Jonas Meers, M.Sc.

jonas@meers.org https://meers.org/

Employment History

2021 – · · · ·	**PhD Student,** Chair of Cryptography, Ruhr University Bochum
2019 – 2021	**Working Student,** IT-Security, aramido GmbH
02.2019 – 07.2019	**Intern,** IT-Security, EXXETA AG

Education

2018 – 2021 **M.Sc. Computer Science, Karlsruher Institut für Technologie** in IT-Security.
Thesis title: *Ramanujan Graphs in Cryptography*.

2014 – 2018 **B.Sc. Computer Science, Universität zu Lübeck** in IT-Security.
Thesis title: *The Computational Complexity Of Worst Case Flows In Unreliable Flow Networks*.

Experiences

09.2024 – · · · · **Research Visitor,** COSIC, KU Leuven
Host: Frederik Vercauteren

Research Publications

1. **J. Meers** and D. Riepel, "CCA secure updatable encryption from non-mappable group actions," in *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part I*, M.-J. Saarinen and D. Smith-Tone, Eds., Springer, Cham, Jun. 2024, pp. 137–169. DOI: 10.1007/978-3-031-62743-9_5.
2. J. Duman, D. Hartmann, E. Kiltz, S. Kunzweiler, **J. Lehmann**, and D. Riepel, "Generic models for group actions," in *PKC 2023, Part I*, A. Boldyreva and V. Kolesnikov, Eds., ser. LNCS, vol. 13940, Springer, Cham, May 2023, pp. 406–435. DOI: 10.1007/978-3-031-31368-4_15.
3. **J. Meers** and J. Nowakowski, "Solving the hidden number problem for CSIDH and CSURF via automated coppersmith," in *ASIACRYPT 2023, Part IV*, J. Guo and R. Steinfeld, Eds., ser. LNCS, vol. 14441, Springer, Singapore, Dec. 2023, pp. 39–71. DOI: 10.1007/978-981-99-8730-6_2.
4. J. Duman, D. Hartmann, E. Kiltz, S. Kunzweiler, **J. Lehmann**, and D. Riepel, "Group action key encapsulation and non-interactive key exchange in the QROM," in *ASIACRYPT 2022, Part II*, S. Agrawal and D. Lin, Eds., ser. LNCS, vol. 13792, Springer, Cham, Dec. 2022, pp. 36–66. DOI: 10.1007/978-3-031-22966-4_2.

Academic Service

External Reviews
2023: CRYPTO, TCC, ESORICS
2024: EUROCRYPT, PQCrypto
2025: PKC

Teaching

2021 – 2022 **Teaching Assistant** in Cryptography, Lectured by Eike Kiltz at Ruhr University Bochum
Topics: Symmetric and Asymmetric Cryptography

2019 – 2020 **Tutor** in Mathematics for Economists, Lectured by Martin Folkers at Karlsruher Institut für Technologie
Topics: Introductory Topics in Combinatorics, Calculus and Linear Algebra

2016 – 2017 **Tutor** in Logic, Lectured by Till Tantau at University of Lübeck
Topics: Propositional Logic, First-Order Logic, Temporal Logic, Modal Logic

Skills

Languages Business fluent in English. Elementary knowledge of Spanish and French.

Coding Java, Python, Bash, LaTeX

Misc. Academic teaching, Secure Coding

Miscellaneous Experience

CVE Entries

2019 **CVE-2019-13990**, XXE in Quartz Scheduler
CVSS 3.x Base Score: **9.8** Critical