Thomas Schneider

Curriculum Vitae (Online Version)

Last changed: September 16, 2019

Personal Data

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, Technische Universität 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, Technische Universität 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), Technische Universität Darmstadt, Germany.

2011/03-09 **Postdoctoral Researcher**, *System Security Lab (headed by Prof. Dr.-Ing. Ahmad-Reza Sadeghi), Center for Advanced Security Research Darmstadt (CASED)*, Technische Universität Darmstadt, Germany.
Worked in EU research project TCLOUDS (see list of projects below).

2008/04-2011/02 **Doctoral Researcher**, *System Security Lab (headed by Prof. Dr.-Ing. 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. Dr.-Ing. Jürgen Teich), 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 and Funding

2020-2025 ERC Starting Grant Privacy-preserving Services On The Internet (PSOTI) funded by the European Research Council (ERC), principal investigator, `https://encrypto.de/PSOTI`

since 2019 Doctoral College Privacy and Trust for Mobile Users funded by the German Research Foundation (DFG), principal investigator, `http://www.privacy-trust.tu-darmstadt.de`

since 2017 Intel Collaborative Research Institute for Collaborative Autonomous & Resilient Systems (ICRI-CARS), associated principal investigator, `https://icri-cars.org`

since 2015 National Research Center for Applied Cybersecurity 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

since 2015 Profile Area CYSEC at Technische Universität Darmstadt, member of the steering board, responsible for gender equality and Claude Shannon fellow research groups, http://www.cysec.tu-darmstadt.de

since 2014 Collaborative Research Center Cryptography-Based Security Solutions (CROSSING) funded by the German Research Foundation (DFG), principal investigator and responsible for family-friendliness and gender equality, http://www.crossing.tu-darmstadt.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 (TCLOUDS), 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

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. Dr.-Ing. Ahmad-Reza Sadeghi (Ruhr-University Bochum, now at TU Darmstadt); External referee: Prof. Dr. Benny Pinkas (Bar-Ilan University, Ramat Gan, Israel)

2003/10-2008/03 **Dipl.-Inf. (Univ.) (M.Sc. in Computer Science) with distinction**,
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. Dr. 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. Dr.-Ing. Jürgen Teich (Friedrich-Alexander University Erlangen-Nürnberg)

1993-2002 **Abitur (Baccalaureate) with distinction**, *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, Scholarships, and Travel Grants

Honors and Awards

2019 **ERC Starting Grant**.

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 Prize for IT-Security 2016**, *Our submission "Praktikable Private Schnittmengenberechnung" was among the 9 finalists chosen from 45 submissions*.

2012 **Intel Early Career Faculty Honor Program Award**.

2012 **Science Award in Data Protection and Data Security of the German Association for Data Protection and Data Security (GDD)**, Köln.

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 PhD Award IT Security (CAST Promotionspreis IT-Sicherheit)**, Darmstadt.

2011 **Best Paper Award 12. Communications and Multimedia Security Conference (CMS'11)**, *Twin Clouds: Secure Cloud Computing with Low Latency by Sven Bugiel, Ahmad-Reza Sadeghi, Thomas Schneider, Stefan Nürnberger*.

2009 **Research School Section Days**, *poster prize*, Ruhr-University Bochum.

2008 **Finalist CAST B.Sc. Award IT Security (CAST Förderpreis IT-Sicherheit, Kategorie Bachelor- und Studienarbeiten)**, Darmstadt.

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*, Paderborn.

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*, scholar.

2004-2008 **German National Academic Foundation (Studienstiftung des Deutschen Volkes)**, scholar, 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)**, scholar.

Travel Grants

2011 **1st Bar-Ilan Winter School: Secure Computation and Efficiency**, *stipend*, Bar-Ilan University, Israel.

2010-2011 **Rectorate Program for Special Activities of PhD Students**, *travel grant*, Ruhr-University Bochum.

2010 **ACM CCS'10**, *student travel grant*.

2010 **Summer School on Applied Cryptographic Protocols**, *stipend*, ECRYPT II.

2009 **CANS'09**, *travel grant*.

2009 **German Academic Exchange Service (DAAD)**, *travel grant*.

2008-2009 **Rectorate Program for Special Activities of PhD Students**, *grant for research collaboration with Bell Labs, NJ, USA*, Ruhr-University Bochum.

