

# Thomas Schneider

## Curriculum Vitae (Online Version)

Last changed: June 13, 2026

### Personal Data

born 1983/06 in Koblenz, Germany  
citizenship German  
family status married, one child (born 2016/06)  
web <https://thomaschneider.de>

### Work and Research Experience

- since 2018/03 **Full Professor**, *Cryptography and Privacy Engineering (ENCRYPTO)*, <https://encrypto.de>, Department of Computer Science, TU Darmstadt, Germany.
- 2013/02-2018/02 **Independent Research Group Leader**, *Head of the Engineering Cryptographic Protocols (ENCRYPTO) group*, <https://encrypto.de>, positive evaluation 2015/08, Department of Computer Science, TU Darmstadt, Germany.
- 2011/10-2018/02 **Claude Shannon Fellow**, *similar to DFG's Emmy Noether Program*, Center for Research in Security and Privacy (CRISP), previously European Center for Security and Privacy by Design (EC SPRIDE), TU Darmstadt, Germany.
- 2011/03-09 **Postdoctoral Researcher**, *System Security Lab (headed by Prof. Ahmad-Reza Sadeghi)*, Center for Advanced Security Research Darmstadt (CASED), TU Darmstadt, Germany.  
Worked in EU research project TLOUDS (see list of projects below).
- 2008/04-2011/02 **Doctoral Researcher**, *System Security Lab (headed by Prof. Ahmad-Reza Sadeghi)*, Horst-Görtz Institute for IT Security (HGI), Ruhr-University Bochum, Germany.  
Worked in EU research projects CACE, SPEED, and ECRYPT II (see list of projects below).
- 2007/06-11 **Research Intern**, *Nokia Bell Labs, Security Solutions/Cryptographic Systems*, Murray-Hill, NJ, USA.  
"Practical Secure Function Evaluation" advised by Dr. Vladimir Kolesnikov.
- 2006/06-09 **Student Research Assistant**, *Chair for Hardware-Software-Co-Design (headed by Prof. Jürgen Teich, supervised by Dr.-Ing. Dirk Koch)*, Department of Computer Science, Friedrich-Alexander University Erlangen-Nürnberg, Germany.  
VHDL programming in DFG project ReCoNets.
- 2002/09-2003/06 **Civilian Service**, *Information Center for Communication Assistance ELECOK*, Wichernhaus Altdorf, Germany.  
Website construction, network administration, PC maintenance, in-house training.
- 2000/08-09 **Intern**, *Lucent Technologies*, Nürnberg, Germany.  
Investigation for using FrontPage 2000 as Web editing and publishing tool for PC users publishing on UNIX (Netscape-)Web Servers.

### Research Projects (Running)

- 2025-2030 ERC Consolidator Grant 2023 Tools for Protecting Data and Function Privacy (PRIVTOOLS) funded by the European Research Council (ERC), principal investigator, <https://encrypto.de/PRIVTOOLS>

- 2014-2026 Collaborative Research Center Cryptography-Based Security Solutions (CROSSING) funded by the German Research Foundation (DFG), principal investigator and member of directorate responsible for equal opportunities: gender equality, family-friendliness and diversity; researchers from our project E4 won the CROSSING Collaboration Award in 2025/2024/2022/2019/2017/2016; <https://www.crossing.tu-darmstadt.de>
- 2026-2030 & 2019-2022 National Research Center for Applied Cybersecurity ATHENE funded by the German Federal Ministry of Research, Technology and Space (BMFTR, former BMBF) and the Hessen State Ministry for Higher Education, Research and the Arts (HMWK), principal investigator, <https://www.athene-center.de/en/>

### Research Projects (Finished)

- 2020-2025 ERC Starting Grant 2019 Privacy-preserving Services On The Internet (PSOTI) funded by the European Research Council (ERC), principal investigator, <https://encrypto.de/PSOTI>
- 2019-2024 Doctoral College Privacy and Trust for Mobile Users funded by the German Research Foundation (DFG), principal investigator and responsible for internationalization, <https://www.privacy-trust.tu-darmstadt.de>
- 2021-2023 Intel/Avast/VMware Private AI Collaborative Research Institute, Project "Engineering Private AI Systems (EPAI), principal investigator, <https://www.private-ai.org>
- 2015-2019 Center for Research in Security and Privacy CRISP funded by the German Federal Ministry of Education and Research (BMBF) and the Hessen State Ministry for Higher Education, Research and the Arts (HMWK), principal investigator, <https://crisp-da.de>
- 2013-2016 EU FP7 project Privacy-Preserving Computation in the Cloud (PRACTICE), principal investigator, <https://cordis.europa.eu/project/rcn/111030/factsheet/en>
- 2012-2016 Center for Advanced Security Research Darmstadt (CASED) funded by the Hessen State Ministry for Higher Education, Research and the Arts (HMWK), principal investigator, <https://proloewe.de/cased>
- 2011-2015 European Center for Security and Privacy by Design (EC SPRIDE) funded by the German Federal Ministry of Education and Research (BMBF), Claude Shannon fellow
- 2011 EU FP7 project Trustworthy Clouds (TLOUDS), <https://cordis.europa.eu/project/rcn/97862/factsheet/en>
- 2008-2013 European Network of Excellence in Cryptology (ECRYPT II), <https://cordis.europa.eu/project/rcn/85556/factsheet/en>
- 2008-2010 EU FP7 project Computer-Aided Cryptography Engineering (CACE), <https://cordis.europa.eu/project/rcn/85344/factsheet/en>
- 2008-2009 EU FP6 project Signal Processing in the EncryptEd Domain (SPEED), <https://cordis.europa.eu/project/rcn/80454/factsheet/en>

### Academic Self-Administration (selection)

- since 2015 CYSEC, Profile Area at TU Darmstadt; deputy coordinator (since 05/2026); principal investigator; member of steering board (2019-2020); member of management team (2015-2019): responsible for gender equality and Claude Shannon fellow research groups; <https://www.cysec.tu-darmstadt.de>
- 2025 Member of Selection Committee for Visiting Female Professor Programme at TU Darmstadt, [Link](#)
- since 10/2024 Member of PhD Board of CS Department at TU Darmstadt, [Link](#)
- 10/2023-09/2027 Member of Department Council of CS Department at TU Darmstadt: representative for IT Security, [Link](#)
- since 10/2019 Member of Study Commission of CS Department at TU Darmstadt, aka Commission for Improving Quality of Study Conditions and Teaching (QSL), [Link](#)

## Education

- 2008/04-2011/02 **Dr.-Ing. (PhD) in Security in Information Technology with distinction**,  
*Department of Electrical Engineering and Information Sciences, Ruhr-University Bochum, Germany.*  
Thesis: *Engineering Secure Two-Party Computation Protocols – Advances in Design, Optimization, and Applications of Efficient Secure Function Evaluation.*  
Advisor: Prof. Ahmad-Reza Sadeghi (Ruhr-University Bochum, now at TU Darmstadt); External referee: Prof. Benny Pinkas (Bar-Ilan University, Ramat Gan, Israel)
- 2003/10-2008/03 **Dipl.-Inf. (Univ.) (M.Sc. in Computer Science) with distinction (grade 1.0)**,  
*Department of Computer Science, Friedrich-Alexander University Erlangen-Nürnberg, Germany.*  
Focus on Theoretical Computer Science (Cryptography & Security), Hardware-Software-Co-Design, Programming Systems, and Technical Electronics. Minor field of studies in Electrical, Electronic and Communication Engineering.  
Diplomarbeit (Master thesis): *Practical Secure Function Evaluation.*  
Advisors: Dr. Vladimir Kolesnikov (Nokia Bell Labs, USA) and Prof. Volker Strehl (Friedrich-Alexander University Erlangen-Nürnberg)  
Studienarbeit (Bachelor thesis): *Secure Task Migration and Interprocess Communication in Reconfigurable, Distributed, Embedded Systems.*  
Advisors: Dr.-Ing. Dirk Koch and Prof. Jürgen Teich (Friedrich-Alexander University Erlangen-Nürnberg)
- 1993-2002 **Abitur (Baccalaureate) with distinction (grade 1.0)**, *Leibniz-Gymnasium Altdorf, Germany*,  
Leistungskurse (advanced classes): Mathematics and Physics, Facharbeit (Research Paper): *Computersimulation eines idealen Gases (Computer Simulation of an Ideal Gas).*

## Honors, Awards, and Scholarships

### Honors and Awards

- 2024 **Athene Prize for Good Teaching of the Department of Computer Science 2024** “for the practice-oriented restructuring of the first-semester course “Digital Technology” in the interest of the students” in WS23/24 awarded by the Carlo and Karin Giersch Foundation at TU Darmstadt
- 2024 **Runner-up Distinguished Paper Award 2. IEEE Conference on Secure and Trustworthy Machine Learning (SaTML’24)**, *ScionFL: Secure Quantized Aggregation for Federated Learning.*
- 2023 **ERC Consolidator Grant**, *Tools for Protecting Data and Function Privacy (PRIVTOOLS)*, funding volume 2 Mio EUR, success rate 14.5%.
- 2023 **Prize for Best Exercise at CS Department of TU Darmstadt in SS23** for our course Cryptographic Protocols (CRYPROT) awarded by the Student Association Computer Science
- 2021 **8. German IT-Security Award 2020: 2. Prize**, *Our submission “ContactGuard: Mobile Private Contact Discovery” won the 2. prize (60,000 EUR) among 46 submissions.*
- 2019 **ERC Starting Grant**, *Privacy-preserving Services On The Internet (PSOTI)*, funding volume 1.5 Mio EUR, success rate 13.1%.
- 2019 **Research Award by Intel Corporation**, for research on “Secure and Privacy Preserving AI Frameworks and Run-Times for Data Scientists and Service Providers”.
- 2019 **List position #3 for the W3 Professorship (Full Professor) in IT-Security with Focus on Practical Security Methods and -Systems**, *Karlsruhe Institute of Technology (KIT), Germany.*
- 2017 **Job offer (Ruf) for the W3 Professorship (Full Professor) in Security and Privacy**, *Albert-Ludwigs-University Freiburg, Germany, list position #1, declined.*
- 2017 **Job offer (Ruf) for the W2 Professorship (Associate Professor) in Information Security**, *Ruhr-University Bochum, Germany, list position #2, declined.*
- 2016 **Finalist 6. German IT-Security Award 2016**, *Our submission “Praktikable Private Schnittmengeberechnung” was among the 9 finalists chosen from 45 submissions.*
- 2012 **Intel Early Career Faculty Honor Program Award.**
- 2012 **Science Award for Junior Researchers by the Society for Data Protection and Data Security**, *Gesellschaft für Datenschutz und Datensicherheit e.V., GDD.*

- 2011 **Job offer (Ruf) for a W1 Professorship (Assistant Professor with tenure track) at Center for IT-Security, Privacy and Accountability (CISPA), Saarland University, Germany, declined.**
- 2011 **Finalist CAST Dissertation Award IT Security (CAST Promotionspreis IT-Sicherheit).**
- 2011 **Best Paper Award 12. Communications and Multimedia Security Conference (CMS'11), Twin Clouds: Secure Cloud Computing with Low Latency.**
- 2009 **Research School Section Days, poster prize, Ruhr-University Bochum.**
- 2008 **CAST B.Sc. Award IT Security: 4. Prize (CAST Förderpreis IT-Sicherheit, Kategorie Bachelor- und Studienarbeiten).**
- 2008 **Association for Software Quality and Further Education (ASQF), sponsorship award for excellent studies, Friedrich-Alexander University Erlangen-Nürnberg.**
- 2006 **Best Vordiplom (corresponds to B.Sc.), Department of Computer Science, Friedrich-Alexander University Erlangen-Nürnberg, book prize signed and awarded by Prof. Joseph Weizenbaum.**
- 2003 **21. German Informatics Contest (Bundeswettbewerb Informatik), finalist and laureate.**

### Scholarships

- 2008-2011 **Ruhr-University Bochum Research School, within framework of German excellence initiative.**
- 2007-2008 **Leonardo-Kolleg, outstanding students of Friedrich-Alexander University Erlangen-Nürnberg.**
- 2004-2008 **German Academic Scholarship Foundation (Studienstiftung des Deutschen Volkes), attended summer academy 2006 on "Security and Privacy in a Networked World" and annual conference North America 2007 in San Francisco.**
- 2003-2008 **Bavarian Elite Program (BayBFG).**

### Scientific Service

- Reviewer for ERC Starting, Consolidator, and Advanced Grants
- Reviewer for Dutch Research Council (NWO)
- Reviewer for German Research Foundation (DFG)
- Reviewer for Israel Science Foundation (ISF)
- Reviewer for Swiss National Science Foundation (SNF)
- Reviewer for Villum Foundation, Denmark
- External Reviewer for CAST Förderpreis IT-Sicherheit '19 '16 '14 (CAST IT Security Award)
- 2024 **Main Organizer 10. Theory and Practice of Multi-Party Computation Workshop (TPMPC'24) at TU Darmstadt together with ENCRYPTO group: 4 days, 162 participants, 12 invited talks, 25 contributed talks, 15 sessions, diversity panel, industry session, rump session, and guided tour; Link**
- since 2016 **Member of steering committee of TPMPC (Theory and Practice of Multi-Party Computation Workshops); Link**
- 2016 **Family Support Chair 16. Privacy Enhancing Technologies Symposium (PETS'16)**
- 2013 **Poster & Demo Co-Chair 20. ACM Conference on Computer and Communications Security (CCS'13)**
- 2013 **Publicity Co-Chair (technical strand) 6. International Conference on Trust & Trustworthy Computing (TRUST'13)**

### Program Committee Member

- ACM ASIACCS '18 '17 (ACM Asia Conference on Computer and Communications Security, CORE rank A)**
- ACM CCS '26 '24 '21 (ACM Conference on Computer and Communications Security, CORE rank A\*)**
- ACM CCSW '20 '19 '17 '16 '15 '14 (ACM Cloud Computing Security Workshop)
- ACM DRM '11 (ACM Workshop on Digital Rights Management, CORE rank C)

ACM IH&MMSEC '20 '19 '18 '17 '16 '15 '14 (ACM Workshop on Information Hiding & Multimedia Security, CORE rank C)

ACM STC '11 (ACM Workshop on Scalable Trusted Computing, CORE rank B)

ACNS '17 '16 (International Conference on Applied Cryptography and Network Security, CORE rank B)

CANS '18 '17 '12 (International Conference on Cryptology and Network Security, CORE rank B)

**CRYPTO '23** (Annual International Cryptology Conference, CORE rank A\*)

**EUROCRYPT '18 '16** (Annual International Conference on the Theory and Applications of Cryptographic Techniques, CORE rank A\*)

**FC '15 '14 '13** (International Conference on Financial Cryptography and Data Security, CORE rank A)

IEEE ICIP '20 '19 '18 '17 '16 '15 '14 (IEEE International Conference on Image Processing, CORE rank B)

**IEEE S&P '16** (IEEE Symposium on Security and Privacy, CORE rank A\*)

INDOCRYPT '17 (International Conference on Cryptology in India, CORE rank B)

**INTERSPEECH '23** (Conference of the International Speech Communication Association, CORE rank A)

**NDSS '21 '20** (Network & Distributed System Security Symposium, CORE rank A\*)

LATINCRYPT '25 (Cryptology and Information Security in Latin America)

PPML '19 (Privacy Preserving Machine Learning – CCS Workshop)

SECRYPT '23 (International Conference on Security and Cryptography, CORE rank C)

TPMPC '26 '25 '24 '23 '22 '20 '19 '18 (Theory and Practice of Multi-Party Computation Workshop)

TrustED '12 (International Workshop on Trustworthy Embedded Devices)

**USENIX Security '27 '26 '25 '23** (USENIX Security Symposium, CORE rank A\*)

WEWoRC '13 (Western European Workshop on Research in Cryptology)

WPES '20 (Workshop on Privacy in the Electronic Society)

### Reviewer for Journals

**ACM CSUR '24 '14** (ACM Computing Surveys, CORE rank A\*)

**ACM TOPS '17 '13** (ACM Transactions on Privacy and Security, CORE rank A)

AMC '15 (Advances in Mathematics and Communications)

Bioinformatics '19

CACM '13 (Communications of the ACM)

**COMPJ '12** (The Computer Journal, CORE rank A\*)

**DIST '17** (Distributed Computing, CORE rank A)

IEEE Signal Processing Magazine '12

**IEEE TC '17** (IEEE Transactions on Computers, CORE rank A\*)

**IEEE TDSC '26 '24 '19** (IEEE Transactions on Dependable and Secure Computing, CORE rank A\*)

**IEEE TIFS '25 '24 '23 '19 '18 '17 '16 '15 '14 '12 '11** (IEEE Transactions on Information Forensics and Security, CORE rank A)

**IEEE TIT '11** (IEEE Transactions on Information Theory, CORE rank A\*)

**IEEE TKDE '13** (IEEE Transactions on Knowledge and Data Engineering, CORE rank A)

**IEEE TMC '25 '16** (IEEE Transactions on Mobile Computing, CORE rank A\*)

IJIS '22 '13 (International Journal of Information Security, CORE rank C)

JCEN '19 (Journal of Cryptographic Engineering)

JCS '15 '12 (Journal of Computer Security, CORE rank B)

**JoC '25 '22 '18 '12 '10** (Journal of Cryptology, CORE rank A\*)

SCN '15 (Security and Communication Networks)

SECRYPT '23 (International Conference on Security and Cryptography, CORE rank C)

## External Reviewer

ACISP '16 (Australasian Conference on Information Security and Privacy)

**ACM ASIACCS '12** (ACM Information, Computer and Communications Security, CORE rank A)

**ACM CCS '19 '15 '14 '11** (ACM Computer and Communications Security, CORE rank A\*)

ACM CCSW '12 (ACM Cloud Computing Security Workshop)

ACM CODASPY '13 (ACM Conference on Data and Application Security and Privacy)

ACM IHI '12 (ACM SIGHT International Health Informatics Symposium)

ACM IH&MMSEC '13 (ACM Information Hiding and Multimedia Security, CORE rank C)

ACM STC '08 (ACM Scalable Trusted Computing, CORE rank B)

ACNS '11 '10 (Applied Cryptography and Network Security, CORE rank B)

**ASIACRYPT '09** (Theory and Application of Cryptology and Information Security, CORE rank A)

CARDIS '12 (Smart Card Research and Advanced Application)

**CRYPTO '19 '17 '16 '14 '12 '11** (Cryptology, CORE rank A\*)

**ESORICS '12 '11** (European Symposium on Research in Computer Security, CORE rank A)

**FC '21 '11 '10** (Financial Cryptography and Data Security, CORE rank A)

ICISC '10 '09 (International Conference on Information Security and Cryptology, CORE rank B)

**IEEE S&P '15** (IEEE Security and Privacy, CORE rank A\*)

IH '11 (Information Hiding, CORE rank C)

INTRUST '11 (International Conference on Trusted Systems)

IWSEC '10 (International Workshop on Security, CORE rank B)

**NDSS '14 '12** (Network & Distributed System Security Symposium, CORE rank A\*)

PST '12 (Privacy, Security and Trust, CORE rank C)

PKC '10 '09 (Public Key Cryptography, CORE rank B)

ReCoSoC '07 (Reconfigurable Communication-centric Systems on Chip)

RFIDSec '09 (RFID Security, CORE rank C)

RLCPS '10 (Real-Life Cryptographic Protocols and Standardization)

SDM '11 (Secure Data Management)

SPEED '09 (Signal Processing in the EncryptEd Domain)

TRUST '10 (Trust and Trustworthy Computing)

**USENIX Security '15** (USENIX Security Symposium, CORE rank A\*)

WISSEC '08 (Workshop on Information and System Security)

---

## Teaching Experience

2018/06-2023/08	<b>Higher Education Teaching Certificate - Professional Competence Level</b> of TU Darmstadt successfully completed: 200 units of work continuing education ( <a href="#">Link</a> )
since 2019 every winter term	<b>Lecture &amp; Exercise</b> , <i>Digitaltechnik</i> , <a href="https://encrypto.de/DT">https://encrypto.de/DT</a> , 800+ first semester Bachelor students, TU Darmstadt, Germany. Athene Prize for Good Teaching 2024 in WS23/24 (see Honors and Awards above)
since 2018 every summer term	<b>Lecture &amp; Exercise</b> , <i>Cryptographic Protocols (CRYPROT)</i> , <a href="https://encrypto.de/CRYPROT">https://encrypto.de/CRYPROT</a> , TU Darmstadt, Germany. Prize for Best Exercise at CS Department of TU Darmstadt in SS23 (see Honors and Awards above)
since 2018 once per year	<b>(Project) Lab</b> , <i>Development for Protecting Privacy (PRIVDEV)</i> , <a href="https://encrypto.de/PRIVDEV">https://encrypto.de/PRIVDEV</a> , TU Darmstadt, Germany.

