

Eduard Hauck

ehauck.me | ehauck@pm.me

Education

- 2018 – PhD. Candidate in Cryptography, *Ruhr-Universität Bochum*
- Methods for (anonymous) authentication
 - Anonymous messaging
 - Security against large-scale adversaries
- 2015 – 2018 Master, Study of IT-Security, Ruhr-Universität Bochum
- Cryptography
 - Establishment of a management system for information security in accordance with DIN ISO/IEC 27001
 - Hacking Internship
- 2012 – 2015 Bachelor, Study of IT-Security, Ruhr-Universität Bochum
- 2004 – 2012 Abitur, Elisabeth-Langgässer Gymnasium Alzey
- 2009 – 2011 Choir director, C Prüfung, Institut für Kirchenmusik Mainz

Experience

- 2017– 2018 Research assistant, *Ruhr-Universität Bochum*
- Exercise correction
 - Conception and Deployment of the Dobbertin Challenge 2017
- 2016 – 2018 Team member 'Unverpackt', Enactus Ruhr-Universität Bochum
- 2016 Certification, SAP ERP Customizing
- 04/2015 – 09/2015 IT-Security Consultant, SEC Consult Unternehmensberatung Berlin
- Web application penetration testing

Publications

- | | |
|------|--|
| 2022 | ASIACRYPT 2022, Strongly Anonymous Ratcheted Key Exchange |
| 2021 | EUROCRYPT 2021, Analysing the HPKE Standard |
| 2020 | CRYPTO 2020, Lattice-Based Blind Signatures, Revisited |
| 2019 | EUROCRYPT 2019, A Modular Treatment of Blind Signatures from Identification Schemes |
| 2017 | eprint.iacr.org , Efficient and Universally Composable Protocols for Oblivious Transfer from the CDH Assumption |
-