Doreen Riepel

CURRICULUM VITAE

✉ riepel@cispa.de | ⌂ 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. I develop and use 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

Tenure-Track Faculty — *Saarbrücken, Germany*
- CISPA Helmholtz Center for Information Security

12/2024 - present

Postdoctoral Researcher — *La Jolla, CA, USA*
- UC San Diego
- Host: Mihir Bellare

04/2023 - 11/2024

Research Visit — *Berkeley, CA, USA*
- UC Berkeley
- Host: Sanjam Garg

03/2022 - 04/2022

Research Internship — *Virtual*
- NTT Research (Cryptography & Information Security Laboratories)
- Host: Hoeteck Wee

06/2021 - 07/2021

Crossdisciplinary Research Internship — *Bochum, Germany*
- Ruhr University Bochum (Chair for Systems Security)
- Host: Thorsten Holz

10/2020 - 12/2020

Erasmus Student — *Gjøvik, Norway*
- NTNU Gjøvik
- Area of Study: Information Security

01/2018 - 06/2018

DualStudy Program — *Bad Homburg, Germany*
- Hewlett Packard Enterprise
- Internships in six different departments at four different locations

10/2013 - 09/2016

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 - 09/2016*

- Main area of study: Software Engineering

Publications

Conference Publications

[AVR+25]	Sven Argo, Marloes Venema, Doreen Riepel, Tim Güneysu, Diego F. Aranha. ABE Cubed: Advanced Benchmarking Extensions for ABE Squared	CHES
[BRS25a]	Mihir Bellare, Doreen Riepel, Laura Shea. Intermundium-DL: Assessing the Resilience of Current Schemes to Discrete-Log-Computation Attacks on Public Parameters	PKC
[BRS25b]	Mihir Bellare, Doreen Riepel, Laura Shea. Public-Algorithm Substitution Attacks: Subverting Hashing and Verification	PKC
[ERC+25]	Thorsten Eisenhofer, Doreen Riepel, Varun Chandrasekaran, Esha Ghosh, Olga Ohrimenko, Nicolas Papernot. Verifiable and Provably Secure Machine Unlearning	SaTML
[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

[JMOR25]	Jonas Janneck, Jonas Meers, Massimo Ostuzzi, Doreen Riepel. Snake Mackerel: An Isogeny-Based AKEM Leveraging Randomness Reuse
[AFMR25]	Joël Alwen, Georg Fuchsbauer, Marta Mularczyk, Doreen Riepel. Lattice-Based Updatable Public-Key Encryption for Group Messaging

Talks

Conference Talks

Count Corruptions, Not Users: Improved Tightness for Signatures, Encryption and Authenticated Key Exchange

12/24	Asiacrypt 2024	*Kolkata, India*

On the Tight Security of the Double Ratchet

10/24	ACM CCS 2024	*Salt Lake City, UT, USA*

CCA Secure Updatable Encryption from Non-Mappable Group Actions

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, Croatia*

Authenticated Key Exchange and Signatures with Tight Security in the Standard Model

08/21	Crypto 2021	*Virtual*

Seminar and Workshop Talks

Modeling and Proving Security: From Foundations of Key Exchange to Real-World Cryptography

06/25	Women in Security and Cryptography Workshop (WISC)	*Bochum, Germany*

Count Corruptions, Not Users: Improved Tightness for Signatures, Encryption and Authenticated Key Exchange

06/25	Ruhr University Bochum	*Bochum, Germany*
06/25	University of Wuppertal	*Wuppertal, Germany*

Key Exchange Security - Pen&Paper Model and Proof of Signed Diffie-Hellman

05/25	Workshop on Computer-Aided Proofs of Security (CAPS)	*Madrid, Spain*

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

02/25	Workshop on PAKE and Password Security & Usability	*Luxembourg*
03/22	UC Berkeley	*Berkeley, CA, USA*
01/22	Max-Planck Institute for Security and Privacy	*Bochum, Germany*
01/22	New York University	*Virtual*

Advising and Mentoring

Current and Past Group Members

PhD Students *CISPA*

- Subham Das *09/2025 - present*

Postdocs *CISPA*

- Xiangyu Liu *06/2025 - present*

Interns *CISPA*

- Agni Datta *06/2025 - 08/2025*
- Weidan Ji (virtual) *06/2025 - present*

Theses Supervision

Updatable Public Key Encryption *Bochum, Germany*

- Master Thesis by Christian Baumhör at Ruhr University Bochum *08/2022 - 01/2023*
- Supervised together with Eike Kiltz

Teaching

Seminars

Cryptoghraphic Foundations of Secure Messaging *Leibniz Universität Hannover*

- Topics: Various papers on provable security of messaging applications *Winter 2025/26*
- Presentation of research papers

Provable Security of Key Exchange Protocols *Saarland University*

- Topics: Various papers on advanced protocols and security models *Summer 2025*
- Presentation of research papers

Teaching Assistant

Post-Quantum Cryptography *Ruhr University Bochum*

- Topics: Quantum algorithms and lattice-based cryptography *Winter 2019/20*
- Lectured by Eike Kiltz at Ruhr-University Bochum

Academic Service

Program Committees

2023	TCC
2024	Eurocrypt
2025	PKC, ACNS
2026	S&P

External Reviewing

2020	Crypto
2021	Eurocrypt
2022	Crypto, ACM TOPS
2023	Eurocrypt, PKC
2024	Crypto, TCC, Asiacrypt, ACM TOPS, JoC
2025	Crypto, JoC

Other Committees

2025	CAST/GI Promotionspreis IT-Sicherheit

Extracurricular Activity

Study Advisory Board *Bochum, Germany*

- Faculty for Computer Science at Ruhr University Bochum *04/2022 - 03/2023*
- Representative of Research Assistants

Equal Opportunities and Diversity Board *Bochum, Germany*

- Cluster of Excellence CASA at Ruhr University Bochum *09/2019 - 09/2021*
- Representative of PhD students and co-speaker in the CASA Management Board