

### 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

- Postdoctoral Researcher at the Faculty for Computer Science and Engineering
- Host: Mihir Bellare

*La Jolla, CA, USA*

*04/2023 - present*

#### UC Berkeley

- Research Visitor at the Faculty of Electrical Engineering and Computer Science
- Host: Sanjam Garg

*Berkeley, CA, USA*

*03/2022 - 04/2022*

#### NTT Research

- Research Intern at the Cryptography & Information Security Laboratories
- Host: Hoeteck Wee

*Virtual*

*06/2021 - 07/2021*

#### Ruhr University Bochum

- Crossdisciplinary Research Project at the Chair for Systems Security
- Host: Thorsten Holz

*Bochum, Germany*

*10/2020 - 12/2020*

#### NTNU Gjøvik

- Erasmus Student at the Faculty of Information Technology and Electrical Engineering
- Area of Study: Information Security

*Gjøvik, Norway*

*01/2018 - 06/2018*

#### Hewlett Packard Enterprise

- Student within the “DualStudy” Program
- Internships in six different departments at four different locations

*Bad Homburg, Germany*

*10/2013 - 09/2016*

### 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 Jäger, Prof. Dr. Shengli Liu
- Honor: Summa cum Laude

*Bochum, Germany*

*02/2019 - 03/2023*

#### M. SC. IN IT SECURITY

##### Ruhr University Bochum

- Thesis title: “Tight Encryption in a Multi-User Setting”
- Thesis reviewers: Prof. Dr. Eike Kiltz, Dr. Sven Schäge

*Bochum, Germany*

*10/2016 - 01/2019*

#### B. SC. IN BUSINESS INFORMATION SYSTEMS

##### DHBW Mannheim

- Main area of study: Software Engineering

*Mannheim, Germany*

*10/2013 - 09/2019*

## Publications

---

### CONFERENCE PUBLICATIONS

[BRR24]	Mihir Bellare, Rishabh Ranjan, Doreen Riepel, Ali Aldakheel. The Concrete Security of Two-Party Computation: Simple Definitions, and Tight Proofs for PSI and OPRFs	<a href="#">Asiacrypt</a>
[DRS24]	Emanuele Di Giandomenico, Doreen Riepel, Sven Schäge. Tightly-Secure Group Key Exchange with Perfect Forward Secrecy	<a href="#">Asiacrypt</a>
[BRTZ24]	Mihir Bellare, Doreen Riepel, Stefano Tessaro, Yizhao Zhang. Count Corruptions, Not Users: Improved Tightness for Signatures, Encryption and Authenticated Key Exchange	<a href="#">Asiacrypt</a>
[CRT24]	Daniel Collins, Doreen Riepel, Si An Oliver Tran. On the Tight Security of the Double Ratchet	<a href="#">CCS</a>
[RV24]	Doreen Riepel, Marloes Venema, Tanya Verma. ISABELLA: Improving Structures of Attribute-Based Encryption Leveraging Linear Algebra	<a href="#">CCS</a>
[MR24]	Jonas Meers, Doreen Riepel. CCA Secure Updatable Encryption from Non-Mappable Group Actions	<a href="#">PQCrypto</a>
[PRZ24]	Jiaxin Pan, Doreen Riepel, Runzhi Zeng. Key Exchange with Tight (Full) Forward Secrecy via Key Confirmation	<a href="#">Eurocrypt</a>
[EQR <sup>+</sup> 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	<a href="#">Usenix Security</a>
[DHK <sup>+</sup> 23]	Julien Duman, Dominik Hartmann, Eike Kiltz, Sabrina Kunzweiler, Jonas Lehmann, Doreen Riepel. Generic Models for Group Actions	<a href="#">PKC</a>
[KPRR23]	Eike Kiltz, Jiaxin Pan, Doreen Riepel, Magnus Ringerud. Multi-User CDH Problems and the Concrete Security of NAXOS and HMQV	<a href="#">CT-RSA</a>
[RW22]	Doreen Riepel, Hoeteck Wee. FABEO: Fast Attribute-Based Encryption with Optimal Security	<a href="#">CCS</a>
[DHK <sup>+</sup> 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	<a href="#">Asiacrypt</a>
[DHRR22]	Benjamin Dowling, Eduard Hauck, Doreen Riepel, Paul Rösler. Strongly Anonymous Ratcheted Key Exchange	<a href="#">Asiacrypt</a>
[AEK <sup>+</sup> 22]	Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler, Doreen Riepel. Password-Authenticated Key Exchange from Group Actions	<a href="#">Crypto</a>
[HJK <sup>+</sup> 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	<a href="#">Crypto</a>
[ABH <sup>+</sup> 21]	Joël Alwen, Bruno Blanchet, Eduard Hauck, Eike Kiltz, Benjamin Lipp, Doreen Riepel. Analysing the HPKE Standard	<a href="#">Eurocrypt</a>
[JKRS21]	Tibor Jager, Eike Kiltz, Doreen Riepel, Sven Schäge. Tightly-Secure Authenticated Key Exchange, Revisited	<a href="#">Eurocrypt</a>

## PREPRINTS

- [BRS24] Mihir Bellare, Doreen Riepel, Laura Shea. Algorithm Substitution Attacks on Public Functions
- [ERC<sup>+</sup>23] Thorsten Eisenhofer, Doreen Riepel, Varun Chandrasekaran, Esha Ghosh, Olga Ohrimenko, Nicolas Papernot. Verifiable and Provably Secure Machine Unlearning

## Talks

---

### CONFERENCE TALKS

- 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

- 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

01/22 Max-Planck Institute for Security and Privacy

01/22 New York University

*Berkeley, CA, USA*

*Bochum, Germany*

*Virtual*

## Teaching and Mentoring

---

### THESES SUPERVISION

Updatable Public Key Encryption

- Master Thesis by Christian Baumh r at Ruhr University Bochum
- Supervised together with Eike Kiltz

*Bochum, Germany*

*08/2022 - 01/2023*

### TEACHING ASSISTANT

Post-Quantum Cryptography

- Topics: Quantum algorithms and lattice-based cryptography
- Lectured by Eike Kiltz at Ruhr-University Bochum

*Bochum, Germany*

*10/2019 - 03/2020*

## 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

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

*Bochum, Germany*

*04/2022 - 03/2023*

### 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

*Bochum, Germany*

*09/2019 - 09/2021*