- since 2018 every term **Advanced Seminar**, *Cryptography and Privacy Engineering (ENCRYPTO)*, <https://encrypto.de/OS-ENCRYPTO>, TU Darmstadt, Germany.
- 2016/03 **Invited Lecture Series**, *21st Estonian Winter School in Computer Science (EWSCS)*, Palmse, Estonia, Title: Practical Secure Two-party Computation and Applications.
- 2015-2023 every winter term **Seminar**, *Privacy Preserving Technologies (PRIVTECH)*, <https://encrypto.de/PRIVTECH>, TU Darmstadt, Germany.
- 2011 **Lecturer**, *Center for Advanced Security Research Darmstadt (CASED)*, TU Darmstadt, Germany, PhD Seminar (co-organized with Prof. Ahmad-Reza Sadeghi and Prof. Michael Waidner).
- 2008/04-2011/02 **Teaching Assistant**, *System Security Lab, Horst-Görtz Institute for IT Security*, Ruhr-University Bochum, Germany, lecture units and exercises on “Secure Computation”, supervised several theses (see below) and seminar works.
- WS 2007/2008 **Student Teaching Assistant**, *Department of Computer Science - Computer Networks and Communication Systems*, Friedrich-Alexander University Erlangen-Nürnberg, exercises on “Network Security”; lectures given by PD Dr.-Ing. habil. Falko Dressler.
- WS 2006/2007 **Student Teaching Assistant**, *Department of Computer Science - Pattern Recognition*, Friedrich-Alexander University Erlangen-Nürnberg, exercises on “Theoretical Computer Science 3 - Complexity of Algorithms”; lectures given by Prof. Volker Strehl.
- 2005 **Trainer** in one-week course about youth group leading.
- 1998-2008 **Private Tutor** for mathematics and physics (classes 5-13).

### PostDocs

- since 2024/11 **Protik Kumar Paul**, *previously PhD with Arpita Patra at Indian Institute of Science (IISc) Bangalore.*
- since 2024/04 **Kasra EdalatNejad**, *previously PhD with Carmela Troncoso at École Polytechnique Fédérale de Lausanne (EPFL), CROSSING Collaboration Awards 2025 & 2024.*
- 2024/01-08 **Nishat Koti**, *previously PhD with Arpita Patra at Indian Institute of Science (IISc) Bangalore; since 2024 Cryptography Researcher at Aztec Labs.*
- 2021/10-2023/03 **Ajith Suresh**, *previously PhD with Arpita Patra at Indian Institute of Science (IISc) Bangalore; since 2023 Lead MPC Researcher at Technology Innovation Institute (TII), Abu Dhabi.*
- 2021/09-2022/02 **Christian Weinert**, *see PhD Students below.*
- 2018/11-2019/10 **Daniel Demmler**, *see PhD Students below.*

### PhD Students

- since 2025/06 **Maximilian Stillger**, *PhD applicant, Working Title: TBD.*
- since 2024/10 **Jan Filipp**, *PhD applicant, Working Title: TBD.*
- since 2022/12 **Nora Khayata**, *PhD applicant, Working Title: TBD.*
- since 2022/06 **Andreas Brüggemann**, *PhD applicant, Working Title: TBD, Contributed talks at TPMPC'25 and TPMPC'26; PC member ASIACRYPT'26.*
- 2021/01-2025/12 **Gowri R Chandran**, *PhD, Inputs, Outputs, and the Computations in Between: Leakage-Resilient Privacy-Preserving Protocols, CROSSING Collaboration Award 2024; since 2026 Postdoc at Simula Research Laboratory, Norway.*
- 2019/12-2025/01 **Daniel Günther**, *PhD, Towards Practical Secure Computation: Exploring Applicability and Privacy Trade-offs, CROSSING Collaboration Award 2022; now Information Security Risk Manager at illwerke vkw, Austria.*

- 2019/06-2024/09 **Hossein Yalame**, *PhD*, Advancing MPC: From Real-World Applications to LUT-Based Protocols, Science Award for Junior Researchers 2024 by Society for Data Protection and Data Security (GDD); Finalist CAST/GI Dissertation Award IT-Security 2025; Among top 11 candidates for Academics.de Junior Researcher of the Year 2025; since 2023 Scientific Researcher at Bosch Research.
- 2019/11-2023/10 **Helen Möllering**, *PhD*, Towards Practical Privacy-Preserving Clustering and Health Care Data Analyses, Contributed talk at CrossFyre@Eurocrypt'23; 2023-2026 Senior Associate and Junior Engagement Manager at McKinsey & Company; since 2026 Cyber and Information Risk Manager at Allianz.
- 2018/07-2022/11 **Amos Treiber**, *PhD*, Analyzing and Applying Cryptographic Mechanisms to Protect Privacy in Applications, contributed talks at RWC'22 and TPMPC'20; since 2023 (Cryptography) Development Engineer at Rohde & Schwarz Cybersecurity.
- 2017/10-2022/06 **Oleksandr Tkachenko**, *PhD*, Towards Deployable MPC: Flexible and Efficient Tools for Real-World Applications, PC member PPML@CCS'21; 2022-2026 Senior Software Engineer at DFINITY.
- 2016/09-2021/08 **Christian Weinert**, *PhD*, Practical Private Set Intersection Protocols for Privacy-Preserving Applications, Winner of 8. German IT-Security Award 2020 (2. place), Prize for best dissertation at the CS department of TU Darmstadt in 2021 by "Friends of TU Darmstadt e.V.", Finalist CAST/GI Dissertation Award IT-Security 2022, CROSSING Collaboration Award 2017; PC member of ICML'22 and PPML@CCS'21; since 2022 Lecturer and since 2026 Associate Professor for Information Security at Royal Holloway University of London (RHUL), UK.
- 2015/02-2020/09 **Ágnes Kiss**, *PhD*, Efficient Private Function Evaluation, invited to Heidelberg Laureate Forum 2018; Winner of CROSSING Collaboration Award 2019; PC member PPML@CCS'19; 2020-2023 Postdoc at CISPA; since 2023 Cryptography Engineer at Sine Foundation.
- 2013/10-2018/11 **Daniel Demmler**, *PhD*, Towards Practical Privacy-Preserving Protocols, Winner of CAST/GI Dissertation Award IT Security 2020, Best dissertation at the CS department of TU Darmstadt in 2018 by "Friends of TU Darmstadt e.V."; CROSSING Collaboration Awards 2017 & 2016; Contributed talk at TPMPC'18; 2019-2022 Postdoc at University of Hamburg; since 2022 at Zama, now MPC Team Director.
- 2012/07-2016/12 **Michael Zohner**, *PhD*, Faster Oblivious Transfer Extension and its Impact on Secure Computation, CROSSING Collaboration Award 2016; 2017-2021 Project Security & Privacy Manager at Continental; since 2021 Professor for IT-Security at University of Applied Sciences Fulda.

### Research Assistants

- 2020/08-2023/07 **Raine Nieminen**, *M.Sc.*.
- 2020/01-10 **Marco Holz**, *M.Sc.*.
- 2013/11-2014/02 **Kai Samelin**, *M.Sc.*.

### Internal Referee for PhD Theses

I was member of 62 internal PhD committees at TU Darmstadt and wrote evaluation letters for the following candidates.

- 2025 **Marco Chilese**, *PhD*, Recent Topics in IT-Security and Applications of Deep Learning, TU Darmstadt; with Prof. Kristian Kersting.
- 2022 **Patrick Struck**, *PhD*, Security of Cryptographic Primitives in Advanced Security Notions, TU Darmstadt; supervisor: Prof. Juliane Krämer.
- 2019 **Heng Zhang**, *PhD*, On the Effective Use of Data Dependency for Reliable Cloud Service Monitoring, TU Darmstadt; supervisor: Prof. Neeraj Suri.

### External Referee for PhD Theses

- 2026 **Aron van Baarsen**, *PhD*, Scalable Cryptographic Protocols with Financial Applications, Leiden University, The Netherlands; supervisors: Prof. Ronald Cramer and Dr.ir. Marc Stevens.

- 2026 **Andes Y. L. Kei**, *PhD*, Practical Secure Multiparty Computation for Transformers and Lookup Protocols, The Chinese University of Hong Kong, Hong Kong; supervisor: Prof. Sherman Chow.
- 2025 **Eric Pohle**, *PhD*, On Multi-Party Thresholdized Block Ciphers and Applications, KU Leuven, Belgium; supervisors: Prof. Bart Preneel and Aysajan Abidin, PhD.
- 2024 **Mariana Botelho da Gama**, *PhD*, MPC in the Real World: Practical Aspects of Multi-Party Computation, KU Leuven, Belgium; supervisor: Prof. Nigel Smart.
- 2024 **Roman Walch**, *PhD*, Improving Efficient Computation on Private Data, TU Graz, Austria; supervisor: Prof. Christian Rechberger.
- 2023 **Alberto Ibarondo**, *PhD*, Privacy-preserving Biometric Systems with Advanced Cryptographic Techniques, EURECOM, France; supervisors: Prof. Melek Önen and Prof. Hervé Chabanne.
- 2022 **Younes Talibi Alaoui**, *PhD*, Financial Applications for MPC, KU Leuven, Belgium; supervisor: Prof. Nigel Smart.
- 2022 **Ivan Oleynikov**, *PhD applicant*, Server-Aided Privacy-Preserving Proximity Testing, Discussion leader at licentiate seminar; Chalmers University of Technology, Gothenburg, Sweden; supervisor: Prof. Andrei Sabelfeld.
- 2019 **Mark Simkin**, *PhD*, Alice, Bits, and Bob, University of Aarhus, Denmark; supervisor: Prof. Ivan Damgård.
- 2019 **Tim Wood**, *PhD*, Reducing Communication Costs in Multi-Party Computation, KU Leuven, Belgium; supervisor: Prof. Nigel Smart.
- 2017 **Per Hallgren**, *PhD*, Provable Privacy for Location-Based Services, Chalmers University of Technology, Gothenburg, Sweden; supervisor: Prof. Andrei Sabelfeld.
- 2016 **Carsten Baum**, *PhD*, Towards More Efficient Secure Multiparty Computation in the Preprocessing Model, University of Aarhus, Denmark; supervisor: Prof. Ivan Damgård.
- 2016 **Rasmus Winther Zakarias**, *PhD*, Practical Secure Computation with Pre-Processing, University of Aarhus, Denmark; supervisor: Prof. Ivan Damgård.
- 2015 **Tore Kasper Frederiksen**, *PhD*, The Hitchhiker's Guide to Garbled Circuits: Garbled Circuits and their Applications to Maliciously Secure Two-Party Protocols, University of Aarhus, Denmark; supervisor: Prof. Jesper Buus Nielsen.
- 2014 **Ayman Jarrous**, *PhD*, Applied Secure Multi-Party Computation, University of Haifa, Israel; supervisor: Prof. Benny Pinkas.

### Master Theses

- since 2026 **Enea Pane**, *M.Sc.*, Graph Reinforcement Learning for the MPC Protocol Mixing Problem, co-supervised with Nora Khayata.
- since 2026 **Sascha Hoffmann**, *M.Sc.*, Accelerating Private Function Evaluation with a RAM Computation Model, co-supervised with Jan Filipp.
- since 2025 **Magnus Wilhelm**, *M.Sc.*, vMPC: Tool to visualize Multi-Party Computation, co-supervised with Maximilian Stillger.
- 2025-2026 **Tobias Schnitzler**, *M.Sc.*, Federated Secure Computation of Differentially Private Inner Products, co-supervised with Gowri R Chandran.
- 2025 **Joachim Schmidt**, *M.Sc.*, Improving the Efficiency of Multi-Party Computation Protocol Assignment using Neural Networks, co-supervised with Nora Khayata.  
Results published at **USENIX Security'26**; nominated by TUDA's CS department for best Master's thesis award by Fakultätentag Informatik (FTI)
- 2025 **Maximilian Stillger**, *M.Sc.*, LORELEI: Locally Rewriting Logic with Ensemble Improvements, co-supervised with Andreas Brüggemann.  
2. Prize CAST M.Sc. Award IT Security 2025

- 2022-2025 **Lennart Friesecke**, *M.Sc.*, Private-Files: Improved Privacy for Cloud-based File Storages, co-supervised with Gowri R Chandran.
- 2023-2024 **Tamino Goldan**, *M.Sc.*, Privacy-Preserving Online Forms, co-supervised with Andreas Brüggemann and Hossein Yalame.  
Results published as poster at ACSAC'24
- 2023-2024 **Robin William Hundt**, *M.Sc.*, SEEC: Memory-Efficient MPC for Large Circuits, co-supervised with Nora Khayata.  
results published at **ASIACCS'25** and presented as contributed talk at TPMPC'24
- 2022-2023 **Patrick Ehrler**, *M.Sc.*, Using Query Estimators for Attacking Relational Encrypted Search, co-supervised with Amos Treiber and Abdelkarim Kati.  
Results published at CCSW'24
- 2022-2023 **Laura Hetz**, *M.Sc.*, Communication-Efficient Privacy-Preserving Mobile Contact Discovery, co-supervised with Dr.-Ing. Christian Weinert.  
1. Prize CAST M.Sc. Award IT Security 2023 and 1. Prize Frauen-MINT-Award 2023; results published at **ESORICS'23**
- 2021-2023 **Dominique Dittert**, *M.Sc.*, Quantifying and Evaluating Susceptibility to Leakage Attacks against Encrypted Keyword Search, co-supervised with Amos Treiber.  
Results published at CCSW'23
- 2022 **Liang Zhao**, *M.Sc.*, Securely Realizing Output Privacy in MPC using Differential Privacy, co-supervised with Helen Möllering and Oleksandr Tkachenko.  
Results published at ARES'24
- 2022 **Lukas Scheidel**, *M.Sc.*, Outsourced Sublinear Private Decision Tree Evaluation, co-supervised with Amos Treiber.
- 2022 **Hannah Keller**, *M.Sc.*, Understanding Privacy Leakage from Independently Computed Statistics, co-supervised with Prof. Adam Smith and Helen Möllering.
- 2022 **Nora Khayata**, *M.Sc.*, Flexible File Format and Intermediate Representation for Secure Multi-Party Computation, co-supervised with Oleksandr Tkachenko and Lennart Braun.  
Award for excellent M.Sc. thesis by "Friends of TU Darmstadt e.V." 2022; results published at **ASIACCS'23** and presented as contributed talk at TPMPC'23
- 2021-2022 **Michael Yonli**, *M.Sc.*, Efficient MPC via Multi-Party Homomorphic Encryption, co-supervised with Hossein Yalame.  
Results published at SECRYPT'23 and presented as poster at FHE.org'23
- 2021-2022 **Niklas Schwabe**, *M.Sc.*, Efficient Multi-Party Private Function Evaluation for Depth-optimized Circuits, co-supervised with Daniel Günther.
- 2021 **Arthur Wigandt**, *M.Sc.*, Private Function Evaluation for Multi-Input Gates, co-supervised with Prof. Yann Disser and Daniel Günther.  
Results published at **ASIACRYPT'23**
- 2020-2021 **Jean-Pierre Münch**, *M.Sc.*, Accelerating Multi-Party Computation with Vectorized AES Instructions, co-supervised with Hossein Yalame.  
Results published at **ACSAC'21**
- 2020-2021 **Maurice Heymann**, *M.Sc.*, Accelerating Multi-Server Private Information Retrieval using GPUs, co-supervised with Daniel Günther.  
Results published at **USENIX Security'22**
- 2020 **Lennart Braun**, *M.Sc.*, A Generic Hybrid 2PC Framework with Application to Private Inference of Unmodified Neural Networks, co-supervised with Rosario Cammarota, Ph.D..  
Results published as poster at PriML@NeurIPS'21
- 2019 **Daniel Günther**, *M.Sc.*, Optimizing Private Information Retrieval for Compromised Credential Checking, co-supervised with Prof. Benny Pinkas.  
1. Prize CAST M.Sc. Award IT Security 2020; results published at **USENIX Security'22**

