, 2nd Advisor: Eike Kiltz
Supervised five student assistants as part of my teaching duties

10/2015 – 09/2016 **Teaching Assistant** at Chair for Network and Data Security, **Ruhr University Bochum**
Supporting exercises of the courses *XML- and Webservice-Security* and *Security Appliances*

04/2015 – 07/2015 **Internship** at **Security Consulting, KPMG** AG WPG
Assisting privacy audits, risk assessments, software reviews, and design of secure processes

10/2015 – 09/2016 & 09/2014 – 02/2015 **Protocol and Software Developer** at **Qabel** GmbH (open source E2E-encrypted cloud storage startup)
Design and implementation of cryptographic protocols, system security, and quality assurance

Research Visits

09/2023 Cryptography Group, Institute of Science and Technology Austria (ISTA)
With Krzysztof Pietrzak

08/2022 Cryptography Group, University of California San Diego (UCSD)
With Mihir Bellare

01/2020 Cryptography Group, New York University (NYU)
With Yevgeniy Dodis

10/2019 Applied Cryptography Group, Eidgenössische Technische Hochschule Zürich (ETH Zürich)
With Kenny Paterson

11/2018 Security and Cryptography Laboratory, École polytechnique fédérale de Lausanne (EPFL)
With Serge Vaudenay

02/2018 Information Security Group, Royal Holloway, University of London (RHUL)
With Bertram Poettering

Research Guests

07/2023 Daniel Collins
Security and Cryptography Laboratory, École polytechnique fédérale de Lausanne (EPFL)

Teaching

My Own Courses at FAU Erlangen-Nürnberg

Fall 2023 Seminar *Cryptography in Secure Messaging: Understanding and Enhancing Signal* (undergraduate and graduate)

Spr. 2023 Lecture *Cryptographic Communication Protocols: Key Exchange and Channels* (graduate)

Practical course on *Privacy and Cryptography* (graduate)

Guest lectures for course *Introduction to Algorithms* (undergraduate)

Fall 2022 Seminar *Cryptography in Secure Messaging: Understanding and Enhancing Signal* (undergraduate and graduate)

At Cryptography Group, New York University

Spr. 2022 Guest lectures for course *Authenticated Key Agreement: Formal Models and Applications* at Ruhr University Bochum (graduate)

At Chair for Cryptography and Complexity Theory, TU Darmstadt

Spr. 2021 Teaching Assistant for course *Real World Crypto* (graduate)

Guest lectures for course *Authenticated Key Agreement: Formal Models and Applications* at Ruhr University Bochum (graduate)

At Chair for Network and Data Security, Ruhr University Bochum

Fall 2020 Teaching Assistant for *TLS CASA Lecture* (graduate)

Spr. 2020 Teaching Assistant for course *Authenticated Key Agreement: Formal Models and Applications* (graduate)

Guest lecture for course *Real World Crypto Engineering* at Paderborn University (undergraduate and graduate)

Fall 2019 Coordinator for seminar *Network and Data Security* (undergraduate and graduate)

Spr. 2019 Teaching Assistant for course *Authenticated Key Agreement: Formal Models and Applications* (graduate)

Fall 2018 Teaching Assistant for course *Network Security 1* (undergraduate and graduate)

Spr. 2018 Teaching Assistant for course *Authenticated Key Agreement: Formal Models and Applications* (graduate)

Fall 2017 Coordinator for seminars *Network and Data Security* and *Authenticated Key Agreement: Formal Models and Applications* (undergraduate and graduate)

Spr. 2017 Teaching Assistant for course *Authenticated Key Agreement: Formal Models and Applications* (graduate)

Fall 2016 Coordinator for practical course on *Security Appliances* (undergraduate and graduate)

Doctoral Students

Thom Wiggers *Post-Quantum TLS.* Member of examination commission and external referee at Radboud University Nijmegen (2023)

Viktoria Ronge *Security and Privacy of Cryptocurrency Signatures.* Member of examination commission (2023)

Master Students
Melanie Alwardt, Marvin Schirrmacher, Marco Smeets, Juana Keinemann, Dominik Preikschat, Patrick Geisler

