Doreen Riepel

CURRICULUM VITAE

☑ doreen.riepel@gmail.com | 🔏 www.doreenriepel.de | 🞓 Doreen Riepel

Summary

My research focuses on the theoretical foundations of applied cryptography and in particular on provable security. With my work, I aim to contribute to improving the theoretical guarantees for cryptography used in practice as well as designing new cryptographic schemes that are theoretically sound and practical. To this end, I develop and use rigorous security definitions that formally capture security properties and adversarial behavior. I then build protocols and prove their security relying on the security of other cryptographic primitives or hardness assumptions.

Experience _____

UC San Diego
 Postdoctoral Researcher at the Faculty for Computer Science and Engineering
 04/2023 - present

• Host: Mihir Bellare

UC Berkeley, CA, USA

• Research Visitor at the Faculty of Electrical Engineering and Computer Science 03/2022 - 04/2022

· Host: Sanjam Garg

NTT Research Virtual

Research Intern at the Cryptography & Information Security Laboratories
 06/2021 - 07/2021

· Host: Hoeteck Wee

Ruhr University Bochum Bochum, Germany

• Crossdisciplinary Research Project at the Chair for System Security 10/2020 - 12/2020

• Host: Thorsten Holz

NTNU Gjøvik Gjøvik, Norway

• Erasmus Student at the Faculty of Information Technology and Electrical Engineering 01/2018 - 06/2018

• Area of Study: Information Security

Hewlett Packard Enterprise

• Student within the "DualStudy" Program 10/2013 - 09/2016

• Internships in six different departments at four different locations

Education __

Dr. rer. nat. in Computer Science

Ruhr University Bochum

Advisor: Prof. Dr. Eike Kiltz

• Thesis title: "Tightly-Secure Authenticated Key Exchange"

• Thesis reviewers: Prof. Dr. Eike Kiltz, Prof. Dr. Tibor Jager, Prof. Dr. Shengli Liu

• Honor: Summa cum Laude

M. Sc. IN IT SECURITY Bochum, Germany

Ruhr University Bochum

• Thesis title: "Tight Encryption in a Multi-User Setting"

• Thesis reviewers: Prof. Dr. Eike Kiltz, Dr. Sven Schäge

B. Sc. in Business Information Systems

DHBW Mannheim

· Main area of study: Software Engineering

Bochum, Germany

Bad Homburg, Germany

02/2019 - 03/2023

10/2016 - 01/2019

Mannheim, Germany 10/2013 - 09/2019

Publications _____

CONFERENCE PUBLICATIONS

[KPRR23]	Eike Kiltz, Jiaxin Pan, Doreen Riepel, Magnus Ringerud. Multi-User CDH Problems and the Concrete Security of NAXOS and HMQV	CT-RSA	
[DHK ⁺ 23]	Julien Duman, Dominik Hartmann, Eike Kiltz, Sabrina Kunzweiler, Jonas Lehmann, Doreen Riepel. Generic Models for Group Actions		
[EQR+23]	Thorsten Eisenhofer, Erwin Quiring, Doreen Riepel, Jonas Möller, Konrad Rieck, Thorsten Holz. No more Reviewer #2: Subverting Automatic Paper-Reviewer Assignment using Adversarial Learning		
[AEK ⁺ 22]	Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler, Doreen Riepel. Password-Authenticated Key Exchange from Group Actions		
[DHK ⁺ 22]	Julien Duman, Dominik Hartmann, Eike Kiltz, Sabrina Kunzweiler, Jonas Lehmann, Doreen Riepel. Group Action Key Encapsulation and Non-Interactive Key Exchange in the QROM		
[DHRR22]	Benjamin Dowling, Eduard Hauck, Doreen Riepel, Paul Rösler. Strongly Anonymous Ratcheted Key Exchange		
[RW22]	Doreen Riepel, Hoeteck Wee. FABEO: Fast Attribute-Based Encryption with Optimal Security	CCS	
[ABH ⁺ 21]	Joël Alwen, Bruno Blanchet, Eduard Hauck, Eike Kiltz, Benjamin Lipp, Doreen Riepel. Analysing the HPKE Standard	Eurocrypt	
[JKRS21]	Tibor Jager, Eike Kiltz, Doreen Riepel, Sven Schäge. Tightly-Secure Authenticated Key Exchange, Revisited	Eurocrypt	
[HJK ⁺ 21]	Shuai Han, Tibor Jager, Eike Kiltz, Shengli Liu, Jiaxin Pan, Doreen Riepel, Sven Schäge. Authenticated Key Exchange and Signatures with Tight Security in the Standard Model	Crypto	
PREPRINTS			
[ERC ⁺ 23]	Thorsten Eisenhofer, Doreen Riepel, Varun Chandrasekaran, Esha Ghosh, Olga Ohrimenko, Nicolas Papernot. Verifiable and Provably Secure Machine Unlearning		

Talks_____

CONFERENCE TALKS

Multi-User CI 04/23	DH Problems and the Concrete Security of NAXOS and HMQV RSA Conference 2023	San Francisco, CA, USA		
FABEO: Fast Attribute-Based Encryption with Optimal Security 11/22 ACM CCS 2022 Los Angeles, CA, USA				
Password-Au 08/22	nthenticated Key Exchange from Group Actions Crypto 2022	Santa Barbara, CA, USA		
Tightly-Secure Authenticated Key Exchange, Revisited 10/21 Eurocrypt 2021 Zagreb, Crotic				
Authenticate 08/21	Virtual			

SEMINAR AND WORKSHOP TALKS

Advanced Key Exchange Protocols from CSIDH

Microsoft Research and University of Washington Redmond, WA, USA

Analysis of Key Exchange Protocols based on Group Actions

NTNU Trondheim 03/23 Trondheim, Norway

Generic Models for Group Actions

Young Researcher Crypto Seminar (YRCS) Regensburg, Germany 03/23

Password-Authenticated Key Exchange from Group Actions

UC San Diego 11/22 La Jolla, CA, USA

FABEO: Fast Attribute-Based Encryption with Optimal Security

NTT Research CIS Update 2022 Santa Barbara, CA, USA 08/22

On Key Exchange from Group Actions

07/22 Secure Key Exchange and Channel Protocols (SKECH) Bertinoro, Italy

Password-Authenticated Key Exchange from Group Actions

03/22 Berkeley, CA, USA UC Berkeley 01/22 Max-Planck Institute for Security and Privacy Bochum, Germany 01/22 New York University Virtual

Teaching and Mentoring

THESES SUPERVISION

Updatable Public Key Encryption

08/2022 - 01/2023 • Master Thesis by Christian Baumhör at Ruhr University Bochum

• Supervised together with Eike Kiltz

Bochum, Germany

TEACHING ASSISTANT

Post-Quantum Cryptography

Bochum, Germany 10/2019 - 03/2020

• Topics: Quantum algorithms and lattice-based cryptography

• Lectured by Eike Kiltz at Ruhr-University Bochum

Academic Service

PROGRAM COMMITTEES EXTERNAL REVIEWING

2023 TCC 2020 Crypto 2024 Eurocrypt 2021 Eurocrypt

> 2022 Crypto, ACM TOPS 2023 Eurocrypt, PKC

Extracurricular Activity _____

Study Advisory Board Bochum, Germany

• Faculty for Computer Science at Ruhr University Bochum

• Representative of Research Assistants

Equal Opportunities and Diversity Board

• Cluster of Excellence CASA at Ruhr University Bochum

• Representative of PhD students and co-speaker in the CASA Management Board

04/2022 - 03/2023

Bochum, Germany 09/2019 - 09/2021