- 2018-2019 **Marco Holz**, *M.Sc.*, A Systematic Comparison of HE-based Private Function Evaluation Protocols, co-supervised with Ágnes Kiss.  
Results published at **ESORICS'20**
- 2018-2019 **Susanne Felsen**, *M.Sc.*, Secure Two-Party Computation: ABY versus Intel SGX, co-supervised with Christian Weinert.  
Results published at CCSW'19
- 2017-2018 **Matthias Senker**, *M.Sc.*, PSI meets Signal: Integrating a Malicious-Secure Private Contact Discovery Solution in an Open-Source Instant Messaging Service, co-supervised with Christian Weinert. Winner of 8. German IT-Security Award 2020 (2. place) and award for excellent M.Sc. thesis by "Friends of TU Darmstadt e.V." 2019; results published at **USENIX Security'19**
- 2017-2018 **Masaud Y. Alhassan**, *M.Sc.*, Improving Scalability of Universal Circuits for Large-Scale Private Function Evaluation, co-supervised with Ágnes Kiss.  
Results published in **Journal of Cryptology'19**
- 2017-2018 **Taha Tariq**, *M.Sc.*, Web Application for Privacy-Preserving Assignments, co-supervised with Ágnes Kiss.
- 2017 **Oleksandr Tkachenko**, *M.Sc.*, Large-Scale Privacy-Preserving Statistical Computations for Distributed Genome-Wide Association Studies, co-supervised with Christian Weinert and Prof. Kay Hamacher.  
Results published at **ASIACCS'18** and presented at 29. Kryptotag
- 2012-2013 **Daniel Demmler**, *M.Sc.*, Hardware-Assisted Two-Party Secure Computation on Mobile Devices, co-supervised with Michael Zohner.  
Results published at **USENIX Security'14** and presented at 19. Kryptotag
- 2008-2009 **Annika Paus**, *M.Sc.*, Special Aspects of Secure Function Evaluation with Private Functions, examiner: Prof. Ahmad-Reza Sadeghi (Ruhr-University Bochum, Germany) and Prof. Benny Pinkas (University of Haifa, Israel).  
Finalist CAST M.Sc. Award IT Security 2009; results published at ACNS'09 and WIFS'09

### Bachelor Theses

- since 2026 **Alexander Sachs**, *M.Sc.*, Enhancing UI/UX of Encrypted Multi-Channel Communication, co-supervised with Kasra EdalatNejad.
- since 2025 **Magnus Wilhelm**, *B.Sc.*, vMPC: Tool to visualize Multi-Party Computation, co-supervised by Maximilian Stillger and Andreas Brüggemann.
- 2025-2026 **Finn Schubert**, *B.Sc.*, Leakage Preservation in a Minimalistic Model Compiler, co-supervised with Nora Khayata.
- 2025-2026 **Simon Brunnauer**, *B.Sc.*, Framework for Scalable and Flexible Private Message-Passing-Style Graph Analysis, co-supervised with Andreas Brüggemann.
- 2025 **Henri Dohmen**, *B.Sc.*, libmasking: A Library for Leakage-Resilient Cryptography, co-supervised with Nora Khayata and Maximilian Orlt.
- 2024 **Thanh Long David Nguyen**, *B.Sc.*, Information Extraction Attacks on Private Kidney Exchange (and Beyond), co-supervised with Andreas Brüggemann and Helen Möllering.
- 2022-2023 **Tobias Wehrle**, *B.Sc.*, Defenses against Data Poisoning Attacks on Private Machine Learning Training, co-supervised with Hossein Yalame.  
Results published at **CHES'26** and DLSP'23
- 2022-2023 **Felix Marx**, *B.Sc.*, Framework for Secure and Private Hierarchical Federated Learning, co-supervised with Hossein Yalame.  
Results published at **CHES'26** and DLSP'23
- 2021-2022 **Joachim Schmidt**, *B.Sc.*, Framework for flexible LUT-based Semi-Private Function Evaluation, co-supervised with Daniel Günther.  
Results published at **ACSAC'24**

- 2021-2022 **Maximilian Stillger**, *B.Sc.*, Private Function Evaluation for Multi In- and Output-Gate Circuits, co-supervised with Daniel Günther.  
Results published at **ASIACRYPT'23**
- 2021-2022 **Timm Birka**, *B.Sc.*, Efficient and Practical Privacy-Preserving Kidney Exchange Protocol, co-supervised with Prof. Kay Hamacher, Tobias Kussel, and Helen Möllering.  
Results published at BMC Medical Informatics and Decision Making'22 and presented at 33. Kryptotag
- 2021 **Roman Hergenreder**, *B.Sc.*, Privacy-Preserving Household Finance Analytics, co-supervised with Christian Weinert.
- 2021 **Felix Wiegand**, *B.Sc.*, Combining Multi-Server and Single-Server Private Information Retrieval for Epidemiological Modelling, co-supervised with Daniel Günther.  
Results published as poster at CCS'21
- 2021 **Christopher van der Beets**, *B.Sc.*, Client-Server Privacy-Preserving Indoor Localization with Secret Sharing, co-supervised with Raine Nieminen.  
Results published at SECRYPT'22
- 2020 **Tim Heldmann**, *B.Sc.*, LLVM-based Circuit Compilation for Practical Secure Computation, co-supervised with Christian Weinert and Oleksandr Tkachenko.  
Results published at ACNS'21
- 2019 **Tom Schuster**, *B.Sc.*, Optimizing HyCC with Compiler IR, co-supervised with Christian Weinert.  
Results published at SECRYPT'21
- 2019 **Martin Kromm**, *B.Sc.*, PPSolv - A System for Privacy-Preserving Solvency Verification, co-supervised with Ágnes Kiss.
- 2018 **Robert Nikolai Reith**, *B.Sc.*, Silently Learning your Support Vector Machines Models, co-supervised with Oleksandr Tkachenko.  
Results published at WPES'19
- 2017-2018 **Oliver Schick**, *B.Sc.*, Web Application for Privacy-Preserving Scheduling, co-supervised with Ágnes Kiss.  
Results published at SECRYPT'19 and presented as poster at USENIX Security'18
- 2016-2017 **Daniel Günther**, *B.Sc.*, Valiant's Universal Circuit - Towards a Modular Construction and Implementation, co-supervised with Ágnes Kiss.  
1. Prize CAST B.Sc. Award IT Security 2018; results published at **ASIACRYPT'17** and in **Journal of Cryptology'19**
- 2016 **Nils Schroth**, *B.Sc.*, Demonstrator for Privacy-Preserving Face Recognition, co-supervised with Daniel Demmler.
- 2016 **Julian Götz Bieber**, *B.Sc.*, Generalizing Semi-Private Function Evaluation, co-supervised with Ágnes Kiss.
- 2016 **Marco Holz**, *B.Sc.*, Effective Protection of Sensitive Metadata in Online Communication Networks, co-supervised with Daniel Demmler.  
Results published at ACNS'17
- 2013-2014 **Benedikt Hiemenz**, *B.Sc.*, Analysis and Extensions of the PCF Secure Two-Party Computation Compiler, co-supervised with Daniel Demmler.
- 2009-2011 **Immo Wehrenberg**, *Studienarbeit (corresponds to B.Sc.)*, Design, Implementation, and Evaluation of a System for Efficient Privacy-Preserving Face Recognition, examiner: Prof. Ahmad-Reza Sadeghi.  
Results published at **CCS'10** and ICISC'09

### Student Assistants

- 2009-2011 **Stefan Kögl**, *Computer Aided Cryptography Engineering (CACE)*, professional practical trainee and student assistant.  
Results published at **CCS'10**

- 2009-2011 **Immo Wehrenberg**, *Design, Implementation, and Evaluation of a System for Efficient Privacy-Preserving Face Recognition*, student assistant and Studienarbeit (corresponds to B.Sc.).  
Results published at **CCS'10** and ICISC'09
- 2008-2009 **Wilko Henecka**, *Computer Aided Cryptography Engineering (CACE)*, student assistant.  
Results published at **CCS'10**, **ESORICS'10**, and EUROPKI'09; contributed to many other publications on zero-knowledge and secure function evaluation

## Long-term Visitors

- 2025/10-2026/03 **Lorenzo Bunaj**, research intern, Politecnico di Torino, Italy.
- 2025/03-12 **Olta Bytyçi**, research intern for B.Sc. thesis, Eötvös Loránd University, Budapest, Hungary.  
Results published at Decrypting Diversity Summit'25
- 2023/05-2024/01 **Huan-Chih Wang, M.Sc.**, visiting researcher during PhD, National Taiwan University, Taipei City, Taiwan.  
Results published at WPES'25
- 2023/05-07 **Shreyansh Narayan Maruvada**, research intern, Indian Institute of Information Technology, Agartala, India.
- 2022/09-2023/02 **Abdelkarim Kati, M.Sc.**, visiting researcher during PhD, Mohammed-VI Polytechnic University, Morocco.  
Results published at CCSW'24
- 2020/05-07 **Aditya Hedge**, research intern, Indian Institute of Information Technology (IIIT), Bangalore, India.  
Results published at **PoPETS'21**
- 2020/05-07 **Shreya Sharma**, research intern, Indian Institute of Technology (BHU) Varanasi, India.
- 2020/04-05 **Deepak Kumaraswamy**, research intern, National Institute of Technology Karnataka (NITK), India.
- 2019/11 **Ajith Suresh, M.Tech.**, visiting researcher during PhD, Indian Institute of Science (IISc), Bangalore, India.  
Results published at **USENIX Security'21** and HOST'21
- 2019/05-07 **Deevashwer Rathee**, research intern, Indian Institute of Technology (BHU), Varanasi, India.  
Results published at **ESORICS'20**, ACNS'20, and CANS'19
- 2017/10-11 **Zheng Yang, PhD**, *Location Privacy*, visiting researcher as postdoc, University of Helsinki, Finland.  
Results published at EuroS&P'19, CANS'18, and ICL-GNSS'18
- 2016 **Roberto Trifiletti, M.Sc.**, *Actively Secure Computation with Precomputations*, multiple research visits as part of the PhD program, University of Aarhus, Denmark.  
Results published at **NDSS'17**
- 2015 **Masoud Naderpour, B.Sc.**, *Privacy-Preserving Machine Learning*, Erasmus+ trainee, University of Turku, Finland.  
Results published at **PoPETS'19**

## Personal

- languages German (native), English (fluent), French (basic)
- member Association for Computing Machinery (ACM)  
Deutscher Hochschulverband (DHV)  
Gesellschaft für Informatik e.V. (GI)  
International Association for Cryptologic Research (IACR)

## Professional Skills

- programming Assembler, C, C++, Java, Maple, Octave, Perl, Python, Scheme, Shell, Turbo Pascal, Visual Basic

web Apache, JavaScript, MySQL, PHP, (X)HTML  
misc L<sup>A</sup>T<sub>E</sub>X, Microsoft Office, UML, VHDL, SystemVerilog  
operating Mac, Linux, Windows  
systems

## Interests

**music** vocals (baritone), tenor saxophone, electronic wind instrument (EWI), flute, cajon  
since 2023 Band Holyphon, St. Jakobus, Darmstadt Kranichstein: vocals, tenor saxophone, EWI  
since 2011 Kantorei St. Elisabeth, Darmstadt Martinsviertel: vocals (tenor)  
2008-2011 Katholische Hochschulgemeinde Bochum: vocals, cajon  
2006-2008 Katholische Hochschulgemeinde Erlangen: vocals, flute  
1996-2008 Stilbruch: Jugendchor und -band der kath. Pfarrei Winkelhaid-Burgthann: vocals, flute  
1995-2007 Blasorchester Markt Feucht: flute, tenor saxophone  
1995-2002 Bigband des Leibniz-Gymnasiums Altdorf: tenor saxophone

**sports** jogging, cycling, inline skating, juggling  
1992-2000 table tennis

**youth work** Honorary Associate in Youth Work, Catholic Parish Winkelhaid-Burgthann  
2002-2011 Technical coordinator of web team, <http://www.kapfwibu.de>  
2005 Teacher in course about youth group leading  
1998-2005 Tutor in several youth camps, ministrant  
2002-2003 Representative of youth work (Pfarrjugendleiter)  
2001-2002 Leader of youth group (14-16 year old teenagers)  
1998-2001 Leader of youth group (6-10 year old children)  
1998-2004 Participant in courses about youth group leading

---

## List of Publications

Publications in cryptography usually order authors alphabetically and conferences are more common than journals. We publish our results in top venues for applied cryptography and privacy such as ACM CCS, EUROCRYPT, IEEE S&P, Journal of Cryptology, NDSS, and USENIX Security. Top venues with CORE ranking A\* or A are marked in **bold**.

See <https://thomaschneider.de/pubs> for details on the publications.

Google Scholar: <https://scholar.google.com/citations?user=E31PR1oAAAAJ>

Semantic Scholar: <https://www.semanticscholar.org/author/145139628>

DBLP: [https://dblp.uni-trier.de/pers/hd/s/Schneider\\_0003:Thomas.html](https://dblp.uni-trier.de/pers/hd/s/Schneider_0003:Thomas.html)

ORCID: <https://orcid.org/0000-0001-8090-1316>

## Journal Articles (all peer reviewed)

- 1) F. Marx, T. Schneider, A. Suresh, T. Wehrle, C. Weinert, and H. Yalame, WW-FL: Secure and Private Large-Scale Federated Learning. ***IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES)***, vol. 2026, no. 1, pp. 185–224, Antalya, Türkiye, January 16, 2026. Full version: <https://arxiv.org/abs/2302.09904>. CORE rank A. doi:10.46586/tches.v2026.i1.185-224.
- 2) A. Patra, J. Schmidt, T. Schneider, A. Suresh, and H. Yalame, SynCirc: Efficient Synthesis of Depth-Optimized Circuits from High-Level Languages. ***IEEE Transactions on Computers (TC)***, vol. 75, no. 6, pp. 2200–2211, March 16, 2026. Online: <https://ia.cr/2026/561>. Code: <https://encrypto.de/code/SynCirc>. CORE rank A\*. doi:10.1109/TC.2026.3673169.
- 3) A. Brüggemann, N. Koti, V. B. Kukkala, and T. Schneider, MultiCent: Secure and Scalable Computation of Centrality Measures on Multilayer Graphs. ***Proceedings on Privacy Enhancing Technolo-***

- gies (PoPETs)*, vol. 2025, no. 4, pp. 944–968, Washington DC, USA & online, July 2025. Online: <https://ia.cr/2025/652>. Code: <https://encrypto.de/code/MultiCent> (Artifact Reproduced Badge). Acceptance rate 25.7%. CORE rank A. doi:10.56553/popets-2025-0166.
- 4) D. Günther, M. Holz, B. Judkewitz, H. Möllering, B. Pinkas, T. Schneider, and A. Suresh, Privacy-Preserving Epidemiological Modeling on Mobile Graphs. *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 20, no. 2, pp. 3088–3101, February 28, 2025. Online: <https://ia.cr/2020/1546>. Code: <https://encrypto.de/code/RIPPLE>. CORE rank A. doi:10.1109/TIFS.2025.3546850.
  - 5) T. Reinhold, P. Kühn, D. Günther, T. Schneider, and C. Reuter, ExTRUST: Reducing Exploit Stockpiles with a Privacy-Preserving Depletion System for Inter-State Relationships. *IEEE Transactions on Technology and Society*, vol. 4, no. 2, pp. 158–170, May 29, 2023. Online: <http://arxiv.org/abs/2306.00589>. doi:10.1109/TTS.2023.3280356.
  - 6) R. Nieminen and T. Schneider, Breaking and Fixing Garbled Circuits when a Gate has Duplicate Input Wires. *Journal of Cryptology (JoC)*, vol. 36, no. 4, August 3, 2023. Part of Topical Collection on Computing on Encrypted Data. Online: <https://ia.cr/2023/530>. CORE rank A\*. doi:10.1007/s00145-023-09472-4.
  - 7) C. Hagen, C. Weinert, C. Sendner, A. Dmitrienko, and T. Schneider, Contact Discovery in Mobile Messengers: Low-Cost Attacks, Quantitative Analyses, and Efficient Mitigations. *ACM Transactions on Privacy and Security (TOPS)*, vol. 26, no. 1, pp. 1–44, February, 2023. Online: <https://ia.cr/2022/875>. Code: <https://github.com/contact-discovery>. CORE rank A. doi:10.1145/3546191.
  - 8) T. Schneider, A. Suresh, and H. Yalame, Comments on “Privacy-Enhanced Federated Learning Against Poisoning Adversaries”. *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 18, pp. 1407–1409, January 20, 2023. CORE rank A. doi:10.1109/TIFS.2023.3238544.
  - 9) T. Birka, K. Hamacher, T. Kussel, H. Möllering, and T. Schneider, SPIKE: Secure and Private Investigation of the Kidney Exchange problem. *BMC Medical Informatics and Decision Making*, vol. 22, no. 1, p. 253, September 22, 2022. Online: <https://arxiv.org/abs/2204.09937>. Code: <https://encrypto.de/code/PPKE>. CORE rank B. doi:10.1186/s12911-022-01994-4.
  - 10) L. Braun, D. Demmler, T. Schneider, and O. Tkachenko, MOTION – A Framework for Mixed-Protocol Multi-Party Computation. *ACM Transactions on Privacy and Security (TOPS)*, vol. 25, no. 2, pp. 8:1–8:35, March 4, 2022. Online: <https://ia.cr/2020/1137>. Code: <https://encrypto.de/code/MOTION>. CORE rank A. doi:10.1145/3490390.
  - 11) A. Hegde, H. Möllering, T. Schneider, and H. Yalame, SoK: Efficient Privacy-Preserving Clustering. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, vol. 2021, no. 4, pp. 225–248, Virtual Event, July 2021. Online: <https://ia.cr/2021/809>. Code: [https://encrypto.de/code/SoK\\_ppClustering](https://encrypto.de/code/SoK_ppClustering). Acceptance rate 18.8%. CORE rank A. doi:10.2478/popets-2021-0068.
  - 12) K. Järvinen, A. Kiss, T. Schneider, O. Tkachenko, and Z. Yang, Faster Privacy-Preserving Location Proximity Schemes for Circles and Polygons. *IET Information Security*, vol. 14, no. 3, pp. 254–265, May, 2020. CORE rank C. doi:10.1049/iet-ifs.2019.0125.
  - 13) M. Y. Alhassan, D. Günther, A. Kiss, and T. Schneider, Efficient and Scalable Universal Circuits. *Journal of Cryptology (JoC)*, vol. 33, no. 3, pp. 1216–1271, April 8, 2020. Preliminary version: <https://ia.cr/2019/348>. Code: <https://encrypto.de/code/UC>. CORE rank A\*. doi:10.1007/s00145-020-09346-z.
  - 14) T. Schneider and A. Treiber, A Comment on Privacy-Preserving Scalar Product Protocols as proposed in “SPOC”. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, vol. 31, no. 3, pp. 543–546, March, 2020. Full version: <https://arxiv.org/abs/1906.04862>. Code: <https://encrypto.de/code/SPOCattack>. CORE rank A\*. doi:10.1109/TPDS.2019.2939313.
  - 15) A. Treiber, A. Nautsch, J. Kolberg, T. Schneider, and C. Busch, Privacy-Preserving PLDA Speaker Verification using Outsourced Secure Computation. *Speech Communication*, vol. 114, pp. 60–71, November, 2019. Code: <https://encrypto.de/code/PrivateASV>. CORE rank B. doi:10.1016/j.specom.2019.09.004.
  - 16) A. Nautsch, A. Jiménez, A. Treiber, J. Kolberg, C. Jasserand, E. Kindt, H. Delgado, M. Todisco, M. A. Hmani, A. Mtibaa, M. A. Abdelraheem, A. Abad, F. Teixeira, D. Matrouf, M. Gomez-Barrero, D. Petrovskadelacrétaz, G. Chollet, N. Evans, T. Schneider, J.-F. Bonastre, B. Raj, I. Trancoso, and C. Busch, Preserving Privacy in Speaker and Speech Characterisation. *Computer Speech and Language (CSL)*, vol. 2019, no. 58, pp. 441–480, November, 2019. CORE rank A. doi:10.1016/j.csl.2019.06.001.
  - 17) A. Kiss, M. Naderpour, J. Liu, N. Asokan, and T. Schneider, SoK: Modular and Efficient Private Decision Tree Evaluation. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, vol. 2019, no. 2, pp. 187–208, Stockholm, Sweden, April 2019. Full version: <https://ia.cr/2018/1099>. Code: <https://encrypto.de/code/PDTE>. Acceptance rate 22.3%. CORE rank A. doi:10.2478/popets-2019-0026.

