Doreen Riepel

Curriculum Vitae

doreen.riepel@gmail.com | www.doreenriepel.me | 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 well-considered 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 — *La Jolla, CA, USA*
- Postdoctoral Researcher at the Faculty for Computer Science and Engineering — *04/2023 - present*
- Host: Mihir Bellare

UC Berkeley — *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 Systems 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 — *Bad Homburg, Germany*
- 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 — *Bochum, Germany*
Ruhr University Bochum — *02/2019 - 03/2023*
- 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 — *10/2016 - 01/2019*
- Thesis title: "Tight Encryption in a Multi-User Setting"
- Thesis reviewers: Prof. Dr. Eike Kiltz, Dr. Sven Schäge

B. Sc. in Business Information Systems — *Mannheim, Germany*
DHBW Mannheim — *10/2013 - 09/2019*
- Main area of study: Software Engineering

Publications

Conference Publications

[BRRA24]	Mihir Bellare, Rishabh Ranjan, Doreen Riepel, Ali Aldakheel. The Concrete Security of Two-Party Computation: Simple Definitions, and Tight Proofs for PSI and OPRFs	Asiacrypt
[DRS24]	Emanuele Di Giandomenico, Doreen Riepel, Sven Schäge. Tightly-Secure Group Key Exchange with Perfect Forward Secrecy	Asiacrypt
[BRTZ24]	Mihir Bellare, Doreen Riepel, Stefano Tessaro, Yizhao Zhang. Count Corruptions, Not Users: Improved Tightness for Signatures, Encryption and Authenticated Key Exchange	Asiacrypt
[CRT24]	Daniel Collins, Doreen Riepel, Si An Oliver Tran. On the Tight Security of the Double Ratchet	CCS
[RVV24]	Doreen Riepel, Marloes Venema, Tanya Verma. ISABELLA: Improving Structures of Attribute-Based Encryption Leveraging Linear Algebra	CCS
[MR24]	Jonas Meers, Doreen Riepel. CCA Secure Updatable Encryption from Non-Mappable Group Actions	PQCrypto
[PRZ24]	Jiaxin Pan, Doreen Riepel, Runzhi Zeng. Key Exchange with Tight (Full) Forward Secrecy via Key Confirmation	Eurocrypt
[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	Usenix Security
[DHK+23]	Julien Duman, Dominik Hartmann, Eike Kiltz, Sabrina Kunzweiler, Jonas Lehmann, Doreen Riepel. Generic Models for Group Actions	PKC
[KPRR23]	Eike Kiltz, Jiaxin Pan, Doreen Riepel, Magnus Ringerud. Multi-User CDH Problems and the Concrete Security of NAXOS and HMQV	CT-RSA
[RW22]	Doreen Riepel, Hoeteck Wee. FABEO: Fast Attribute-Based Encryption with Optimal Security	CCS
[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	Asiacrypt
[DHRR22]	Benjamin Dowling, Eduard Hauck, Doreen Riepel, Paul Rösler. Strongly Anonymous Ratcheted Key Exchange	Asiacrypt
[AEK+22]	Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler, Doreen Riepel. Password-Authenticated Key Exchange from Group Actions	Crypto
[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
[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

Preprints

[BRS24] Mihir Bellare, Doreen Riepel, Laura Shea. Algorithm Substitution Attacks on Public Functions

[ERC+23] Thorsten Eisenhofer, Doreen Riepel, Varun Chandrasekaran, Esha Ghosh, Olga Ohrimenko, Nicolas Papernot. Verifiable and Provably Secure Machine Unlearning

Talks

Conference Talks

06/24 PQCrypto 2024 *Oxford, UK*

Key Exchange with Tight (Full) Forward Secrecy via Key Confirmation
05/24 Eurocrypt 2024 *Zürich, Switzerland*

Multi-User CDH Problems and the Concrete Security of NAXOS and HMQV
04/23 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-Authenticated Key Exchange from Group Actions
08/22 Crypto 2022 *Santa Barbara, CA, USA*

Tightly-Secure Authenticated Key Exchange, Revisited
10/21 Eurocrypt 2021 *Zagreb, Crotia*

Authenticated Key Exchange and Signatures with Tight Security in the Standard Model
08/21 Crypto 2021 *Virtual*

Seminar and Workshop Talks

On the Tight Security of the Double Ratchet
06/24 NTNU Trondheim *Trondheim, Norway*

Tightly-Secure AKE: Overview, Challenges and New Directions
06/24 Secure Key Exchange and Channel Protocols (SKECH) *Bertinoro, Italy*

Advanced Key Exchange Protocols from CSIDH
07/23 Microsoft Research and University of Washington *Redmond, WA, USA*

Analysis of Key Exchange Protocols based on Group Actions
03/23 NTNU Trondheim *Trondheim, Norway*

Generic Models for Group Actions
03/23 Young Researcher Crypto Seminar (YRCS) *Regensburg, Germany*

Password-Authenticated Key Exchange from Group Actions
11/22 UC San Diego *La Jolla, CA, USA*

FABEO: Fast Attribute-Based Encryption with Optimal Security
08/22 NTT Research CIS Update 2022 *Santa Barbara, CA, USA*

On Key Exchange from Group Actions
07/22 Secure Key Exchange and Channel Protocols (SKECH) *Bertinoro, Italy*

Seminar and Workshop Talks (Cont'd)

Password-Authenticated Key Exchange from Group Actions

03/22	UC Berkeley	*Berkeley, CA, USA*
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 — *Bochum, Germany*, *08/2022 - 01/2023*

- Master Thesis by Christian Baumhör at Ruhr University Bochum
- Supervised together with Eike Kiltz

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

2023	TCC
2024	Eurocrypt
2025	PKC, ACNS

External Reviewing

2020	Crypto
2021	Eurocrypt
2022	Crypto, ACM TOPS
2023	Eurocrypt, PKC

Extracurricular Activity

Study Advisory Board — *Bochum, Germany*, *04/2022 - 03/2023*

- Faculty for Computer Science at Ruhr University Bochum
- Representative of Research Assistants

Equal Opportunities and Diversity Board — *Bochum, Germany*, *09/2019 - 09/2021*

- Cluster of Excellence CASA at Ruhr University Bochum
- Representative of PhD students and co-speaker in the CASA Management Board