Doreen Riepel

Curriculum Vitae

Universitätsstr. 150
44801 Bochum
Germany
✉ *doreen.riepel@rub.de*
doreenriepel.me

Academic Education

02/2019 – 03/2023 **Ph.D. Student, Cryptography**
Faculty for Computer Science, Ruhr-Universität Bochum, Germany
- 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*

10/2016 – 01/2019 **Master of Science (M.Sc.), IT-Security**
Ruhr-Universität Bochum, Germany
- Thesis title: *"Tight Encryption in a Multi-User Setting"*
- Final grade: *95% out of 100%*

10/2013 – 09/2016 **Bachelor of Science (B.Sc.), Business Information Systems**
Duale Hochschule Baden-Württemberg, Mannheim, Germany
- Main area of study: *Software Engineering*
- Final grade: *1.6*

Experience

04/2023 – 04/2024 **UC San Diego**
Postdoctoral Researcher at the Faculty of Electrical Engineering and Computer Science
- Host: *Mihir Bellare*

03/2022 **UC Berkeley**
Research Visitor at the Faculty of Electrical Engineering and Computer Science
- Host: *Sanjam Garg*

06/2021 – 07/2021 **NTT Research**
Research Intern at the Cryptography & Information Security Laboratories
- Advisor: *Hoeteck Wee*

01/2018 – 06/2018 **NTNU in Gjøvik, Norway**
Exchange Student in Information Security
- Semester abroad within the European Erasmus program

10/2013 – 09/2016 **Hewlett Packard Enterprise**

"Dual Study" program with internships in the following departments:

- Financial Services Industry, Walldorf, Germany
- Server Automation, Sunnyvale, USA
- Applications Transformation, Berlin, Germany
- HP Networking, Bad Homburg, Germany
- Communications and Media Solutions, Bad Homburg, Germany

Teaching Activities and Further Training

09/2022 Summer School crypt@b-it on Isogeny-Based Cryptography and Secure Distributed Computation (Bonn, Germany)

10/2019 – 03/2020 Teaching Assistant for Post-Quantum Cryptography

02/2019 Winter School on Zero Knowledge (Tel Aviv, Israel)

07/2016 Summer School on Internet of Things (Ontario, Canada)

Publications and Research Activities

[1] Tibor Jager, Eike Kiltz, Doreen Riepel, Sven Schäge: "Tightly-Secure Authenticated Key Exchange, Revisited" (EUROCRYPT 2021)

[2] Joël Alwen, Bruno Blanchet, Eduard Hauck, Eike Kiltz, Benjamin Lipp, Doreen Riepel: "Analysing the HPKE Standard" (EUROCRYPT 2021)

[3] 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 2021)

[4] Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler, Doreen Riepel: "Password-Authenticated Key Exchange from Group Actions" (CRYPTO 2022)

[5] 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 2022)

[6] Benjamin Dowling, Eduard Hauck, Doreen Riepel, Paul Rösler: "Strongly Anonymous Ratcheted Key Exchange" (ASIACRYPT 2022)

[7] Doreen Riepel, Hoeteck Wee: "FABEO: Fast Attribute-Based Encryption with Optimal Security" (ACM CCS 2022)

[8] Thorsten Eisenhofer, Doreen Riepel, Varun Chandrasekaran, Esha Ghosh, Olga Ohrimenko, and Nicolas Papernot: "Verifiable and Provably Secure Machine Unlearning" (Computing Research Repository)

[9] Eike Kiltz, Jiaxin Pan, Doreen Riepel, Magnus Ringerud: "Multi-User CDH Problems and the Concrete Security of NAXOS and HMQV" (CT-RSA 2023)

[10] Julien Duman, Dominik Hartmann, Eike Kiltz, Sabrina Kunzweiler, Jonas Lehmann, Doreen Riepel: "Generic Models for Group Actions" (PKC 2023)

[11] Thorsten Eisenhofer, Erwin Quiring, Jonas Möller, Doreen Riepel, Thorsten Holz, Konrad Rieck: "No more Reviewer #2: Subverting Automatic Paper-Reviewer Assignment using Adversarial Learning" (USENIX 2023)

Other

Member	Equal Opportunities Board in the Excellence Cluster CASA
Sub-Reviewer	Eurocrypt 2021, 2023; Crypto 2020, 2022; PKC 2023; ACM TOPS Journal 2022
Scholarship	"Deutschlandstipendium", funded by the Horst Görtz Stiftung
Languages	German, English