Scientific Service

TPMPC (Theory and Practice of Multi-Party Computation Workshops) member of the steering committee, `http://www.multipartycomputation.com`

Reviewer for Swiss National Science Foundation 2019

Reviewer for ERC Starting Grants 2018

PETS '16 (16. Privacy Enhancing Technologies Symposium) family support chair

CAST Förderpreis IT-Sicherheit '19 '16 '14 (CAST IT Security Award) external reviewer

ACM CCS '13 (20. ACM Conference on Computer and Communications Security) poster & demo co-chair, session chair (Session 7-B Privacy-Preserving Protocols)

TRUST '13 (6. International Conference on Trust & Trustworthy Computing) publicity co-chair (technical strand)

Program Committee Member

ACM ASIACCS '18 '17 (ACM Asia Conference on Computer and Communications Security, CORE rank B)

ACM CCSW '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 '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)

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 B)

IEEE ICIP '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)

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

PPML '19 (Privacy Preserving Machine Learning – CCS 2019 Workshop)

TrustED '12 (International Workshop on Trustworthy Embedded Devices)

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

Reviewer for Journals

ACM CSUR '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 '19 (IEEE Transactions on Dependable and Secure Computing, CORE rank A*)

IEEE TIFS '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 '16 (IEEE Transactions on Mobile Computing, CORE rank A*)
IJIS '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 '18 '12 '10 (Journal of Cryptology, CORE rank A*)
SCN '15 (Security and Communication Networks)

External Reviewer

ACISP '16 (Australasian Conference on Information Security and Privacy)
ACM ASIACCS '12 (ACM Information, Computer and Communications Security, CORE rank B)
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 SIGHIT International Health Informatics Symposium)
ACM IH&MMSEC '13 (ACM Workshop on 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 Conference)
CRYPTO '19 '17 '16 '14 '12 '11 (Cryptology Conference, CORE rank A*)
ESORICS '12 '11 (European Symposium on Research in Computer Security, CORE rank A)
FC '11 '10 (Financial Cryptography and Data Security, CORE rank B)
ICISC '10 '09 (International Conference on Information Security and Cryptology, CORE rank B)
IEEE S&P '15 (IEEE Symposium on 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

WS 2019 **Integrated Course**, *Digitaltechnik*, `https://encrypto.de/DT`, Technische Universität Darmstadt, Germany.

since WS 2018 every term — **(Project) Lab**, *Development for Protecting Privacy (PRIVDEV)*, `https://encrypto.de/PRIVDEV`, Technische Universität Darmstadt, Germany.

since 2018 every summer term — **Lecture & Exercise**, *Cryptographic Protocols (CRYPROT)*, `https://encrypto.de/CRYPROT`, Technische Universität Darmstadt, Germany.

since 2018 every term — **Advanced Seminar**, *Cryptography and Privacy Engineering (ENCRYPTO)*, `https://encrypto.de/OS-ENCRYPTO`, Technische Universität 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.

2015-2018 every winter term — **Seminar**, *Privacy Preserving Technologies (PRIVTECH)*, `https://encrypto.de/PRIVTECH`, Technische Universität Darmstadt, Germany.

2015/09 — **Invited Lecturer**, *Summer School on Secure and Trustworthy Computing*, University Politehnica of Bucharest, Romania, Title: Practical Aspects of Secure Two-Party Computation.

2015/02 — **Invited Lecturer**, *5. Bar-Ilan Winter School: Advances in Practical Multiparty Computation*, Bar-Ilan University, Israel, lecture slides: Optimizations of Yao's Protocol for Semi-Honest Adversaries.

2011/09 — **Invited Lecturer**, *6. European Trusted Infrastructure Summer School (ETISS)*, Darmstadt, Germany, Title: Hardware-assisted Cryptographic Protocols.

2011 — **Lecturer**, *Center for Advanced Security Research Darmstadt (CASED)*, Technische Universität Darmstadt, Germany, PhD Seminar (co-organized with Prof. Dr.-Ing. Ahmad-Reza Sadeghi and Prof. Dr. 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. Dr. Volker Strehl.

2005 — **Trainer** in one-week course about youth group leading.

1998-2008 — **Private Tutor** for mathematics and physics (classes 5-13).

Supervised PostDocs

since 2018/11 — **Daniel Demmler**, full position.