- 18) B. Pinkas, T. Schneider, and M. Zohner, Scalable Private Set Intersection Based on OT Extension. *ACM Transactions on Privacy and Security (TOPS)*, vol. 21, no. 2, pp. 7:1–7:35, January 2018. Preliminary version: <https://ia.cr/2016/930>. Code: <https://encrypto.de/code/JournalPSI>. CORE rank A. doi:10.1145/3154794.
- 19) A. Kiss, J. Liu, T. Schneider, N. Asokan, and B. Pinkas, Private Set Intersection for Unequal Set Sizes with Mobile Applications. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, vol. 2017, no. 4, pp. 177–197, Minneapolis, MN, USA, October 2017. Full version: <https://ia.cr/2017/670>. Code: <https://encrypto.de/code/MobilePSI>. Acceptance rate 22.7%. CORE rank A. doi:10.1515/popets-2017-0044.
- 20) G. Asharov, Y. Lindell, T. Schneider, and M. Zohner, More Efficient Oblivious Transfer Extensions. *Journal of Cryptology (JoC)*, vol. 30, no. 3, pp. 805–858, July 2017. Updated version: <https://ia.cr/2016/602>. CORE rank A\*. doi:10.1007/s00145-016-9236-6.
- 21) G. Asharov, D. Demmler, M. Schapira, T. Schneider, G. Segev, S. Shenker, and M. Zohner, Privacy-Preserving Interdomain Routing at Internet Scale. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, vol. 2017, no. 3, pp. 143–163, Minneapolis, MN, USA, July 2017. Full version: <https://ia.cr/2017/393>. Acceptance rate 22.7%. CORE rank A. doi:10.1515/popets-2017-0033.
- 22) M. S. Riazi, E. M. Songhori, A.-R. Sadeghi, T. Schneider, and F. Koushanfar, Toward Practical Secure Stable Matching. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, vol. 2017, no. 1, pp. 62–78, Minneapolis, MN, USA, January 2017. Acceptance rate 22.7%. CORE rank A. doi:10.1515/popets-2017-0005.
- 23) V. Kolesnikov, A.-R. Sadeghi, and T. Schneider, A Systematic Approach to Practically Efficient General Two-Party Secure Function Evaluation Protocols and their Modular Design. *Journal of Computer Security (JCS)*, vol. 21, no. 2, pp. 283–315, January 2013. Preliminary version: <https://ia.cr/2010/079>. CORE rank B. doi:10.3233/JCS-130464.
- 24) M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, Privacy-Preserving ECG Classification with Branching Programs and Neural Networks. *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 6, no. 2, pp. 452–468, June 2011. CORE rank A. doi:10.1109/TIFS.2011.2108650.

### Conferences / Workshops with Proceedings (all peer reviewed)

- 25) L. Gu, G. R. Chandran, S. Zeitouni, T. Schneider, and Z. István, Differentially Private Intermediate Result Resizing for Scalable Secure Multi-Party Analytics. In **31. European Symposium on Research in Computer Security (ESORICS'26)**, LNCS, Springer, Rome, Italy, September 14-18, 2026. To appear. CORE rank A.
- 26) Kasra Edalatnejad and Sebastian Faust and Jonas Hofmann and Philipp-Florens Lehwalder and Thomas Schneider, Do you need a receipt? anonymous credential revocation at continental scale via private record certification. In **35. USENIX Security Symposium (USENIX Security'26)**, USENIX, Baltimore, MD, USA, August 12-14, 2026. To appear. Full version: <https://ia.cr/2026/1189>. Code: <https://encrypto.de/code/PRC>. CORE rank A\*.
- 27) J. Blüml, M. Huppert, N. Khayata, J. Schmidt, and T. Schneider, SING: Improving the Efficiency of MPC Protocol Assignment using Graph Neural Networks. In **35. USENIX Security Symposium (USENIX Security'26)**, USENIX, Baltimore, MD, USA, August 12-14, 2026. To appear. Online: <https://ia.cr/2026/1237>. Code: <https://encrypto.de/code/SING>. CORE rank A\*.
- 28) G. R. Chandran, M. Önen, and T. Schneider, FLiPD: Privacy-Preserving Federated Learning via Multi-Party Computation and Differential Privacy. In **23. International Conference on Security and Cryptography (SECRYPT'26)**, SciTePress, Porto, Portugal, July 16-18, 2026. Online: <https://ia.cr/2026/324>. CORE rank C.
- 29) A. Brüggemann and T. Schneider, When Trying to Catch Cheaters Breaks the MPC: Breaking and Fixing Delayed Consistency Checks in Trident, Fantastic Four, SWIFT, and Quad. In **45. Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT'26**, vol. 16543 of LNCS, pp. 457–487, Springer, Rome, Italy, May 10-14, 2026. Full version: <https://ia.cr/2026/234>. Code: <https://encrypto.de/code/F4attack>. Acceptance rate 20.4%. CORE rank A\*. doi:10.1007/978-3-032-25324-8\_16.
- 30) T. Schneider, H.-C. Wang, and H. Yalame, HE-SecureNet: An Efficient and Usable Framework for Model Training via Homomorphic Encryption. In **24. Workshop on Privacy in the Electronic Society (WPES'25)**, pp. 104–115, ACM, Taipei, Taiwan, November 18, 2025. Online: <https://ia.cr/2025/1591>. Acceptance rate 48.4% for full papers. doi:10.1145/3733802.3764063.
- 31) H. Dohmen, R. W. Hundt, N. Khayata, and T. Schneider, SEEC: Memory Safety Meets Efficiency in Secure Two-Party Computation. In **20. ACM ASIA Conference on Computer and Communications**

- Security (ASIACCS'25)**, pp. 118–135, ACM, Ha Noi, Vietnam, August 25–29, 2025. Full version: <https://ia.cr/2025/930>. Code: <https://crypto.de/code/SEEC>. Acceptance rate 20.4%. CORE rank A. doi:10.1145/3708821.3736224.
- 32) G. R. Chandran, T. Schneider, M. Stillger, and C. Weinert, Concretely Efficient Private Set Union via Circuit-Based PSI. In **20. ACM ASIA Conference on Computer and Communications Security (ASIACCS'25)**, pp. 149–162, ACM, Ha Noi, Vietnam, August 25–29, 2025. Online: <https://ia.cr/2024/1494>. Code: <https://crypto.de/code/circuitPSU>. Acceptance rate 20.4%. CORE rank A. doi:10.1145/3708821.3710839.
- 33) D. Günther, J. Schmidt, T. Schneider, and H. Yalame, FLUENT: A Tool for Efficient Mixed-Protocol Semi-Private Function Evaluation. In **40. Annual Computer Security Applications Conference (ACSAC'24)**, pp. 733–746, ACM, Waikiki, Hawaii, USA, December 9–13, 2024. Online: <https://ia.cr/2024/1561>. Code: <https://crypto.de/code/FLUENT> (Artifact Available Badge). Acceptance rate 21.8%. CORE rank A. doi:10.1109/ACSAC63791.2024.00066.
- 34) P. Ehrler, A. Kati, T. Schneider, and A. Treiber, Evaluating Leakage Attacks Against Relational Encrypted Search. In **16. ACM Cloud Computing Security Workshop (CCSW'24)**, pp. 15–28, ACM, Salt Lake City, USA, October 18, 2024. Online: <https://ia.cr/2024/1525>. Acceptance rate 41.2%. doi:10.1145/3689938.3694776.
- 35) G. R. Chandran, K. Demuth, K. Edalatnejad, S. Linsner, C. Reuter, and T. Schneider, Encrypted MultiChannel Communication (EMC2): Johnny should use Secret Sharing. In **23. Workshop on Privacy in the Electronic Society (WPES'24)**, pp. 34–39, ACM, Salt Lake City, USA, October 14, 2024. Short paper. Online: <https://ia.cr/2024/1407>. Code: <https://cryptogroup.github.io/EMC2>. Acceptance rate 50.0%. doi:10.1145/3689943.3695051.
- 36) L. Seyda, A. Brüggemann, G. Hornung, and T. Schneider, Multi-Party Computation als Instrument zur Umsetzung datenschutzkonformer behördlicher Datenabgleiche: Eine interdisziplinäre Analyse am Beispiel der Diskussionen um das Gesetz zur Selbstbestimmung über den Geschlechtseintrag. In **INFORMATIK 2024, Workshop Recht und Technik: Datenschutz im Diskurs (RuT'24)**, LNI, pp. 153–167, GI, Wiesbaden, Germany, September 26, 2024. doi:10.18420/inf2024\_11.
- 37) V. Duddu, A. Das, N. Khayata, H. Yalame, T. Schneider, and N. Asokan, Attesting Distributional Properties of Training Data for Machine Learning. In **29. European Symposium on Research in Computer Security (ESORICS'24)**, vol. 14982 of LNCS, pp. 3–23, Springer, Bydgoszcz, Poland, September 16–20, 2024. Full version: <https://arxiv.org/abs/2308.09552>. Code: <https://github.com/ssg-research/distribution-attestation>. Acceptance rate 16.1%. CORE rank A. doi:10.1007/978-3-031-70879-4\_1.
- 38) H. Keller, H. Möllering, T. Schneider, O. Tkachenko, and L. Zhao, Secure Noise Sampling for DP in MPC with Finite Precision. In **19. International Conference on Availability, Reliability and Security (ARES'24)**, pp. 25:1–25:12, ACM, Vienna, Austria, July 30 - August 2, 2024. Full version: <https://ia.cr/2023/1594>. Acceptance rate 20.5%. CORE rank B. doi:10.1145/3664476.3664490.
- 39) L. Reichert, G. R. Chandran, P. Schoppmann, T. Schneider, and B. Scheuermann, Menhir: An Oblivious Database with Protection against Access and Volume Pattern Leakage. In **19. ACM ASIA Conference on Computer and Communications Security (ASIACCS'24)**, pp. 1675–1690, ACM, Singapore, July 1–5, 2024. Online: <https://ia.cr/2024/556>. Code: <https://github.com/ReichertL/Menhir>. Acceptance rate 19.4%. CORE rank A. doi:10.1145/3634737.3657005.
- 40) H. Mantel, J. Schmidt, T. Schneider, M. Stillger, T. Weißmantel, and H. Yalame, HyCaMi: High-Level Synthesis for Cache Side Mitigation. In **61. Design Automation Conference (DAC'24)**, pp. 323:1–223:6, ACM, San Francisco, CA, USA, June 23–27, 2024. Code: <https://crypto.de/code/HyCaMi>. Online: <https://ia.cr/2024/533>. Acceptance rate 23%. CORE rank A. doi:10.1145/3649329.3657394.
- 41) A. Brüggemann, O. Schick, T. Schneider, A. Suresh, and H. Yalame, Don't Eject the Impostor: Fast Three-Party Computation With a Known Cheater. In **45. IEEE Symposium on Security and Privacy (IEEE S&P'24)**, pp. 503–522, IEEE, San Francisco, CA, USA, May 20–23, 2024. Full version: <https://ia.cr/2023/1744>. Code: <https://crypto.de/code/MOTION-FD>. Acceptance rate 17.8%. CORE rank A\*. doi:10.1109/SP54263.2024.00164.
- 42) Q. Pang, J. Zhu, H. Möllering, W. Zheng, and T. Schneider, BOLT: Privacy-Preserving, Accurate and Efficient Inference for Transformers. In **45. IEEE Symposium on Security and Privacy (IEEE S&P'24)**, pp. 4753–4771, IEEE, San Francisco, CA, USA, May 20–23, 2024. Online: <https://ia.cr/2023/1893>. Acceptance rate 17.8%. CORE rank A\*. doi:10.1109/SP54263.2024.00130.
- 43) Y. Ben-Itzhak, H. Möllering, B. Pinkas, T. Schneider, A. Suresh, O. Tkachenko, S. Vargaftik, C. Weinert, H. Yalame, and A. Yanai, ScionFL: Secure Quantized Aggregation for Federated Learning. In **2. IEEE Conference on Secure and Trustworthy Machine Learning (SaTML'24)**, pp. 490–511, IEEE, Toronto, Canada,

- April 9-11, 2024. **Runner-up Distinguished Paper Award**. Online: <https://ia.cr/2023/652>. Acceptance rate 21.5%. doi:10.1109/SaTML59370.2024.00031.
- 44) Y. Disser, D. Günther, T. Schneider, M. Stillger, A. Wigandt, and H. Yalame, Breaking the Size Barrier: Universal Circuits meet Lookup Tables. In **29. International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT'23**, vol. 14438 of LNCS, pp. 3–37, Springer, Guangzhou, China, December 4–8, 2023. Full version: <https://ia.cr/2022/1652>. Code: <https://crypto.de/code/LUC>. Acceptance rate 28.2%. CORE rank A. doi:10.1007/978-981-99-8721-4\_1.
  - 45) D. Dittert, T. Schneider, and A. Treiber, Too Close for Comfort? Measuring Success of Sampled-Data Leakage Attacks Against Encrypted Search. In **15. ACM Cloud Computing Security Workshop (CCSW'23)**, pp. 3–15, ACM, Copenhagen, Denmark, November 26, 2023. Online: <https://ia.cr/2023/1465>. Acceptance rate 50.0%. doi:10.1145/3605763.3625243.
  - 46) G. R. Chandran, R. Nieminen, T. Schneider, and A. Suresh, PrivMail: A Privacy-Preserving Framework for Secure Emails. In **28. European Symposium on Research in Computer Security (ESORICS'23)**, vol. 14345 of LNCS, pp. 145–165, Springer, The Hague, The Netherlands, September 25–29, 2023. Full version: <https://ia.cr/2023/1294>. Code: <https://crypto.de/code/PrivMail>. Acceptance rate 19.5%. CORE rank A. doi:10.1007/978-3-031-51476-0\_8.
  - 47) L. Hetz, T. Schneider, and C. Weinert, Scaling Mobile Private Contact Discovery to Billions of Users. In **28. European Symposium on Research in Computer Security (ESORICS'23)**, vol. 14344 of LNCS, pp. 455–476, Springer, The Hague, The Netherlands, September 25–29, 2023. Full version: <https://ia.cr/2023/758>. Code: <https://crypto.de/code/disco>. Acceptance rate 19.5%. CORE rank A. doi:10.1007/978-3-031-50594-2\_23.
  - 48) L. Braun, M. Huppert, N. Khayata, T. Schneider, and O. Tkachenko, FUSE – Flexible File Format and Intermediate Representation for Secure Multi-Party Computation. In **18. ACM ASIA Conference on Computer and Communications Security (ASIACCS'23)**, pp. 649–663, ACM, Melbourne, Australia, July 10–14, 2023. Full version: <https://ia.cr/2023/563>. Code: <https://crypto.de/code/FUSE>. Acceptance rate 17.3%. CORE rank A. doi:10.1145/3579856.3590340.
  - 49) T. Schneider, H. Yalame, and M. Yonli, Griffin: Towards Mixed Multi-Key Homomorphic Encryption. In **20. International Conference on Security and Cryptography (SECRYPT'23)**, pp. 147–158, SciTePress, Rome, Italy, July 10–12, 2023. Full version: <https://ia.cr/2023/654>. Acceptance rate 13.0% for full papers. CORE rank C. doi:10.5220/0012090200003555.
  - 50) T. Gehlhar, F. Marx, T. Schneider, A. Suresh, T. Wehrle, and H. Yalame, SafeFL: MPC-Friendly Framework for Private and Robust Federated Learning. In **6. Deep Learning Security and Privacy Workshop (DLSP'23)**, pp. 69–76, IEEE, San Francisco, CA, USA, May 25, 2023. Full version: <https://ia.cr/2023/555>. doi:10.1109/SPW59333.2023.00012.
  - 51) A. Brüggemann, R. Hundt, T. Schneider, A. Suresh, and H. Yalame, FLUTE: Fast and Secure Lookup Table Evaluations. In **44. IEEE Symposium on Security and Privacy (IEEE S&P'23)**, pp. 515–533, IEEE, San Francisco, CA, USA, May 22–25, 2023. Full version: <https://ia.cr/2023/499>. Code: <https://crypto.de/code/FLUTE>. Acceptance rate 17.0%. CORE rank A\*. doi:10.1109/SP46215.2023.10179345.
  - 52) A. Brüggemann, M. Breuer, A. Klinger, T. Schneider, and U. Meyer, Secure Maximum Weight Matching Approximation on General Graphs. In **21. Workshop on Privacy in the Electronic Society (WPES'22)**, pp. 83–87, ACM, Los Angeles, CA, USA, November 7, 2022. Short paper. Full version: <https://ia.cr/2022/1173>. Acceptance rate 33.9%. doi:10.1145/3559613.3563209.
  - 53) A. Treiber, D. Müllmann, T. Schneider, and I. Spiecker genannt Döhmann, Data Protection Law and Multi-Party Computation: Applications to Information Exchange between Law Enforcement Agencies. In **21. Workshop on Privacy in the Electronic Society (WPES'22)**, pp. 69–82, ACM, Los Angeles, CA, USA, November 7, 2022. Online: <https://ia.cr/2022/1242>. Acceptance rate 20.3% for full papers. doi:10.1145/3559613.3563192.
  - 54) K. Hamacher, T. Kussel, T. Schneider, and O. Tkachenko, PEA: Practical Private Epistasis Analysis using MPC. In **27. European Symposium on Research in Computer Security (ESORICS'22)**, vol. 13556 of LNCS, pp. 320–339, Springer, Copenhagen, Denmark, September 26–30, 2022. Full version: <https://ia.cr/2022/1185>. Acceptance rate 18.5%. CORE rank A. doi:10.1007/978-3-031-17143-7\_16.
  - 55) D. Günther, M. Heymann, B. Pinkas, and T. Schneider, GPU-Accelerated PIR with Client-Independent Preprocessing for Large-Scale Applications. In **31. USENIX Security Symposium (USENIX Security'22)**, pp. 1759–1776, USENIX, Boston, MA, USA, August 10–12, 2022. Online: <https://ia.cr/2021/823>. Code: <https://crypto.de/code/cip-pir>. Acceptance rate 18.1%. CORE rank A\*.
  - 56) T. D. Nguyen, P. Rieger, H. Chen, H. Yalame, H. Möllering, H. Fereidooni, S. Marchal, M. Miettinen, A. Mirhoseini, S. Zeitouni, F. Koushanfar, A.-R. Sadeghi, and T. Schneider, FLAME: Taming Backdoors