Bachelor Students
Linus Köhn, Moritz Sonntag, Theodros Zelleke, Jan Holthuis

Peer-Reviewing

Program Committees	CRYPTO (2024, 2023, 2022) EUROCRYPT (2023) RWC (2024, 2023) PETS (2023, 2022)
Journals	Communications in Cryptography (Editorial Board Member: 2024) Journal of Cryptology (Reviews: 2021, 2020, 2018, 2017) ACM TOPS (Review: 2019)
External Reviews	CRYPTO (2021, 2020, 2019) EUROCRYPT (2022, 2021, 2020) ASIACRYPT (2023, 2022, 2021, 2018) IEEE S&P (2021, 2020) USENIX Security (2019) ACM CCS (2018) TCC (2020, 2019, 2018) PKC (2021, 2019) CT-RSA (2022, 2020) CANS (2021)

Publications

Citations: 450, h-Index: 9, i10-Index: 9 (according to Google Scholar)

Preprint

[1] Julia Len, Esha Ghosh, Paul Grubbs, and **Paul Rösler**. Interoperability in end-to-end encrypted messaging. *IACR Cryptology ePrint Archive*, 2023:386, 2023. †

Journal Article

[2] Bertram Poettering and **Paul Rösler**. Combiners for AEAD. *IACR Transactions on Symmetric Cryptology*, (1), 2020. ∘

Conference Articles

[3] Alexander Bienstock, **Paul Rösler**, and Yi Tang. ASMesh: Secure messaging in mesh networks using stronger, anonymous double ratchet. In *ACM Conference on Computer and Communications Security (CCS)*, 2023. ∘

[4] Edita Bajramovic, Christofer Fein, Marius Frinken, **Paul Rösler**, and Felix Freiling. LAVA: Log authentication and verification algorithm. In *IEEE International Conference on IT Security Incident Management & IT Forensics (IMF)*, 2023. †

[5] **Paul Rösler**, Daniel Slamanig, and Christoph Striecks. Unique-path identity based encryption with applications to strongly secure messaging. In *Advances in Cryptology (EUROCRYPT)*, 2023. ∘

[6] Alexander Bienstock, Yevgeniy Dodis, Sanjam Garg, Garrison Grogan, Mohammad Hajiabadi, and **Paul Rösler**. On the worst-case inefficiency of CGKA. In *Theory of Cryptography (TCC)*, 2022. ∘

[7] Benjamin Dowling, Eduard Hauck, Doreen Riepel, and **Paul Rösler**. Strongly anonymous ratcheted key exchange. In *Advances in Cryptology (ASIACRYPT)*, 2022. ∘

[8] Bertram Poettering, **Paul Rösler**, Jörg Schwenk, and Douglas Stebila. SoK: Game-based security models for group key exchange. In *Topics in Cryptology (CT-RSA)*, 2021. ∘

[9] Alexander Bienstock, Yevgeniy Dodis, and **Paul Rösler**. On the price of concurrency in group ratcheting protocols. In *Theory of Cryptography (TCC)*, 2020. ∘

[10] Fatih Balli, **Paul Rösler**, and Serge Vaudenay. Determining the core primitive for optimally secure ratcheting. In *Advances in Cryptology (ASIACRYPT)*, 2020. ∘

[11] Benjamin Dowling, **Paul Rösler**, and Jörg Schwenk. Flexible authenticated and confidential channel establishment (fACCE): Analyzing the noise protocol framework. In *Public-Key Cryptography (PKC)*, 2020. ∘

[12] Bertram Poettering and **Paul Rösler**. Towards bidirectional ratcheted key exchange. In *Advances in Cryptology (CRYPTO)*, 2018. ∘

[13] **Paul Rösler**, Christian Mainka, and Jörg Schwenk. More is less: On the end-to-end security of group chats in signal, whatsapp, and threema. In *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2018. †

[14] Damian Poddebniak, Juraj Somorovsky, Sebastian Schinzel, Manfred Lochter, and **Paul Rösler**. Attacking deterministic signature schemes using fault attacks. In *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2018. †

[15] Martin Grothe, Christian Mainka, **Paul Rösler**, Johanna Jupke, Jan Kaiser, and Jörg Schwenk. Your cloud in my company: Modern rights management services revisited. In *International Conference on Availability, Reliability and Security (ARES)*, 2016. †

[16] Martin Grothe, Christian Mainka, **Paul Rösler**, and Jörg Schwenk. How to break microsoft rights management services. In *USENIX Workshop on Offensive Technologies (WOOT)*, 2016. †

∘: Authors listed alphabetically; †: Authors listed in order of their contributions.