Supervised PhD Students

since 2019/06 — **Hossein Yalame**, *PhD applicant*, Working Title: tbd, full position.

since 2018/07 — **Amos Treiber**, *PhD applicant*, Working Title: Mechanisms for Protecting Privacy in Applications, full position.

since 2017/10 — **Oleksandr Tkachenko**, *PhD applicant*, Working Title: Efficient Outsourcing and Multi-Party Computations, full position.

since 2016/09 — **Christian Weinert**, *PhD applicant*, Working Title: Privacy-Preserving Protocols at Scale, full position; winner of CROSSING Collaboration Award 2017.

since 2015/02 — **Ágnes Kiss**, *PhD applicant*, Working Title: Practical Aspects of Private Function Evaluation, full position; 3. Prize CAST M.Sc. IT Security Award 2015; invited to Heidelberg Laureate Forum 2018; winner of CROSSING Collaboration Award 2019.

2013/10-2018/11 — **Daniel Demmler**, *PhD with distinction*, Towards Practical Privacy-Preserving Protocols, full position; winner of CROSSING Collaboration Awards 2016 and 2017; award for the best dissertation at the CS department of TU Darmstadt in 2018 by "Friends of TU Darmstadt e.V.".

2012/07-2016/12 **Michael Zohner**, *PhD with distinction*, Faster Oblivious Transfer Extension and its Impact on Secure Computation, full position; winner of CROSSING Collaboration Award 2016; now Security Engineer at Continental.

External Referee of PhD Theses

Beyond the PhD theses listed above and below, I was also part of 18 internal PhD committees at TU Darmstadt.

2019 **Mark Simkin**, *PhD*, Alice, Bits, and Bob, University of Aarhus, Denmark; supervisor: Prof. Dr. Ivan Damgård.

2019 **Tim Wood**, *PhD applicant*, Reducing Communication Costs in Multi-Party Computation, KU Leuven, Belgium; supervisor: Prof. Dr. Nigel Smart.

2017 **Per Hallgren**, *PhD*, Provable Privacy for Location-Based Services, Chalmers University of Technology, Gothenburg, Sweden; supervisor: Prof. Dr. Andrei Sabelfeld.

2016 **Carsten Baum**, *PhD*, Towards More Efficient Secure Multiparty Computation in the Preprocessing Model, University of Aarhus, Denmark; supervisor: Prof. Dr. Ivan Damgård.

2016 **Rasmus Winther Zakarias**, *PhD*, Practical Secure Computation with Pre-Processing, University of Aarhus, Denmark; supervisor: Prof. Dr. 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. Dr. Jesper Buus Nielsen.

2014 **Ayman Jarrous**, *PhD*, Applied Secure Multi-Party Computation, University of Haifa, Israel; supervisor: Prof. Dr. Benny Pinkas.

Supervised Master Theses

since 2019 **Daniel Günther**, *Efficient Private Checks for Leaked Passwords*, M.Sc., co-supervised with Prof. Dr. Benny Pinkas.

since 2018 **Marco Holz**, *M.Sc. applicant*, A Systematic Comparison of Private Function Evaluation Protocols, co-supervised with Ágnes Kiss.

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.
Results published at USENIX Security'19; award for excellent M.Sc. thesis by "Friends of TU Darmstadt e.V." 2019.

2017-2018 **Masaud Y. Alhassan**, *M.Sc.*, Improving Scalability of Universal Circuits for Large-Scale Private Function Evaluation, co-supervised with Ágnes Kiss.

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. Dr. 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. Dr.-Ing. Ahmad-Reza Sadeghi (Ruhr-University Bochum, Germany) and Prof. Dr. Benny Pinkas (University of Haifa, Israel).
Results published at ACNS'09 and WIFS'09. Finalist CAST M.Sc. Award IT Security 2009.

Supervised Bachelor Theses

since 2019 **Tom Florian Schuster**, *B.Sc. applicant*, Optimizing HyCC with Compiler Intermediate Representation, co-supervised with Christian Weinert.

since 2019 **Martin Kromm**, *B.Sc. applicant*, 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 at USENIX Security'18 poster session.

2016-2017 **Daniel Günther**, *B.Sc.*, Valiant's Universal Circuit - Towards a Modular Construction and Implementation, co-supervised with Ágnes Kiss.
Results published at ASIACRYPT'17 and presented at 29. Kryptotag; 1. Prize CAST B.Sc. Award IT Security 2018.

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. Dr.-Ing. Ahmad-Reza Sadeghi.
Results published at ICISC'09 and ACM CCS'10.

Supervised Student Assistants

2009-2011 **Stefan Kögl**, *Computer Aided Cryptography Engineering (CACE)*, professional practical trainee and student assistant.
Results published at ACM 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 ICISC'09 and ACM CCS'10.