- in Federated Learning. In **31. USENIX Security Symposium (USENIX Security'22)**, pp. 1415–1432, USENIX, Boston, MA, USA, August 10-12, 2022. Online: <https://ia.cr/2021/025>. Acceptance rate 18.1%. CORE rank A\*.
- 57) G. R. Chandran, C. Hazay, R. Hundt, and T. Schneider, Comparison-Based MPC in Star Topology. In **19. International Conference on Security and Cryptography (SECRYPT'22)**, pp. 69–82, SciTePress, Lisbon, Portugal, July 11-13, 2022. Full version: <https://ia.cr/2022/574>. Acceptance rate 18.6% for full papers. CORE rank C. doi:10.5220/0011144100003283.
- 58) C. van der Beets, R. Nieminen, and T. Schneider, FAPRIL: Towards Faster Privacy-Preserving Fingerprint-Based Localization. In **19. International Conference on Security and Cryptography (SECRYPT'22)**, pp. 108–120, SciTePress, Lisbon, Portugal, July 11-13, 2022. Full version: <https://ia.cr/2022/564>. Code: <https://encrypto.de/code/ppIndoorLocalization>. Acceptance rate 18.6% for full papers. CORE rank C. doi:10.5220/0011263500003283.
- 59) S. Kamara, A. Kati, T. Moataz, T. Schneider, A. Treiber, and M. Yonli, SoK: Cryptanalysis of Encrypted Search with LEAKER – A framework for LEakage AttacK Evaluation on Real-World data. In **7. IEEE European Symposium on Security and Privacy (EuroS&P'22)**, pp. 90–108, IEEE, Genoa, Italy, June 6-10, 2022. Full version: <https://ia.cr/2021/1035>. Code: <https://encrypto.de/code/LEAKER>. Acceptance rate 30.0%. CORE rank A. doi:10.1109/EuroSP53844.2022.00014.
- 60) A. Patra, T. Schneider, A. Suresh, and H. Yalame, SynCirc: Efficient Synthesis of Depth-Optimized Circuits for Secure Computation. In **14. IEEE International Workshop on Hardware-Oriented Security and Trust (HOST'21)**, pp. 147–157, IEEE, Washington D.C., USA, June 27-30, 2022. Full version: <https://ia.cr/2021/1153>. Acceptance rate 23%. doi:10.1109/HOST49136.2021.9702293.
- 61) J.-P. Münch, T. Schneider, and H. Yalame, VASA: Vector AES Instructions for Security Applications. In **37. Annual Computer Security Applications Conference (ACSAC'21)**, pp. 131–145, ACM, Austin, TX, USA, December 6-10, 2021. Full version: <https://ia.cr/2021/1493>. Code: <https://encrypto.de/code/VASA>. Acceptance rate 21.0%. CORE rank A. doi:10.1145/3485832.3485897.
- 62) A. Heinrich, M. Hollick, T. Schneider, M. Stute, and C. Weinert, PrivateDrop: Practical Privacy-Preserving Authentication for Apple AirDrop. In **30. USENIX Security Symposium (USENIX Security'21)**, pp. 3577–3594, USENIX, Virtual Event, August 11-13, 2021. Website: <https://privatedrop.github.io>. Full version: <https://ia.cr/2021/481>. Code: <https://encrypto.de/code/privatedrop>. Acceptance rate 19%. CORE rank A\*.
- 63) A. Patra, T. Schneider, A. Suresh, and H. Yalame, ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation. In **30. USENIX Security Symposium (USENIX Security'21)**, pp. 2165–2182, USENIX, Virtual Event, August 11-13, 2021. Full version: <https://ia.cr/2020/1225>. Acceptance rate 19%. CORE rank A\*.
- 64) H. Keller, H. Möllering, T. Schneider, and H. Yalame, Balancing Quality and Efficiency in Private Clustering with Affinity Propagation. In **18. International Conference on Security and Cryptography (SECRYPT'21)**, pp. 173–184, SciTePress, Virtual Event, July 6-8, 2021. Full version: <https://ia.cr/2021/825>. Code: <https://encrypto.de/code/ppAffinityPropagation>. Acceptance rate 18.4% for full papers. CORE rank C. doi:10.5220/0010547801730184.
- 65) D. Demmler, S. Katzenbeisser, T. Schneider, T. Schuster, and C. Weinert, Improved Circuit Compilation for Hybrid MPC via Compiler Intermediate Representation. In **18. International Conference on Security and Cryptography (SECRYPT'21)**, pp. 444–451, SciTePress, Virtual Event, July 6-8, 2021. Short paper. Full version: <https://ia.cr/2021/521>. Acceptance rate 35.6%. CORE rank C. doi:10.5220/0010540504440451.
- 66) T. Heldmann, T. Schneider, O. Tkachenko, C. Weinert, and H. Yalame, LLVM-Based Circuit Compilation for Practical Secure Computation. In **19. International Conference on Applied Cryptography and Network Security (ACNS'21)**, vol. 12727 of LNCS, pp. 99–121, Springer, Virtual Event, June 21-24, 2021. Online: <https://ia.cr/2021/797>. Code: <https://encrypto.de/code/LLVM>. Acceptance rate 19.9%. CORE rank B. doi:10.1007/978-3-030-78375-4\_5.
- 67) B. Bozdemir, S. Canard, O. Ermiş, H. Möllering, M. Önen, and T. Schneider, Privacy-preserving Density-Based Clustering. In **16. ACM ASIA Conference on Computer and Communications Security (ASIACCS'21)**, pp. 658–671, ACM, Virtual Event, June 7-11, 2021. Online: <https://ia.cr/2021/612>. Code: <https://encrypto.de/code/ppDBSCAN>. Acceptance rate 18.9%. CORE rank A. doi:10.1145/3433210.3453104.
- 68) H. Fereidooni, S. Marchal, M. Miettinen, A. Mirhoseini, H. Möllering, T. D. Nguyen, P. Rieger, A.-R. Sadeghi, T. Schneider, H. Yalame, and S. Zeitouni, SAFELearn: Secure Aggregation for private FEderated Learning. In **4. Deep Learning and Security Workshop (DLS'21)**, pp. 56–62, IEEE, Virtual Event, May 27, 2021. Full version: <https://ia.cr/2021/386>. Acceptance rate 40%. doi:10.1109/SPW53761.2021.00017.

- 69) C. Hagen, C. Weinert, C. Sendner, A. Dmitrienko, and T. Schneider, All the Numbers are US: Large-Scale Abuse of Contact Discovery in Mobile Messengers. In **28. Network and Distributed System Security Symposium (NDSS'21)**, Internet Society, Virtual Event, February 21-24, 2021. Website: <https://contact-discovery.github.io>. Online: <https://ia.cr/2020/1119>. Code: <https://github.com/contact-discovery>. Acceptance rate 15.2%. CORE rank A\*. doi:10.14722/ndss.2021.23159.
- 70) H. Mantel, L. Scheidel, T. Schneider, A. Weber, C. Weinert, and T. Weißmantel, RiCaSi: Rigorous Cache Side channel mitigation via selective circuit compilation. In **19. International Conference on Cryptology And Network Security (CANS'20)**, vol. 12579 of LNCS, pp. 505–525, Springer, Virtual Event, December 14-16, 2020. Acceptance rate 25.4%. CORE rank B. doi:10.1007/978-3-030-65411-5\_25.
- 71) N. Büscher, D. Demmler, N. P. Karvelas, S. Katzenbeisser, J. Krämer, D. Rathee, T. Schneider, and P. Struck, Secure Two-Party Computation in a Quantum World. In **18. International Conference on Applied Cryptography and Network Security (ACNS'20)**, vol. 12146 of LNCS, pp. 461–480, Springer, Virtual Event, October 19-22, 2020. Full version: <https://ia.cr/2020/411>. Code: <https://encrypto.de/code/pq-mpc>. Acceptance rate 21.5%. CORE rank B. doi:10.1007/978-3-030-57808-4\_23.
- 72) J. Buchmann, G. Dessouky, T. Frassetto, A. Kiss, A.-R. Sadeghi, T. Schneider, G. Traverso, and S. Zeitouni, SAFE: A Secure and Efficient Long-Term Distributed Storage System. In **8. ACM International Workshop on Security in Blockchain and Cloud Computing (SBC@ASIACCS'20)**, pp. 8–13, ACM, Virtual Event, October 6, 2020. Online: <https://ia.cr/2020/690>. Acceptance rate 44.4%. doi:10.1145/3384942.3406868.
- 73) M. Holz, A. Kiss, D. Rathee, and T. Schneider, Linear-Complexity Private Function Evaluation is Practical. In **25. European Symposium on Research in Computer Security (ESORICS'20)**, vol. 12309 of LNCS, pp. 401–420, Springer, Virtual Event, September 14-18, 2020. Full version: <https://ia.cr/2020/853>. Code: <https://encrypto.de/code/linearPFE>. Acceptance rate 19.7%. CORE rank A. doi:10.1007/978-3-030-59013-0\_20.
- 74) A. Treiber, A. Molina, C. Weinert, T. Schneider, and K. Kersting, CryptoSPN: Privacy-Preserving Sum-Product Network Inference. In **24. European Conference on Artificial Intelligence (ECAI'20)**, pp. 1946–1953, IOS Press, Virtual Event, August 29-September 5, 2020. Online: <https://arxiv.org/abs/2002.00801>. Code: <https://encrypto.de/code/CryptoSPN>. Acceptance rate 26.8%. CORE rank A. doi:10.3233/FAIA200313.
- 75) F. Boemer, R. Cammarota, D. Demmler, T. Schneider, and H. Yalame, MP2ML: A Mixed-Protocol Machine Learning Framework for Private Inference. In **15. International Conference on Availability, Reliability and Security (ARES'20)**, pp. 14:1–14:10, ACM, Virtual Event, August 25-28, 2020. Full version: <https://ia.cr/2020/721>. Code: <https://github.com/IntelAI/he-transformer>. Acceptance rate 21.3%. CORE rank B. doi:<https://dl.acm.org/doi/10.1145/3407023.3407045>.
- 76) S. P. Bayerl, T. Frassetto, P. Jauernig, K. Riedhammer, A.-R. Sadeghi, T. Schneider, E. Stapf, and C. Weinert, Offline Model Guard: Secure and Private ML on Mobile Devices. In **23. Design, Automation & Test in Europe Conference & Exhibition (DATE'20)**, pp. 460–465, IEEE, Grenoble, France, March 9-13, 2020. Online: <https://arxiv.org/abs/2007.02351>. Acceptance rate 26%. CORE rank B. doi:10.23919/DATE48585.2020.9116560.
- 77) R. N. Reith, T. Schneider, and O. Tkachenko, Efficiently Stealing your Machine Learning Models. In **18. Workshop on Privacy in the Electronic Society (WPES'19)**, pp. 198–210, ACM, London, UK, November 11, 2019. Acceptance rate 20.9%. doi:10.1145/3338498.3358646.
- 78) S. Felsen, A. Kiss, T. Schneider, and C. Weinert, Secure and Private Function Evaluation with Intel SGX. In **10. ACM Cloud Computing Security Workshop (CCSW'19)**, pp. 165–181, ACM, London, UK, November 11, 2019. Acceptance rate 37.5%. doi:10.1145/3338466.3358919.
- 79) D. Rathee, T. Schneider, and K. K. Shukla, Improved Multiplication Triple Generation over Rings via RLWE-Based AHE. In **18. International Conference on Cryptology And Network Security (CANS'19)**, vol. 11829 of LNCS, pp. 347–359, Springer, Fuzhou, China, October 25-27, 2019. Short paper. Full version: <https://ia.cr/2019/577>. Acceptance rate 52.7%. CORE rank B. doi:10.1007/978-3-030-31578-8\_19.
- 80) A. Nautsch, J. Patino, A. Treiber, T. Stafylakis, P. Mizera, M. Todisco, T. Schneider, and N. Evans, Privacy-Preserving Speaker Recognition with Cohort Score Normalisation. In **20. Conference of the International Speech Communication Association (INTERSPEECH'19)**, pp. 2868–2872, International Speech Communication Association (ISCA), Graz, Austria, September 15-19, 2019. Online: <https://arxiv.org/abs/1907.03454>. Acceptance rate 49.3%. CORE rank A. doi:10.21437/Interspeech.2019-2638.
- 81) D. Kales, C. Rechberger, T. Schneider, M. Senker, and C. Weinert, Mobile Private Contact Discovery at Scale. In **28. USENIX Security Symposium (USENIX Security'19)**, pp. 1447–1464, USENIX, Santa Clara, CA, USA, August 14-16, 2019. Website: <https://contact-discovery.github.io>.

- Full version: <https://ia.cr/2019/517>. Code: <https://github.com/contact-discovery>. Acceptance rate 16.2%. CORE rank A\*.
- 82) A. Kiss, O. Schick, and T. Schneider, Web Application for Privacy-Preserving Scheduling using Secure Computation. In *16. International Joint Conference on e-Business and Telecommunications (ICETE'19)*, pp. 456–463, SciTePress, Prague, Czech Republic, July 26–28, 2019. Short paper. Code: <https://encrypto.de/code/scheduling>. Acceptance rate 31.5%. doi:10.5220/0007947704560463.
  - 83) T. Schneider and O. Tkachenko, EPISODE: Efficient Privacy-Preserving Similar Sequence Queries on Outsourced Genomic Databases. In *14. ACM ASIA Conference on Computer and Communications Security (ASIACCS'19)*, pp. 315–327, ACM, Auckland, New Zealand, July 7–12, 2019. Online: <https://ia.cr/2021/029>. Acceptance rate 17.1%. CORE rank A. doi:10.1145/3321705.3329800.
  - 84) K. Järvinen, H. Leppäkoski, E. S. Lohan, P. Richter, T. Schneider, O. Tkachenko, and Z. Yang, PILOT: Practical Privacy-Preserving Indoor Localization using Outsourcing. In *4. IEEE European Symposium on Security and Privacy (EuroS&P'19)*, pp. 448–463, IEEE, Stockholm, Sweden, June 17–19, 2019. Acceptance rate 20.0%. CORE rank A. doi:10.1109/EuroSP.2019.00040.
  - 85) B. Pinkas, T. Schneider, O. Tkachenko, and A. Yanai, Efficient Circuit-Based PSI with Linear Communication. In *38. Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT'19*, vol. 11478 of LNCS, pp. 122–153, Springer, Darmstadt, Germany, May 19–23, 2019. Online: <https://ia.cr/2019/241>. Code: <https://encrypto.de/code/OPPRF-PSI>. Acceptance rate 23.2%. CORE rank A\*. doi:10.1007/978-3-030-17659-4\_5.
  - 86) N. Büscher, D. Demmler, S. Katzenbeisser, D. Kretzmer, and T. Schneider, HyCC: Compilation of Hybrid Protocols for Practical Secure Computation. In *25. ACM Conference on Computer and Communications Security (CCS'18)*, pp. 847–861, ACM, Toronto, Canada, October 15–19, 2018. Code: <https://gitlab.com/securityengineering/HyCC>. Acceptance rate 16.6%. CORE rank A\*. doi:10.1145/3243734.3243786.
  - 87) O. Tkachenko and T. Schneider, Towards Efficient Privacy-Preserving Similar Sequence Queries on Outsourced Genomic Databases. In *17. Workshop on Privacy in the Electronic Society (WPES'18)*, pp. 71–75, ACM, Toronto, Canada, October 15, 2018. Short paper. Acceptance rate 36.5%. doi:10.1145/3267323.3268956.
  - 88) K. Järvinen, A. Kiss, T. Schneider, O. Tkachenko, and Z. Yang, Faster Privacy-Preserving Location Proximity Schemes. In *17. International Conference on Cryptology And Network Security (CANS'18)*, vol. 11124 of LNCS, pp. 3–22, Springer, Naples, Italy, September 30–October 3, 2018. Full version: <https://ia.cr/2018/694>. Acceptance rate 32.9%. CORE rank B. doi:10.1007/978-3-030-00434-7\_1.
  - 89) F. Brasser, T. Frassetto, K. Riedhammer, A.-R. Sadeghi, T. Schneider, and C. Weinert, VoiceGuard: Secure and Private Speech Processing. In *19. Conference of the International Speech Communication Association (INTERSPEECH'18)*, pp. 1303–1307, International Speech Communication Association (ISCA), Hyderabad, India, September 2–6, 2018. Acceptance rate 54%. CORE rank A. doi:10.21437/Interspeech.2018-2032.
  - 90) P. Richter, Z. Yang, O. Tkachenko, H. Leppäkoski, K. Järvinen, T. Schneider, and E. S. Lohan, Received Signal Strength Quantization for Secure Indoor Positioning via Fingerprinting. In *8. International Conference on Localization and GNSS (ICL-GNSS'18)*, pp. 1–6, IEEE, Guimarães, Portugal, June 26–28, 2018. doi:10.1109/ICL-GNSS.2018.8440910.
  - 91) O. Tkachenko, C. Weinert, T. Schneider, and K. Hamacher, Large-Scale Privacy-Preserving Statistical Computations for Distributed Genome-Wide Association Studies. In *13. ACM ASIA Conference on Computer and Communications Security (ASIACCS'18)*, pp. 221–235, ACM, Songdo, South Korea, June 4–8, 2018. Acceptance rate 16.8%. CORE rank A. doi:10.1145/3196494.3196541.
  - 92) M. S. Riazi, C. Weinert, O. Tkachenko, E. M. Songhori, T. Schneider, and F. Koushanfar, Chameleon: A Hybrid Secure Computation Framework for Machine Learning Applications. In *13. ACM ASIA Conference on Computer and Communications Security (ASIACCS'18)*, pp. 707–721, ACM, Songdo, South Korea, June 4–8, 2018. Preliminary version: <https://ia.cr/2017/1164>. Acceptance rate 16.8%. CORE rank A. doi:10.1145/3196494.3196522.
  - 93) B. Pinkas, T. Schneider, C. Weinert, and U. Wieder, Efficient Circuit-Based PSI via Cuckoo Hashing. In *37. Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT'18*, vol. 10822 of LNCS, pp. 125–157, Springer, Tel Aviv, Israel, April 29–May 3, 2018. Full version: <https://ia.cr/2018/120>. Code: <https://encrypto.de/code/2DCH>. Acceptance rate 23.0%. CORE rank A\*. doi:10.1007/978-3-319-78372-7\_5.
  - 94) M. Chiesa, D. Demmler, M. Canini, M. Schapira, and T. Schneider, SIXPACK: Securing Internet eXchange Points Against Curious onlookers. In *13. International Conference on emerging Networking*