Technical Reports

[17] Paul Gerhart, **Paul Rösler**, and Dominique Schröder. Security of ibex. 2023. Technical report commissioned by Threema GmbH

[18] **Paul Rösler** and Jörg Schwenk. Interoperability between messaging services – secure implementation of encryption. 2023. Technical report commissioned by the German Federal Network Agency (BNetzA)

Theses

[19] **Doctoral Thesis**. Cryptographic foundations of modern stateful and continuous key exchange primitives. Ruhr University Bochum, 2021

[20] **Master's Thesis**. On the end-to-end security of group chats in instant messaging protocols. Ruhr University Bochum, 2018. Full version of [13] including an introduction into, and a discussion of the background of modeling messaging in groups

[21] **Bachelor's Thesis**. Analysis of tresorit and tresorit DRM regarding architecture and security. Ruhr University Bochum, 2015. Title translated from German

Research Impact and Media Attention

To support strong security guarantees in upcoming interoperable messaging protocols as required by the European DMA, I published an overview article [1] as well as a technical report for the German Federal Network Agency [18]. Furthermore, I actively participate in the discussion hosted by the European Commission, I reflect about the matter with non-governmental organizations, and I provide information to journalists (e.g., for ORF).

Our analysis of group messaging protocols [13] resulted in protocol updates in Threema (V3.14 Android), influenced a new group management protocol for Signal, and was broadly covered in international media (e.g., Wired, Der Spiegel, The Telegraph, Süddeutsche Zeitung, Schneier on Security, Matthew Green's Blog). In addition to this, I contributed to press articles on many related topics in cryptography and IT security (e.g., my perspective on disclosure and responsible media communication after security incidents in Golem, comments on guarding and monitoring apps in Deutschlandfunk, and the differences between WhatsApp and Signal in Stern).

Talks

- ASMesh: Anonymous and Secure Messaging in Mesh Networks Using Stronger, Anonymous Double Ratchet (Invited). ISTA Mathematics and CS Seminar 2023
- Unique-Path Identity Based Encryption With Applications to Strongly Secure Messaging (Invited). NYU Crypto Reading Group 2023
- Interoperability between Messaging Services – Secure Implementation of Encryption. Bundesnetzagentur 2023
- Unique-Path Identity Based Encryption With Applications to Strongly Secure Messaging. IACR EUROCRYPT 2023
- Interoperable Messaging (Invited). DMA Stakeholder Workshop at European Commission 2023
- Strongly Anonymous Ratcheted Key Exchange. IACR ASIACRYPT 2022
- Systematic Approach to Practical Security Definitions, Automatically. NYU Crypto Reading Group 2022
- SoK: Game-based Security Models for Group Key Exchange. CT-RSA 2021
- Resolving Concurrency in Group Ratcheting Protocols. IACR RWC 2021
- Determining the Core Primitive for Optimally Secure Ratcheting. IACR ASIACRYPT 2020
- On the Price of Concurrency in Group Ratcheting Protocols. IACR TCC 2020
- Combiners for AEAD. IACR FSE 2020

- Resolving Concurrency in Group Ratcheting Protocols. Secure Messaging Summit 2020
- Guest lecture on the Signal Protocol (Invited). Real World Crypto Engineering Course 2020, Paderborn University
- Flexible Authenticated and Confidential Channel Establishment (fACCE): Analyzing the Noise Protocol Framework. IACR PKC 2020
- Taming Complexity of Messaging to understand its Security (Invited). ETH Zürich ZISC Lunch Seminar 2019
- Definitional Foundations of Ratcheting and their Impact on Practice (Invited). Workshop on Secure Messaging, IACR EUROCRYPT 2019
- Towards Bidirectional Ratcheted Key Exchange. IACR CRYPTO 2018
- Generalization and Modularization of the ACCE Model. Workshop on Secure Key Exchange and Channels SKECH 2018
- Consequences of Complexity in Group Instant Messaging using the Example of WhatsApp and Signal. RuhrSec 2018
- More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema. IEEE EuroS&P 2018
- Complexity of Group Communication in Instant Messaging. COST CryptoAction Symposium 2018
- On the End-to-End Security of Group Chats. IACR RWC 2018

Additional Skills

Soft Skills	*Management Skills for Engineers* by Schläper Management Consulting Training on self-management and leadership of a team
	Speaker of Ph.D. students in graduate school NERD NRW (03/2018-09/2020)
Language Skills	German: Mother tongue English: Fluent (Level C1 CEFR, UniCert III) Java, PHP, SQL
Hobbies	Playing piano, the drums, squash, and climbing
Social Engagement	Organization of demonstrations for climate justice in Bochum