2008-2009 **Wilko Henecka**, *Computer Aided Cryptography Engineering (CACE)*, student assistant.
Results published at EUROPKI'09, ESORICS'10, and ACM CCS'10. Contributed to many other publications on zero-knowledge and secure function evaluation.

Long-term Visitors

2019/05-07 **Deevashwer Rathee**, research intern, Indian Institute of Technology (BHU), Varanasi, India.
Results published at CANS'19.

2017/10-11 **Zheng Yang, PhD**, *Location Privacy*, visiting researcher, University of Helsinki, Finland.
Results published at ICL-GNSS'18, CANS'18, and EuroS&P'19.

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 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 LaTeX, Microsoft Office, UML, VHDL

operating systems Mac, Linux, Windows

List of References

Available upon request.

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`

DBLP: `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) 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)***, 2019. Full version: `https://arxiv.org/abs/1906.04862`. Code: `https://encrypto.de/code/SPOCattack`. To appear. CORE rank A*. doi:10.1109/TPDS.2019.2939313.

2) 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. Petrovska-Delacrétaz, 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, June 8, 2019. CORE rank A. doi:10.1016/j.csl.2019.06.001.

3) 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 21.1%. CORE rank B. doi:10.2478/popets-2019-0026.

4) 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.

5) 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 21.7%. CORE rank B. doi:10.1515/popets-2017-0044.

6) 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.

7) 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 18.6%. CORE rank B. doi:10.1515/popets-2017-0033.

8) 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 37.9%. CORE rank B. doi:10.1515/popets-2017-0005.

9) 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.

10) 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 and Workshops with Proceedings (all peer reviewed)

11) 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)*, ACM, London, UK, November 11, 2019. To appear. doi:10.1145/3338498.3358646.

12) 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)*, ACM, November 11, 2019. To appear. doi:10.1145/3338466.3358919.

13) 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. 1–13, Springer, Fuzhou, China, October 25-27, 2019. Short paper. To appear. Full version: https://ia.cr/2019/577. CORE rank B. doi:10.1007/978-3-030-31578-8_19.

14) 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. Annual Conference of the International Speech Communication Association (INTERSPEECH'19)***, International Speech Communication Association (ISCA), Graz, Austria, September 15-19, 2019. To appear. Online: https://arxiv.org/abs/1907.03454. CORE rank A.

15) 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: http://contact-discovery.github.io. Full version: https://ia.cr/2019/517. Acceptance rate 16.2%. CORE rank A*.

16) A. Kiss, O. Schick, and T. Schneider, Web application for privacy-preserving scheduling using secure computation. In *16. International Conference on Security and Cryptography (SECRYPT'19)*, pp. 456–463, SciTePress, Prague, Czech Republic, July 26-28, 2019. Short paper. Code: https://encrypto.de/code/scheduling. Acceptance rate 15.2%. CORE rank B. doi:10.5220/0007947704560463.

17) T. Schneider and O. Tkachenko, EPISODE: Efficient Privacy-PreservIng Similar Sequence Queries on Outsourced Genomic DatabasEs. In *14. ACM Asia Conference on Information, Computer and Communications Security (ASIACCS'19)*, pp. 315–327, ACM, Auckland, New Zealand, July 7-12, 2019. Acceptance rate 17.1%. CORE rank B. doi:10.1145/3321705.3329800.

18) 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)*, IEEE, Stockholm, Sweden, June 17-19, 2019. To appear. Acceptance rate 20.0%.

19) B. Pinkas, T. Schneider, O. Tkachenko, and A. Yanai, Efficient circuit-based PSI with linear communication. In ***38. Advances in Cryptology – 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.

20) 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.

21) 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. Acceptance rate 36.5%. doi:10.1145/3267323.3268956.

22) 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.

23) F. Brasser, T. Frassetto, K. Riedhammer, A.-R. Sadeghi, T. Schneider, and C. Weinert, VoiceGuard: Secure and private speech processing. In ***19. Annual 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 44.9%. CORE rank A. doi:10.21437/Interspeech.2018-2032.

24) 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.

25) 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 Information, Computer and Communications Security (ASIACCS'18)*, pp. 221–235, ACM, Songdo, South Korea, June 4-8, 2018. Acceptance rate 16.8%. CORE rank B. doi:10.1145/3196494.3196541.

26) 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 Information, 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 B. doi:10.1145/3196494.3196522.