- Experiments and Technologies (CoNEXT'17)**, pp. 120–133, ACM, Seoul, South Korea, December 12–15, 2017. Code: <https://six-pack.bitbucket.io>. Acceptance rate 18.1%. CORE rank A. doi:10.1145/3143361.3143362.
- 95) D. Günther, A. Kiss, and T. Schneider, More Efficient Universal Circuit Constructions. In **23. International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT'17**, vol. 10625 of LNCS, pp. 443–470, Springer, Hong Kong, China, December 3–7, 2017. Full version: <https://ia.cr/2017/798>. Code: <https://crypto.de/code/UC>. Acceptance rate 27.6%. CORE rank A. doi:10.1007/978-3-319-70697-9\_16.
  - 96) D. Demmler, K. Hamacher, T. Schneider, and S. Stammel, Privacy-Preserving Whole-Genome Variant Queries. In **16. International Conference on Cryptology And Network Security (CANS'17)**, vol. 11261 of LNCS, pp. 1–22, Springer, Hong Kong, China, November 30–December 2, 2017. Acceptance rate 31.8%. CORE rank B. doi:10.1007/978-3-030-02641-7\_4.
  - 97) D. Demmler, M. Holz, and T. Schneider, OnionPIR: Effective Protection of Sensitive Metadata in Online Communication Networks. In **15. International Conference on Applied Cryptography and Network Security (ACNS'17)**, vol. 10355 of LNCS, pp. 599–619, Springer, Kanazawa, Japan, July 10–12, 2017. Code: <https://crypto.de/code/onionPIR>. Acceptance rate 22.8%. CORE rank B. doi:10.1007/978-3-319-61204-1\_30.
  - 98) J. B. Nielsen, T. Schneider, and R. Trifiletti, Constant Round Maliciously Secure 2PC with Function-Independent Preprocessing using LEGO. In **24. Network and Distributed System Security Symposium (NDSS'17)**, Internet Society, San Diego, CA, USA, February 26–March 1, 2017. Acceptance rate 16.1%. CORE rank A\*. doi:10.14722/ndss.2017.23075.
  - 99) G. Dessouky, F. Koushanfar, A.-R. Sadeghi, T. Schneider, S. Zeitouni, and M. Zohner, Pushing the Communication Barrier in Secure Computation using Lookup Tables. In **24. Network and Distributed System Security Symposium (NDSS'17)**, Internet Society, San Diego, CA, USA, February 26–March 1, 2017. Full version: <https://ia.cr/2018/486>. Code: <https://crypto.de/code/ABY>. Acceptance rate 16.1%. CORE rank A\*. doi:10.14722/ndss.2017.23097.
  - 100) M. Chiesa, D. Demmler, M. Canini, M. Schapira, and T. Schneider, Towards Securing Internet eXchange Points Against Curious onlookers. In **ACM, IRTF & ISOC Applied Networking Research Workshop (ANRW'16)**, pp. 32–34, ACM, Berlin, Germany, July 16, 2016. Short paper. doi:10.1145/2959424.2959427.
  - 101) E. M. Songhori, S. Zeitouni, G. Dessouky, T. Schneider, A.-R. Sadeghi, and F. Koushanfar, Garbled-CPU: A MIPS Processor for Secure Computation in Hardware. In **53. Design Automation Conference (DAC'16)**, pp. 73:1–73:6, ACM, Austin, TX, USA, June 5–9, 2016. Acceptance rate 17.4%. CORE rank A. doi:10.1145/2897937.2898027.
  - 102) A. Kiss and T. Schneider, Valiant's Universal Circuit is Practical. In **35. Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT'16**, vol. 9665 of LNCS, pp. 699–728, Springer, Vienna, Austria, May 8–12, 2016. Full version: <https://ia.cr/2016/093>. Code: <https://crypto.de/code/UC>. Acceptance rate 22.6%. CORE rank A\*. doi:10.1007/978-3-662-49890-3\_27.
  - 103) D. Demmler, G. Dessouky, F. Koushanfar, A.-R. Sadeghi, T. Schneider, and S. Zeitouni, Automated Synthesis of Optimized Circuits for Secure Computation. In **22. ACM Conference on Computer and Communications Security (CCS'15)**, pp. 1504–1517, ACM, Denver, CO, USA, October 12–16, 2015. Acceptance rate 19.8%. CORE rank A\*. doi:10.1145/2810103.2813678.
  - 104) P. Koeberl, V. Phegade, A. Rajan, T. Schneider, S. Schulz, and M. Zhdanova, Time to Rethink: Trust Brokerage using Trusted Execution Environments. In **8. International Conference on Trust and Trustworthy Computing (TRUST'15)**, vol. 9229 of LNCS, pp. 181–190, Springer, Heraklion, Crete, Greece, August 24–26, 2015. Short paper. doi:10.1007/978-3-319-22846-4\_11.
  - 105) B. Pinkas, T. Schneider, G. Segev, and M. Zohner, Phasing: Private Set Intersection using Permutation-Based Hashing. In **24. USENIX Security Symposium (USENIX Security'15)**, pp. 515–530, USENIX, Washington, DC, USA, August 12–14, 2015. Full version: <https://ia.cr/2015/634>. Code: <https://crypto.de/code/PSI>. Acceptance rate 15.7%. CORE rank A\*.
  - 106) E. M. Songhori, S. U. Hussain, A.-R. Sadeghi, T. Schneider, and F. Koushanfar, TinyGarble: Highly Compressed and Scalable Sequential Garbled Circuits. In **36. IEEE Symposium on Security and Privacy (IEEE S&P'15)**, pp. 411–428, IEEE, San Jose, CA, USA, May 18–20, 2015. Acceptance rate 13.5%. CORE rank A\*. doi:10.1109/SP.2015.32.
  - 107) G. Asharov, Y. Lindell, T. Schneider, and M. Zohner, More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries. In **34. Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT'15**, vol. 9056 of LNCS, pp. 673–701, Springer,

- Sofia, Bulgaria, April 26-30, 2015. Full version: <https://ia.cr/2015/061>. Code: <https://encrypto.de/code/OTExtension>. Acceptance rate 29.4%. CORE rank A\*. doi:10.1007/978-3-662-46800-5\_26.
- 108) M. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, and M. Zohner, Ciphers for MPC and FHE. In **34. Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT'15**, vol. 9056 of LNCS, pp. 430–454, Springer, Sofia, Bulgaria, April 26-30, 2015. Full version: <https://ia.cr/2016/687>. Acceptance rate 29.4%. CORE rank A\*. doi:10.1007/978-3-662-46800-5\_17.
- 109) D. Demmler, T. Schneider, and M. Zohner, ABY – A Framework for Efficient Mixed-Protocol Secure Two-Party Computation. In **22. Network and Distributed System Security Symposium (NDSS'15)**, Internet Society, San Diego, CA, USA, February 8-11, 2015. Code: <https://encrypto.de/code/ABY>. Acceptance rate 18.4%. CORE rank A\*.
- 110) D. Demmler, A. Herzberg, and T. Schneider, RAID-PIR: Practical Multi-Server PIR. In **6. ACM Cloud Computing Security Workshop (CCSW'14)**, pp. 45–56, ACM, Scottsdale, AZ, USA, November 7, 2014. Code: <https://encrypto.de/code/RAID-PIR>. Acceptance rate 33.3%. doi:10.1145/2664168.2664181.
- 111) D. Demmler, T. Schneider, and M. Zohner, Ad-Hoc Secure Two-Party Computation on Mobile Devices using Hardware Tokens. In **23. USENIX Security Symposium (USENIX Security'14)**, pp. 893–908, USENIX, San Diego, CA, USA, August 20-22, 2014. Full version: <https://ia.cr/2014/467>. Acceptance rate 19.1%. CORE rank A\*.
- 112) B. Pinkas, T. Schneider, and M. Zohner, Faster Private Set Intersection based on OT Extension. In **23. USENIX Security Symposium (USENIX Security'14)**, pp. 797–812, USENIX, San Diego, CA, USA, August 20-22, 2014. Full version: <https://ia.cr/2014/447>. Code: <https://encrypto.de/code/PSI>. Acceptance rate 19.1%. CORE rank A\*.
- 113) J. Bringer, H. Chabanne, M. Favre, A. Patey, T. Schneider, and M. Zohner, GSHADE: Faster Privacy-Preserving Distance Computation and Biometric Identification. In **2. ACM Workshop on Information Hiding and Multimedia Security (IH&MMSEC'14)**, pp. 187–198, ACM, Salzburg, Austria, June 11-13, 2014. Code: <https://encrypto.de/code/GSHADE>. Acceptance rate 37.5%. CORE rank C. doi:10.1145/2600918.2600922.
- 114) M. Schneider and T. Schneider, Notes on Non-Interactive Secure Comparison in “Image Feature Extraction in the Encrypted Domain with Privacy-Preserving SIFT”. In **2. ACM Workshop on Information Hiding and Multimedia Security (IH&MMSEC'14)**, pp. 432–440, ACM, Salzburg, Austria, June 11-13, 2014. Acceptance rate 37.5%. CORE rank C. doi:10.1145/2600918.2600927.
- 115) F. Kerschbaum, T. Schneider, and A. Schröpfer, Automatic Protocol Selection in Secure Two-Party Computations. In **12. International Conference on Applied Cryptography and Network Security (ACNS'14)**, vol. 8479 of LNCS, pp. 566–584, Springer, Lausanne, Switzerland, June 10-13, 2014. Full version: <https://ia.cr/2014/200>. Acceptance rate 22.4%. CORE rank B. doi:10.1007/978-3-319-07536-5\_33.
- 116) G. Asharov, Y. Lindell, T. Schneider, and M. Zohner, More Efficient Oblivious Transfer and Extensions for Faster Secure Computation. In **20. ACM Conference on Computer and Communications Security (CCS'13)**, pp. 535–548, ACM, Berlin, Germany, November 4-8, 2013. Full version: <https://ia.cr/2013/552>. Code: <https://encrypto.de/code/OTExtension>. Acceptance rate 19.8%. CORE rank A\*. doi:10.1145/2508859.2516738.
- 117) N. Asokan, A. Dmitrienko, M. Nagy, E. Reshetova, A.-R. Sadeghi, T. Schneider, and S. Stelle, CrowdShare: Secure Mobile Resource Sharing. In **11. International Conference on Applied Cryptography and Network Security (ACNS'13)**, vol. 7954 of LNCS, pp. 432–440, Springer, Banff, Alberta, Canada, June 25-28, 2013. Short paper. Full version: [https://encrypto.de/papers/ADNRSSS13\\_TR.pdf](https://encrypto.de/papers/ADNRSSS13_TR.pdf). CORE rank B. doi:10.1007/978-3-642-38980-1\_27.
- 118) W. Henecka and T. Schneider, Faster Secure Two-Party Computation with Less Memory. In **8. ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIACCS'13)**, pp. 437–446, ACM, Hangzhou, China, May 7-10, 2013. Code: <https://encrypto.de/code/me-sfe>. Acceptance rate 16.2% for full papers. CORE rank A. doi:10.1145/2484313.2484369.
- 119) T. Schneider and M. Zohner, GMW vs. Yao? Efficient Secure Two-Party Computation with Low Depth Circuits. In **17. International Conference on Financial Cryptography and Data Security (FC'13)**, vol. 7859 of LNCS, pp. 275–292, Springer, Okinawa, Japan, April 1-5, 2013. Acceptance rate 12.5% for regular papers. CORE rank A. doi:10.1007/978-3-642-39884-1\_23.
- 120) J. J. Ahmad, S. Li, A.-R. Sadeghi, and T. Schneider, CTL: A Platform-Independent Crypto Tools Library Based on Dataflow Programming Paradigm. In **16. International Conference on Financial Cryptography and Data Security (FC'12)**, vol. 7397 of LNCS, pp. 299–313, Springer, Bonaire, February 27 -

- March 2, 2012. Full version: <https://ia.cr/2011/679>. Acceptance rate 26.1%. CORE rank A. doi:10.1007/978-3-642-32946-3\_22.
- 121) S. Bugiel, S. Nürnberger, A.-R. Sadeghi, and T. Schneider, Twin Clouds: Secure Cloud Computing with Low Latency. In *12. Communications and Multimedia Security Conference (CMS'11)*, vol. 7025 of LNCS, pp. 32–44, Springer, October 19–21, 2011. **Best Paper Award**. Acceptance rate 21.2%. CORE rank C. doi:10.1007/978-3-642-24712-5\_3.
  - 122) S. Bugiel, S. Nürnberger, T. Pöppelmann, A.-R. Sadeghi, and T. Schneider, AmazonIA: When Elasticity Snaps Back. In *18. ACM Conference on Computer and Communications Security (CCS'11)*, pp. 389–400, ACM, Chicago, IL, USA, October 17–21, 2011. Info: <https://encrypto.de/AMID>. Acceptance rate 14.0%. CORE rank A\*. doi:10.1145/2046707.2046753.
  - 123) T. Schneider, Reden ist Silber - Schweigen ist Gold: Datensparsamkeit durch effizientes Rechnen unter Verschlüsselung. In *12. Deutscher IT-Sicherheitskongress des BSI: Sicher in die digitale Welt von morgen*, pp. 191–198, SecuMedia-Verlag, Bonn, Germany, May 10–12, 2011.
  - 124) M. Fischlin, B. Pinkas, A.-R. Sadeghi, T. Schneider, and I. Visconti, Secure Set Intersection with Untrusted Hardware Tokens. In *11. Cryptographers' Track at the RSA Conference (CT-RSA'11)*, vol. 6558 of LNCS, pp. 1–16, Springer, San Francisco, CA, USA, February 14–18, 2011. Acceptance rate 29.9%. CORE rank B. doi:10.1007/978-3-642-19074-2\_1.
  - 125) W. Henecka, S. Kögl, A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, TASTY: Tool for Automating Secure Two-partY computations. In *17. ACM Conference on Computer and Communications Security (CCS'10)*, pp. 451–462, ACM, Chicago, IL, USA, October 4–8, 2010. Full version: <https://ia.cr/2010/365>. Code: <https://encrypto.de/code/TASTY>. Acceptance rate 17.2%. CORE rank A\*. doi:10.1145/1866307.1866358.
  - 126) J. B. Almeida, E. Bangerter, M. Barbosa, S. Krenn, A.-R. Sadeghi, and T. Schneider, A Certifying Compiler for Zero-Knowledge Proofs of Knowledge Based on Sigma-Protocols. In *15. European Symposium on Research in Computer Security (ESORICS'10)*, vol. 6345 of LNCS, pp. 151–167, Springer, Athens, Greece, September 20–22, 2010. Full version: <https://ia.cr/2010/339>. Acceptance rate 20.9%. CORE rank A. doi:10.1007/978-3-642-15497-3\_10.
  - 127) A.-R. Sadeghi and T. Schneider, Verschlüsselt Rechnen: Sichere Verarbeitung verschlüsselter medizinischer Daten am Beispiel der Klassifikation von EKG-Daten. In *Workshop Innovative und sichere Informationstechnologie für das Gesundheitswesen von morgen (perspeGktive'10)*, vol. P-174 of LNI, pp. 11–25, Bonner Köllen Verlag, Darmstadt, Germany, September 8, 2010.
  - 128) K. Järvinen, V. Kolesnikov, A.-R. Sadeghi, and T. Schneider, Garbled Circuits for Leakage-Resilience: Hardware Implementation and Evaluation of One-Time Programs. In *12. International Workshop on Cryptographic Hardware and Embedded Systems (CHES'10)*, vol. 6225 of LNCS, pp. 383–397, Springer, Santa Barbara, CA, USA, August 17–20, 2010. Full version: <https://ia.cr/2010/276>. Acceptance rate 27.8%. CORE rank A. doi:10.1007/978-3-642-15031-9\_26.
  - 129) A.-R. Sadeghi, T. Schneider, and M. Winandy, Token-Based Cloud Computing – Secure Outsourcing of Data and Arbitrary Computations with Lower Latency. In *3. International Conference on Trust and Trustworthy Computing (TRUST'10) - Workshop on Trust in the Cloud*, vol. 6101 of LNCS, pp. 417–429, Springer, Berlin, Germany, June 21–23, 2010. doi:10.1007/978-3-642-13869-0\_30.
  - 130) K. Järvinen, V. Kolesnikov, A.-R. Sadeghi, and T. Schneider, Embedded SFE: Offloading Server and Network using Hardware Tokens. In *14. International Conference on Financial Cryptography and Data Security (FC'10)*, vol. 6052 of LNCS, pp. 207–221, Springer, Tenerife, Canary Islands, Spain, January 25–28, 2010. Full version: <https://ia.cr/2009/591>. Acceptance rate 14.6%. CORE rank A. doi:10.1007/978-3-642-14577-3\_17.
  - 131) V. Kolesnikov, A.-R. Sadeghi, and T. Schneider, Improved Garbled Circuit Building Blocks and Applications to Auctions and Computing Minima. In *8. International Conference on Cryptology And Network Security (CANS'09)*, vol. 5888 of LNCS, pp. 1–20, Springer, Kanazawa, Japan, December 12–14, 2009. Full version: <https://ia.cr/2009/411>. Acceptance rate 29.4%. CORE rank B. doi:10.1007/978-3-642-10433-6\_1.
  - 132) B. Pinkas, T. Schneider, N. P. Smart, and S. C. Williams, Secure Two-Party Computation is Practical. In *15. International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT'09*, vol. 5912 of LNCS, pp. 250–267, Springer, Tokyo, Japan, December 6–10, 2009. Full version: <https://ia.cr/2009/314>. Acceptance rate 13.7%. CORE rank A. doi:10.1007/978-3-642-10366-7\_15.
  - 133) M. Barni, P. Failla, V. Kolesnikov, R. Lazzeretti, A. Paus, A.-R. Sadeghi, and T. Schneider, Efficient Privacy-Preserving Classification of ECG Signals. In *1. IEEE International Workshop on Information Forensics and Security (IEEE WIFS'09)*, pp. 91–95, IEEE, London, UK, December 6–9, 2009. Acceptance rate 32.5%. doi:10.1109/WIFS.2009.5386475.

