

CURRICULUM VITAE

February 23, 2020

Paul Christoph Rösler

Chair for Network and Data Security
Ruhr University Bochum
Universitätsstr. 150
44801 Bochum, Germany

E-Mail: paul.roesler@rub.de
Web page: roesler-paul.de
DOB: August 19, 1992
Citizenship: German

Research Interests

Topics, question, and primitives in which I am (currently) interested as part of my research in cryptography and protocol security include:

- (Authenticated) key exchange
- (Authenticated and) confidential channel notions
- Stateful protocols and their security under state exposures
- Comparison and comparability of (game-based) security notions
- Generalization of pair-wise primitives to group settings
- Ethical questions and conflicts regarding research on and use of cryptography

Education

- 10/2016 – today Ph.D. Student at Chair for Network and Data Security, Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany (expected to graduate in 12/2020)
Advisor: Jörg Schwenk, Second Advisor: Eike Kiltz
- 10/2019 – today B.A. Philosophy, Ruhr University Bochum, Germany
- 10/2015 – 12/2018 M.Sc. IT Security/Information Technology, Ruhr University Bochum, Germany
Grade: 98%=1.0, best out of 33 graduates in 2018 (ECTS grading scheme: A=96-100%)
Thesis: On the End-to-End Security of Group Chats in Instant Messaging Protocols
- 10/2012 – 09/2015 B.Sc. IT Security/Information Technology, Ruhr University Bochum, Germany
Grade: 94%=1.1 (ECTS grading scheme: A=89-100%)
Thesis: Analysis of Tresorit and Tresorit DRM regarding Architecture and Security (translated)
- 07/2003 – 07/2012 Abitur at St. Ursula Gymnasium, Neheim, Germany

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' share to anti-war NGOs)

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

Funding

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

10/2016 Research assistant at Chair for Network and Data Security, Ruhr University Bochum
– today Funded by project SyncEnc of the Federal Ministry of Education and Research, and as member of the graduate school NERD NRW
05, 09 and 11/2019 Freelance consultant for CYBERCRYPT A/S
11/2019 Technical training and consulting on modern secure messaging protocols (focusing on Signal Messenger)
10/2015 Teaching assistant at Chair for Network and Data Security, Ruhr University Bochum
– 09/2016 Supporting exercises of the courses *XML- and Webservice-Security* and *Security Appliances*
04/2015 Internship at Security Consulting, KPMG AG WPG
– 07/2015 Assisting privacy audits, risk assessment, software reviews, and conception of security architectures
10/2015 Protocol and software developer at Qabel GmbH (open source e2e-encrypted cloud storage)
– 09/2016 Design and implementation of cryptographic protocols, system security, and quality assurance
& 09/2014
– 02/2015

Research Visits

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

Teaching

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)

Master Students

Marvin Schirmmacher, Marco Smeets, Juana Keinemann, Dominik Preikschat, Patrick Geisler

Bachelor Students

Moritz Sonntag, Theodros Zelleke, Jan Holthuis

Peer-Reviewing

- 2020 Journal of Cryptology, RuhrSec
External reviews: CRYPTO, EUROCRYPT, IEEE S&P, CT-RSA
- 2019 ACM TOPS
External reviews: CRYPTO, USENIX Security, TCC, PKC
- 2018 Journal of Cryptology
External reviews: ASIACRYPT, ACM CCS, TCC
- 2017 Journal of Cryptology

Publications

Citations: 96, h-Index: 5, i10-Index: 3

Preprint

- [1] Fatih Balli, Paul Rösler, and Serge Vaudenay. Determining the core primitive for optimally secure ratcheting. *IACR Cryptology ePrint Archive*, 2020:148, 2020

Journal Article

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

Conference Articles

- [3] 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
- [4] Bertram Poettering and Paul Rösler. Towards bidirectional ratcheted key exchange. In *Advances in Cryptology (CRYPTO)*, 2018

- [5] 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
- [6] Damian Poddebniak, Juraž 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
- [7] **Master’s Thesis**. On the end-to-end security of group chats in instant messaging protocols. Ruhr University Bochum, 2018. Full version of [5] including an introduction into and a discussion of the background of modeling messaging in groups
- [8] 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
- [9] Martin Grothe, Christian Mainka, Paul Rösler, and Jörg Schwenk. How to break microsoft rights management services. In *USENIX Workshop on Offensive Technologies (WOOT)*, 2016
- [10] **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

Our analysis of group messaging protocols [5] 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](#), [Schneier on Security](#), [Matthew Green’s Blog](#)).

Talks

- 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
- Complexity of Group Communication in Instant Messaging. COST CryptoAction Symposium 2018
- On the End-to-End Security of Group Chats. IACR Real World Crypto 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

Language German: Mother tongue

Skills English: Fluent (Level C1 CEFR, UniCert III)

Java, PHP, SQL

Hobbies Playing piano and the drums, skiing, bouldering

Social En- Organization of demonstrations against climate change; Member of community council for the
gagement Noise project