- 134) A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, Efficient Privacy-Preserving Face Recognition. In *12. International Conference on Information Security and Cryptology (ICISC'09)*, vol. 5984 of *LNCS*, pp. 229–244, Springer, Seoul, South Korea, December 2-4, 2009. Full version: <https://ia.cr/2009/507>. Acceptance rate 19.8%. doi:10.1007/978-3-642-14423-3\_16.
- 135) M. Barni, P. Failla, V. Kolesnikov, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, Secure Evaluation of Private Linear Branching Programs with Medical Applications. In *14. European Symposium on Research in Computer Security (ESORICS'09)*, vol. 5789 of *LNCS*, pp. 424–439, Springer, Saint Malo, France, September 21-25, 2009. Full version: <https://ia.cr/2009/195>. Acceptance rate 19.1%. CORE rank A. doi:10.1007/978-3-642-04444-1\_26.
- 136) E. Bangerter, T. Briner, W. Henecka, S. Krenn, A.-R. Sadeghi, and T. Schneider, Automatic Generation of Sigma-Protocols. In *6. European Workshop on Public Key Services, Applications and Infrastructures (EUROPKI'09)*, vol. 6391 of *LNCS*, pp. 67–82, Springer, Pisa, Italy, September 10-11, 2009. Acceptance rate 45.0%. CORE rank B. doi:10.1007/978-3-642-16441-5\_5.
- 137) A. Paus, A.-R. Sadeghi, and T. Schneider, Practical Secure Evaluation of Semi-Private Functions. In *7. International Conference on Applied Cryptography and Network Security (ACNS'09)*, vol. 5536 of *LNCS*, pp. 89–106, Springer, Paris-Rocquencourt, France, June 2-5, 2009. Full version: <https://ia.cr/2009/124>. Code: <https://crypto.de/code/FairplaySPF>. Acceptance rate 21.3%. CORE rank B. doi:10.1007/978-3-642-01957-9\_6.
- 138) E. Bangerter, S. Barzan, S. Krenn, A.-R. Sadeghi, T. Schneider, and J.-K. Tsay, Bringing Zero-Knowledge Proofs of Knowledge to Practice. In *17. International Workshop on Security Protocols (SPW'09)*, vol. 7028 of *LNCS*, pp. 51–62, Springer, Cambridge, UK, April 1-3, 2009. Full version: <https://ia.cr/2009/211>. doi:10.1007/978-3-642-36213-2\_9.
- 139) A.-R. Sadeghi and T. Schneider, Generalized Universal Circuits for Secure Evaluation of Private Functions with Application to Data Classification. In *11. International Conference on Information Security and Cryptology (ICISC'08)*, vol. 5461 of *LNCS*, pp. 336–353, Springer, Seoul, South Korea, December 3-5, 2008. Full version: <https://ia.cr/2008/453>. Acceptance rate 19.8%. doi:10.1007/978-3-642-00730-9\_21.
- 140) V. Kolesnikov and T. Schneider, Improved Garbled Circuit: Free XOR Gates and Applications. In *35. International Colloquium on Automata, Languages and Programming (ICALP'08)*, vol. 5126 of *LNCS*, pp. 486–498, Springer, Reykjavik, Iceland, July 6-13, 2008. Acceptance rate 30%. CORE rank A\*. doi:10.1007/978-3-540-70583-3\_40.
- 141) V. Kolesnikov and T. Schneider, A Practical Universal Circuit Construction and Secure Evaluation of Private Functions. In *12. International Conference on Financial Cryptography and Data Security (FC'08)*, vol. 5143 of *LNCS*, pp. 83–97, Springer, Cozumel, Mexico, January 28-31, 2008. Code: <https://crypto.de/code/FairplayPF>. Acceptance rate 19.1%. CORE rank A. doi:10.1007/978-3-540-85230-8\_7.

### Original Contributions: Posters / Demos / Contributed Talks (all peer-reviewed)

- 142) A. Brüggemann, T. Goldan, and T. Schneider, POSTER: PrivForm – A Privacy-Preserving Framework for Online Forms. **40. Annual Computer Security Applications Conference (ACSAC'24) Poster Session**, Waikiki, Hawaii, USA, December 9-13, 2024. CORE rank A.
- 143) G. R. Chandran, P.-F. Lehwalder, L. Rometsch, and T. Schneider, POSTER: Secure and Differentially Private K-th Ranked Element. In **30. ACM Conference on Computer and Communications Security (CCS'23) Posters/Demos**, pp. 3624–3626, ACM, Copenhagen, Denmark, November 26-30, 2023. Code: <https://crypto.de/code/dp-KRE>. Acceptance rate 47.4%. CORE rank A\*. doi:10.1145/3576915.3624392.
- 144) A. Brüggemann, T. Schneider, A. Suresh, and H. Yalame, POSTER: Efficient Three-Party Shuffling Using Precomputation. In **29. ACM Conference on Computer and Communications Security (CCS'22) Posters/Demos**, pp. 3331–3333, ACM, Los Angeles, CA, USA, November 7-11, 2022. CORE rank A\*. doi:10.1145/3548606.3563511.
- 145) D. Günther, M. Holz, B. Judkewitz, H. Möllering, B. Pinkas, T. Schneider, and A. Suresh, POSTER: Privacy-Preserving Epidemiological Modeling on Mobile Graphs. In **29. ACM Conference on Computer and Communications Security (CCS'22) Posters/Demos**, pp. 3351–3353, ACM, Los Angeles, CA, USA, November 7-11, 2022. CORE rank A\*. doi:10.1145/3548606.3563497.
- 146) S. Kamara, A. Kati, T. Moataz, T. Schneider, A. Treiber, and M. Yonli, CONTRIBUTED TALK: All about that Data: Towards a Practical Assessment of Attacks on Encrypted Search. Real World Crypto Symposium (RWC'22), Amsterdam, The Netherlands, April 13-15, 2022. Acceptance rate 33.3%.
- 147) L. Braun, R. Cammarota, and T. Schneider, POSTER: A Generic Hybrid 2PC Framework with Application to Private Inference of Unmodified Neural Networks (Extended Abstract). Privacy in Machine Learning

Workshop (PriML@NeurIPS'21), Virtual Event, December 14, 2021. Code: <https://encrypto.de/code/MOTION2NX>.

- 148) D. Günther, T. Schneider, and F. Wiegand, POSTER: Revisiting Hybrid Private Information Retrieval. In **28. ACM Conference on Computer and Communications Security (CCS'21) Posters/Demos**, pp. 2408–2410, ACM, Virtual Event, November 15–19, 2021. Code: <https://encrypto.de/code/HybridPIR>. CORE rank A\*. doi:10.1145/3460120.3485346.
- 149) T. Birka, T. Kussel, H. Möllering, and T. Schneider, An Efficient and Practical Privacy-Preserving Kidney Exchange Problem Protocol (Abstract). In **33. Kryptotag (crypto day matters)**, Gesellschaft für Informatik e.V. / FG KRYPTO, Virtual Event, September 17, 2021. doi:10.18420/cdm-2021-33-31.
- 150) A. Heinrich, M. Hollick, T. Schneider, M. Stute, and C. Weinert, DEMO: AirCollect: Efficiently Recovering Hashed Phone Numbers Leaked via Apple AirDrop. In **14. ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'21) Demo**, pp. 371–373, ACM, Virtual Event, June 28–July 2, 2021. Website: <https://privatedrop.github.io>. Online: <https://ia.cr/2021/893>. Code: <https://encrypto.de/code/aircollect>. Acceptance rate 78.6%. doi:10.1145/3448300.3468252.
- 151) D. Günther, A. Kiss, L. Scheidel, and T. Schneider, POSTER: Framework for Semi-Private Function Evaluation with Application to Secure Insurance Rate Calculation. In **26. ACM Conference on Computer and Communications Security (CCS'19) Posters/Demos**, pp. 2541–2543, ACM, London, UK, November 11–15, 2019. Code: <https://encrypto.de/code/spfe-framework>. Acceptance rate 67.2%. CORE rank A\*. doi:10.1145/3319535.3363251.
- 152) S. P. Bayerl, F. Brasser, C. Busch, T. Frassetto, P. Jauernig, J. Kolberg, A. Nautsch, K. Riedhammer, A.-R. Sadeghi, T. Schneider, E. Stapf, A. Treiber, and C. Weinert, POSTER: Privacy-Preserving Speech Processing via STPC and TEEs (Extended Abstract). **2. Privacy Preserving Machine Learning Workshop (PPML@CCS'19)**, London, UK, November 15, 2019. Acceptance rate 55.0%.
- 153) E. Bangerter, S. Krenn, A.-R. Sadeghi, and T. Schneider, POSTER: YACZK: Yet Another Compiler for Zero-Knowledge. **19. USENIX Security Symposium (USENIX Security'10) Poster Session**, Washington, DC, USA, August 11–13, 2010. CORE rank A\*.
- 154) A.-R. Sadeghi and T. Schneider, POSTER: Ask Your E-Doctor Without Telling: Privacy-Preserving Medical Diagnostics. Section Days of Ruhr-University Bochum Research School, Bochum, Germany, November 6, 2009. (Poster prize awarded).
- 155) E. Bangerter, J. Camenisch, S. Krenn, A.-R. Sadeghi, and T. Schneider, POSTER: Automatic Generation of Sound Zero-Knowledge Protocols. **28. Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT'09 Poster Session**, Cologne, Germany, April 26–30, 2009. Full version: <https://ia.cr/2008/471>. Acceptance rate 33% for papers and posters. CORE rank A\*.

## Keynotes

- 156) T. Schneider, Private Machine Learning via Multi-Party Computation. In **12. ACM International Workshop on Security and Privacy Analytics (IWSPA'26)**, ACM, Frankfurt am Main, Germany, June 24, 2026. Keynote. doi:10.1145/3806007.3810964.
- 157) T. Schneider, Engineering Privacy-Preserving Machine Learning Protocols. In **Privacy-Preserving Machine Learning in Practice Workshop (PPMLP@CCS'20)**, pp. 3–4, ACM, Virtual Event, November 9, 2020. Keynote. doi:10.1145/3411501.3418607.

## Technical Reports / Preprints (not peer reviewed)

- 158) A. Brüggemann, T. Schneider, and M. Stillger, Additions, Multiplications, and the Interaction In-Between: Optimizing MPC Protocols via Leveled Linear Secret Sharing. Cryptology ePrint Archive, Paper 2026/368, 2026. Online: <https://ia.cr/2026/368>.
- 159) R. Cammarota, M. Schunter, A. Rajan, F. Boemer, A. Kiss, A. Treiber, C. Weinert, T. Schneider, E. Stapf, A.-R. Sadeghi, D. Demmler, H. Chen, S. U. Hussain, S. Riazzi, F. Koushanfar, S. Gupta, T. S. Rosing, K. Chaudhuri, H. Nejatollahi, N. Dutt, M. Imani, K. Laine, A. Dubey, A. Aysu, F. S. Hosseini, C. Yang, E. Wallace, and P. Norton, Trustworthy AI Inference Systems: An Industry Research View. arXiv:2008.04449, August 10, 2020. <https://arxiv.org/abs/2008.04449>.
- 160) P. Pullonen, D. Bogdanov, and T. Schneider, The Design and Implementation of a Two-Party Protocol Suite for SHAREMIND 3. tech. rep., CYBERNETICA Institute of Information Security, 2012. T-4-17.

## NO Original Contributions: Extended Abstracts / Posters / Demos / Contributed Talks / Workshops without Proceedings

- 161) A. Brüggemann and T. Schneider, CONTRIBUTED TALK: When Trying to Catch Cheaters Breaks the MPC: A Cautionary Tale of Postponing Batched Consistency Checks. 12. Theory and Practice of Multi-Party Computation Workshop (TPMPC'26), Aarhus, Denmark, May 18-22, 2026.
- 162) J. Filipp, P. Paul, and T. Schneider, CONTRIBUTED TALK: Secure Evaluation of Authenticated Private Functions. 2. Real-World MPC Workshop (RWMPC'26), Taipei, Taiwan, March 7, 2026. Organized by the MPC Alliance in cooperation with IACR; affiliated event with 15. Real-World Crypto Symposium (RWC'26).
- 163) L. Seyda, A. Brüggemann, G. Hornung, and T. Schneider, POSTER: The German Self-Determination Act—Ignoring Cryptography and Endangering Trans\* People. Decrypting Diversity Summit, Poster Session, Montpellier, France, June 17-20, 2025.
- 164) O. Bytyci, N. Khayata, and T. Schneider, POSTER: Non-Interactive Zero-Knowledge Proofs for Attesting Distributional Properties of Machine Learning Properties. Decrypting Diversity Summit, Poster Session, Montpellier, France, June 17-20, 2025.
- 165) A. Brüggemann, O. Schick, T. Schneider, A. Suresh, and H. Yalame, CONTRIBUTED TALK: Don't Eject the Impostor – Honest-Majority MPC with Fixed Malicious Parties. 11. Theory and Practice of Multi-Party Computation Workshop (TPMPC'25), Bangalore, India, March 3-6, 2025.
- 166) R. W. Hundt, N. Khayata, and T. Schneider, POSTER: SEEC – Memory Safety Meets Efficiency in Secure Two-Party Computation. **40. Annual Computer Security Applications Conference (ACSAC'24) Poster Session**, Waikiki, Hawaii, USA, December 9-13, 2024. Code: <https://encrypto.de/code/SEEC>. CORE rank A.
- 167) R. Hundt, N. Khayata, and T. Schneider, CONTRIBUTED TALK: SEEC: Memory Safety Meets Efficiency in Secure Two-Party Computation. 10. Theory and Practice of Multi-Party Computation Workshop (TPMPC'24), Darmstadt, Germany, June 3-6, 2024.
- 168) L. Braun, M. Huppert, N. Khayata, T. Schneider, and O. Tkachenko, CONTRIBUTED TALK: FUSE – Flexible File Format and Intermediate Representation for Secure Multi-Party Computation. 9. Theory and Practice of Multi-Party Computation Workshop (TPMPC'23), Aarhus, Denmark, June 8-9, 2023.
- 169) G. R. Chandran, R. Nieminen, T. Schneider, and A. Suresh, PrivMail: A Privacy-Preserving Framework for Secure Emails (Short Talk). **44. IEEE Symposium on Security and Privacy (IEEE S&P'23) Short Talk**, San Francisco, CA, USA, May 22-25, 2023. CORE rank A\*.
- 170) A. Brüggemann, T. Schneider, A. Suresh, and H. Yalame, Is Everyone Equally Trustworthy in Practice? (Short Talk). **44. IEEE Symposium on Security and Privacy (IEEE S&P'23) Short Talk**, San Francisco, CA, USA, May 22-25, 2023. CORE rank A\*.
- 171) T. Schneider, H. Yalame, and M. Yonli, POSTER: Towards Mixed Multi-Key Homomorphic Encryption. 2. Annual FHE.org Conference on Fully Homomorphic Encryption (FHE.org'23) Poster Session, Tokyo, Japan, March 26, 2023.
- 172) A. Hegde, H. Möllering, T. Schneider, and H. Yalame, CONTRIBUTED TALK: SoK: Privacy-Preserving Clustering (Extended Abstract). Privacy in Machine Learning Workshop (PriML@NeurIPS'21), Virtual Event, December 14, 2021.
- 173) A. Patra, T. Schneider, A. Suresh, and H. Yalame, POSTER: ABY2.0: New Efficient Primitives for STPC with Applications to Privacy in Machine Learning (Extended Abstract). Privacy in Machine Learning Workshop (PriML@NeurIPS'21), Virtual Event, December 14, 2021.
- 174) A. Patra, T. Schneider, A. Suresh, and H. Yalame, POSTER: ABY2.0: New Efficient Primitives for 2PC with Applications to Privacy Preserving Machine Learning (Extended Abstract). 4. Privacy Preserving Machine Learning Workshop (PPML@CCS'21), Virtual Event, November 19, 2021.
- 175) A. Hegde, H. Möllering, T. Schneider, and H. Yalame, POSTER: SoK: Privacy-Preserving Clustering (Extended Abstract). 4. Privacy Preserving Machine Learning Workshop (PPML@CCS'21), Virtual Event, November 19, 2021.
- 176) H. Keller, H. Möllering, T. Schneider, and H. Yalame, POSTER: Balancing Quality and Efficiency in Private Clustering with Affinity Propagation (Extended Abstract). 4. Privacy Preserving Machine Learning Workshop (PPML@CCS'21), Virtual Event, November 19, 2021.
- 177) A. Heinrich, M. Hollick, T. Schneider, M. Stute, and C. Weinert, CONTRIBUTED TALK: Breaking and Fixing Contact Identifier-Based Mutual Authentication in Apple AirDrop. Future of PI Workshop: Challenges and Perspectives of Personal Identification (FoPI@EuroS&P'21), September 6, 2021.
- 178) A. Patra, T. Schneider, A. Suresh, and H. Yalame, ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation with Applications to Privacy Preserving Machine Learning (Extended Abstract). 3. Privacy-Preserving Machine Learning Workshop (PPML@CRYPTO'21), August 15, 2021.

- 179) H. Keller, H. Möllering, T. Schneider, and H. Yalame, Privacy-Preserving Clustering (Abstract). In 32. *Kryptotag (crypto day matters)*, Gesellschaft für Informatik e.V. / FG KRYPTO, Virtual Event, January 15, 2021. doi:10.18420/cdm-2021-32-42.
- 180) F. Boemer, R. Cammarota, D. Demmler, T. Schneider, and H. Yalame, POSTER: MP2ML: A Mixed-Protocol Machine Learning Framework for Private Inference (Extended Abstract). Privacy Preserving Machine Learning Workshop (PPML@NeurIPS'20), Virtual Event, December 11, 2020.
- 181) A. Treiber, A. Molina, C. Weinert, T. Schneider, and K. Kersting, CryptoSPN: Expanding PPML beyond Neural Networks (Extended Abstract). In *Privacy-Preserving Machine Learning in Practice Workshop (PPMLP@CCS'20)*, pp. 9–14, ACM, Virtual Event, November 9, 2020. Full paper. Acceptance rate 23.5% for full papers. doi:10.1145/3411501.3419417.
- 182) F. Boemer, R. Cammarota, D. Demmler, T. Schneider, and H. Yalame, MP2ML: A Mixed-Protocol Machine Learning Framework for Private Inference (Extended Abstract). In *Privacy-Preserving Machine Learning in Practice Workshop (PPMLP@CCS'20)*, pp. 43–45, ACM, Virtual Event, November 9, 2020. Short paper. Acceptance rate 47.1%. doi:10.1145/3411501.3419425.
- 183) A. Treiber, A. Molina, C. Weinert, T. Schneider, and K. Kersting, CONTRIBUTED TALK: CryptoSPN: Expanding PPML beyond Neural Networks (Extended Abstract). 2. Privacy-Preserving Machine Learning Workshop (PPML@CRYPTO'20), August 16, 2020.
- 184) F. Boemer, R. Cammarota, D. Demmler, T. Schneider, and H. Yalame, MP2ML: A Mixed-Protocol Machine Learning Framework for Private Inference (Extended Abstract). 2. Privacy-Preserving Machine Learning Workshop (PPML@CRYPTO'20), August 16, 2020.
- 185) A. Treiber, A. Molina, C. Weinert, T. Schneider, and K. Kersting, CONTRIBUTED TALK: CryptoSPN: Privacy-Preserving Machine Learning beyond Neural Networks (Extended Abstract). 7. Theory and Practice of Multi-Party Computation Workshop (TPMPC'20), Virtual Event, June 4, 2020.
- 186) A. Kiss, O. Schick, and T. Schneider, POSTER: Web Application for Privacy-Preserving Scheduling. **27. USENIX Security Symposium (USENIX Security'18) Poster Session**, Baltimore, MD, USA, August 15-17, 2018. CORE rank A\*.
- 187) G. Asharov, M. Canini, M. Chiesa, D. Demmler, M. Schapira, T. Schneider, G. Segev, S. Shenker, and M. Zohner, CONTRIBUTED TALK: Towards Practical Private Internet Routing using MPC. 5. Theory and Practice of Multi-Party Computation Workshop (TPMPC'18), Aarhus, Denmark, May 28-31, 2018.
- 188) D. Demmler, T. Schneider, and M. Zohner, Hardware-Assisted Ad-Hoc Secure Two-Party Computation on Smartphones (Abstract). In 19. *Kryptotag (crypto day matters)*, Gesellschaft für Informatik e.V. / FG KRYPTO, Stuttgart, Germany, November 14-15, 2013.
- 189) F. Kerschbaum, T. Schneider, and A. Schröpfer, Automatic Protocol Selection in Secure Two-Party Computations (Short Talk). **20. Network and Distributed System Security Symposium (NDSS'13) Short Talk**, San Diego, CA, USA, February 24-27, 2013. CORE rank A\*.
- 190) T. Schneider and M. Zohner, Efficient Secure Two-Party Computation (Abstract). In 17. *Kryptotag (crypto day matters)*, Gesellschaft für Informatik e.V. / FG KRYPTO, Heidelberg, Germany, December 7, 2012.
- 191) S. Bugiel, S. Nürnberger, A.-R. Sadeghi, and T. Schneider, Twin Clouds: An Architecture for Secure Cloud Computing (Extended Abstract). Workshop on Cryptography and Security in Clouds (WCSC'11), Zurich, Switzerland, March 15-16, 2011.
- 192) V. Kolesnikov, A.-R. Sadeghi, and T. Schneider, Improved Garbled Circuit Building Blocks and Applications to Auctions and Computing Minima. In *ECRYPT workshop on Software Performance Enhancements for Encryption and Decryption and Cryptographic Compilers (SPEED-CC'09)*, Berlin, Germany, October 12-13, 2009.
- 193) E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, and J.-K. Tsay, On the Design and Implementation of Efficient Zero-Knowledge Proofs of Knowledge. In *ECRYPT workshop on Software Performance Enhancements for Encryption and Decryption and Cryptographic Compilers (SPEED-CC'09)*, Berlin, Germany, October 12-13, 2009.
- 194) M. Barni, P. Failla, V. Kolesnikov, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, Combining Signal Processing and Cryptographic Protocol Design for Efficient ECG Classification. In 1. *International Workshop on Signal Processing in the EncryptEd Domain (SPEED'09)*, Lausanne, Switzerland, September 10, 2009.
- 195) V. Kolesnikov, A.-R. Sadeghi, and T. Schneider, How to Combine Homomorphic Encryption and Garbled Circuits – Improved Circuits and Computing the Minimum Distance Efficiently. In 1. *International Workshop on Signal Processing in the EncryptEd Domain (SPEED'09)*, Lausanne, Switzerland, September 10, 2009.
- 196) V. Kolesnikov, T. Schneider, and V. Strehl, Practical Secure Function Evaluation (Abstract). In 8. *Kryptotag (crypto day matters)*, vol. WSI-2008-02, Gesellschaft für Informatik e.V. / FG KRYPTO, Tübingen, Germany, April 11, 2008.

- 197) T. Schneider, POSTER: Practical Secure Function Evaluation. In *Fachwissenschaftlicher Informatik-Kongress (Informatiktage 2008)*, vol. S-6 of *LNI*, pp. 37–40, GI, Bonn, Germany, March 14, 2008.

## Patents

- 198) V. Kolesnikov and T. Schneider, Secure Function Evaluation Techniques for Circuits Containing XOR Gates with Applications to Universal Circuits. U.S. patent no 8443205 (applied 10/24/2008; issued 05/14/2013; EXPIRED 06/21/2021), May 14, 2013.
- 199) V. Kolesnikov and T. Schneider, Universal Circuit for Secure Function Evaluation. U.S. patent no 8175854 (applied 07/14/2008; issued 05/08/2012), May 8, 2012.

## Books / Book Chapters

- 200) T. Schneider, Engineering Secure Two-Party Computation Protocols: Design, Optimization, and Applications of Efficient Secure Function Evaluation. Springer-Verlag Berlin Heidelberg, August 4, 2012. <https://thomaschneider.de/engineeringSFEbook>. doi:10.1007/978-3-642-30042-4.
- 201) K. Järvinen, V. Kolesnikov, A.-R. Sadeghi, and T. Schneider, Efficient Secure Two-Party Computation with Untrusted Hardware Tokens. In *Towards Hardware Intrinsic Security: Foundation and Practice* (A.-R. Sadeghi and D. Naccache, eds.), Information Security and Cryptography, pp. 367–386, Springer-Verlag Berlin Heidelberg, 2010.

## Theses

- 202) T. Schneider, Engineering Secure Two-Party Computation Protocols – Advances in Design, Optimization, and Applications of Efficient Secure Function Evaluation. PhD thesis, Ruhr-University Bochum, Germany, February 9, 2011.
- 203) T. Schneider, Practical Secure Function Evaluation. Master’s thesis, Friedrich-Alexander University Erlangen-Nürnberg, Germany, February 27, 2008.
- 204) T. Schneider, Secure Task Migration and Interprocess Communication in Reconfigurable, Distributed, Embedded Systems. Bachelor’s thesis, Friedrich-Alexander University Erlangen-Nürnberg, Germany, July 10, 2007.

---

## List of Talks

### Invited Talks

- 2026/06/24 **Private Machine Learning via Multi-Party Computation**, 12. *ACM International Workshop on Security and Privacy Analytics (IWSPA'26)*, Frankfurt am Main, Germany.
- 2026/05/18 **Combining Ideas in 2PC: Lessons Learned in Garbling and Secret Sharing**, 12. *Workshop on the Theory and Practice of Multiparty Computation (TPMPC'26); Special Workshop on MPC Security in Practice*, Aarhus, Denmark.
- 2025/10/21 **(Re)search for a Private Tomorrow: Highlights in MPC**, *Internet Privacy Engineering Network (IPEN) event on Secure Multi-Party Computation organized by the European Data Protection Supervisor (EDPS)*, Goethe University Frankfurt, Germany.
- 2025/07/28 **Private Set Intersection for the Society**, *Dagstuhl Seminar on Building Privacy-Preserving Technologies of Societal Impact*, Dagstuhl, Germany.
- 2025/06/24 **Private Machine Learning via Multi-Party Computation**, *CASA & RC Trust Summer School 2025 on AI and Security*, Ruhr-University Bochum, Germany.
- 2025/03/14 **Advanced Cryptography for Data Privacy**, *Workshop on Data Privacy in the Digital Age*, LMU Munich, Germany.
- 2023/11/30 **Recent Advances in Secure Two-Party Computation**, *Carbyne Stack Conference'23*, Renningen, Germany+Virtual.
- 2021/06/15 **Protecting Privacy in Applications**, *Lecture in Lecture Series "What's behind it?"*, Darmstadt, Germany.
- 2020/11/09 **Engineering Privacy-Preserving Machine Learning Protocols**, *Keynote at Privacy-Preserving Machine Learning in Practice (PPMLP@CCS'20), CCS'20 Workshop*, Orlando, USA.  
Talk cancelled due to illness

- 2019/09/13 **Efficiently Protecting Data and Functions**, *CROSSING Week on Sustainable Security & Privacy*, Darmstadt, Germany.
- 2019/06/19 **Private Function Evaluation - From Functions to Data to Code**, 6. *Workshop on the Theory and Practice of Multiparty Computation (TPMPC'19)*, Tel-Aviv, Israel.
- 2018/03/24 **Protecting Privacy with Cryptographic Protocols**, *DAAD Stipendiatentreffen*, Darmstadt, Germany.
- 2017/07/06 **Engineering Privacy-Preserving Cryptographic Protocols**, *Karlsruher Institut für Technologie (KIT)*, Karlsruhe, Germany.
- 2017/01/11 **Engineering Privacy-Preserving Cryptographic Protocols**, *Albert-Ludwigs-Universität Freiburg*, Freiburg, Germany.
- 2016/11/08 **Engineering Privacy-Preserving Cryptographic Protocols**, *TU Darmstadt*, Darmstadt, Germany.
- 2016/10/31 **Engineering Privacy-Preserving Cryptographic Protocols**, *Universität des Saarlandes*, Saarbrücken, Germany.
- 2016/06/22 **Engineering Privacy-Preserving Cryptographic Protocols**, *Ruhr-Universität Bochum*, Germany.
- 2015/09 **Practical Aspects of Secure Two-Party Computation**, *Summer School on Secure and Trustworthy Computing*, University Politehnica of Bucharest, Romania.
- 2015/06/08-12 **ABY - A Framework for Efficient Mixed-Protocol Secure Two-Party Computation**, *Securing Computation Workshop*, Berkeley, USA.
- 2015/02 **Optimizations of Yao's Protocol for Semi-Honest Adversaries**, 5. *Bar-Ilan Winter School: Advances in Practical Multiparty Computation*, Bar-Ilan University, Israel.  
Talk given by Yehuda Lindell due to illness
- 2015/01/15 **GSHADE: Faster Privacy-Preserving Distance Computation and Biometric Identification**, *Privacy Enhancing Technologies for Biometric Data Workshop*, Haifa, Israel.
- 2014/09/11 **Efficient Two-Party Computations from Oblivious Transfer**, *Keynote at Workshop on Usable and Efficient Secure Multiparty Computation, co-located with ESORICS'14*, Wroclaw, Poland.
- 2014/05/05-09 **Efficient Oblivious Transfer Extensions and Applications**, 2. *Workshop on the Theory and Practice of Secure Multiparty Computation (TPMPC'14)*, Aarhus, Denmark.
- 2013/09/19 **Engineering Cryptographic Protocols (ENCRYPTO)**, *BOSCH – 9. BOSCH Experts Organisation Workshop*, Möglingen, Germany.
- 2012/11/06-08 **GMW vs. Yao: Towards more efficient implementations of generic secure two-party computation protocols in the semi-honest setting**, *Workshop on Concrete Efficiency of Multiparty Computation*, Tel Aviv, Israel.
- 2012/10/22-23 **Cloud Security Risks - When Elasticity Snaps Back**, *Intel European Research & Innovation Conference*, Barcelona, Spain.
- 2012/06/04-08 **Secure Set Intersection with Untrusted Hardware Tokens**, 1. *Workshop on the Theory and Practice of Multiparty Computation (TPMPC'12)*, Aarhus, Denmark.
- 2011/09 **Hardware-assisted Cryptographic Protocols**, 6. *European Trusted Infrastructure Summer School (ETISS)*, Darmstadt, Germany.
- 2011/08/08 **Engineering Cryptographic Protocols (ENCRYPTO)**, *EC SPRIDE Colloquium*, TU Darmstadt, Darmstadt, Germany.
- 2011/06/07 **Engineering Privacy-Preserving Cryptographic Protocols**, *Universität des Saarlandes/Max-Planck-Institut für Informatik*, Saarbrücken, Germany.

### Presentations at Conferences and Workshops

Whenever possible, my students give the conference presentations for our joint papers.

- 2014/06/12 **Notes on Non-Interactive Secure Comparison in “Image Feature Extraction in the Encrypted Domain with Privacy-Preserving SIFT”**, *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSEC'14)*, Salzburg, Austria.

- 2013/05/10 **Faster Secure Two-Party Computation with Less Memory**, *ACM Symposium on Information, Computer and Communications Security (ASIACCS'13)*, Hangzhou, China.
- 2011/05/11 **Reden ist Silber - Schweigen ist Gold: Datensparsamkeit durch effizientes Rechnen unter Verschlüsselung**, 12. *Deutscher IT-Sicherheitskongress des BSI*, Bonn, Germany.
- 2011/03/16 **Twin Clouds: An Architecture for Secure Cloud Computing**, *IBM Workshop on Cryptography and Security in Clouds (WCSC'11)*, Zurich, Switzerland.
- 2011/02/15 **Secure Set Intersection with Untrusted Hardware Tokens**, *Cryptographers' Track at the RSA Conference (CT-RSA'11)*, San Francisco, CA, USA.
- 2010/10/06 **TASTY: Tool for Automating Secure Two-partY computations**, *ACM Conference on Computer and Communications Security (CCS'10)*, Chicago, IL, USA.
- 2010/09/08 **Verschlüsselt Rechnen: Sichere Verarbeitung verschlüsselter medizinischer Daten am Beispiel der Klassifikation von EKG-Daten**, *Workshop Innovative und sichere Informationstechnologie für das Gesundheitswesen von morgen (PerspeGktive'10)*, Mannheim, Germany.
- 2010/08/20 **Garbled Circuits for Leakage-Resilience: Hardware Implementation and Evaluation of One-Time Programs**, *International Workshop on Cryptographic Hardware and Embedded Systems (CHES'10)*, Santa Barbara, CA, USA.
- 2010/06/22 **Token-Based Cloud Computing - Secure Outsourcing of Data and Arbitrary Computations with Lower Latency**, *International Conference on Trust and Trustworthy Computing (TRUST'10) - Workshop on Trust in the Cloud*, Berlin, Germany.
- 2010/01/27 **Embedded SFE: Offloading Server and Network using Hardware Tokens**, *International Conference on Financial Cryptography and Data Security (FC'10)*, Tenerife, Canary Islands, Spain.
- 2009/12/12 **Improved Garbled Circuit Building Blocks and Applications to Auctions and Computing Minima**, *International Conference on Cryptology And Network Security (CANS'09)*, Kanazawa, Japan.
- 2009/09/22 **Secure Evaluation of Private Linear Branching Programs with Medical Applications**, *European Symposium on Research in Computer Security (ESORICS'09)*, Saint Malo, France.
- 2009/06/02 **Practical Secure Evaluation of Semi-Private Functions**, *International Conference on Applied Cryptography and Network Security (ACNS'09)*, Paris, France.
- 2009/05/28 **Practical Secure Evaluation of Semi-Private Functions**, *Workshop on Cryptographic Protocols and Public-Key Cryptography (WPK'09)*, Bertinoro, Italy.
- 2009/04/26-30 **Automatic Generation of Sound Zero-Knowledge Protocols**, *Advances in Cryptology – EUROCRYPT'09 Poster Session*, Cologne, Germany.  
Poster presented together with Stephan Krenn.
- 2008/12/05 **Generalized Universal Circuits for Secure Evaluation of Private Functions with Application to Data Classification**, *International Conference on Information Security and Cryptology (ICISC'08)*, Seoul, Korea.
- 2008/07/07 **Improved Garbled Circuit: Free XOR and Applications**, *International Colloquium on Automata, Languages and Programming (ICALP'08)*, Reykjavik, Iceland.
- 2008/04/11 **Practical Secure Function Evaluation**, 8. *Kryptotag of the GI special interest group in "Applied Cryptology"*, Tübingen, Germany.
- 2008/01/29 **A Practical Universal Circuit Construction and Secure Evaluation of Private Functions**, *International Conference on Financial Cryptography and Data Security (FC'08)*, Cozumel, Mexico.