27) B. Pinkas, T. Schneider, C. Weinert, and U. Wieder, Efficient circuit-based PSI via cuckoo hashing. In ***37. Advances in Cryptology – 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. Acceptance rate 23.0%. CORE rank A*. doi:10.1007/978-3-319-78372-7_5.

28) 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. Acceptance rate 18.1%. CORE rank A. doi:10.1145/3143361.3143362.

29) D. Günther, A. Kiss, and T. Schneider, More efficient universal circuit constructions. In ***23. Advances in Cryptology – ASIACRYPT'17***, vol. 10625 of *LNCS*, pp. 443–470, Springer, Hong Kong, China, December 3-7, 2017. Full version: https://ia.cr/2017/798. Acceptance rate 27.6%. CORE rank A. doi:10.1007/978-3-319-70697-9_16.

30) D. Demmler, K. Hamacher, T. Schneider, and S. Stammler, 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.

31) 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://encrypto.de/code/onionPIR. Acceptance rate 22.8%. CORE rank B. doi:10.1007/978-3-319-61204-1_30.

32) J. B. Nielsen, T. Schneider, and R. Trifiletti, Constant round maliciously secure 2PC with function-independent preprocessing using LEGO. In ***24. Annual 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.

33) 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. Annual 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. Acceptance rate 16.1%. CORE rank A*. doi:10.14722/ndss.2017.23097.

34) 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.

35) E. M. Songhori, S. Zeitouni, G. Dessouky, T. Schneider, A.-R. Sadeghi, and F. Koushanfar, GarbledCPU: A MIPS processor for secure computation in hardware. In ***53. Annual 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.

36) A. Kiss and T. Schneider, Valiant's universal circuit is practical. In ***35. Advances in Cryptology – 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://encrypto.de/code/UC. Acceptance rate 22.6%. CORE rank A*. doi:10.1007/978-3-662-49890-3_27.

37) 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.

38) 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.

39) 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://encrypto.de/code/PSI. Acceptance rate 15.7%. CORE rank A*.

40) 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.

41) G. Asharov, Y. Lindell, T. Schneider, and M. Zohner, More efficient oblivious transfer extensions with security for malicious adversaries. In ***34. Advances in Cryptology – 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.

42) M. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, and M. Zohner, Ciphers for MPC and FHE. In ***34. Advances in Cryptology – 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.

43) D. Demmler, T. Schneider, and M. Zohner, ABY – a framework for efficient mixed-protocol secure two-party computation. In ***22. Annual 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*.

44) 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.

45) 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*.

46) 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*.

47) 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.

48) 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.

49) 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.

50) 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.

51) 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://thomaschneider.de/papers/ADNRSSS13_TR.pdf. CORE rank B. doi:10.1007/978-3-642-38980-1_27.

52) W. Henecka and T. Schneider, Faster secure two-party computation with less memory. In *8. ACM 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 B. doi:10.1145/2484313.2484369.

53) 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 B. doi:10.1007/978-3-642-39884-1_23.

54) 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 B. doi:10.1007/978-3-642-32946-3_22.

55) 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.

56) 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. Acceptance rate 14.0%. CORE rank A*. doi:10.1145/2046707.2046753.

57) 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.

58) 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.

59) 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.

60) 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.

61) 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.

62) 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.

63) 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.

64) 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 B. doi:10.1007/978-3-642-14577-3_17.

65) 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.

66) B. Pinkas, T. Schneider, N. P. Smart, and S. C. Williams, Secure two-party computation is practical. In ***15. Advances in Cryptology – 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.

67) 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.

68) 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%. CORE rank B. doi:10.1007/978-3-642-14423-3_16.

69) 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.

70) 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.

71) 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://encrypto.de/code/FairplaySPF. Acceptance rate 21.3%. CORE rank B. doi:10.1007/978-3-642-01957-9_6.

72) 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.

73) 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%. CORE rank B. doi:10.1007/978-3-642-00730-9_21.

74) 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.

75) 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://encrypto.de/code/FairplayPF`. Acceptance rate 19.1%. CORE rank B. doi:10.1007/978-3-540-85230-8_7.

Patents

76) 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 October 24, 2008; issued May 14, 2013), May 14, 2013.

77) V. Kolesnikov and T. Schneider, Universal circuit for secure function evaluation. U.S. patent no 8175854 (applied July 14, 2008; issued May 8, 2012), May 8, 2012.

Books and Book Chapters

78) 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.

79) 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.

Workshops without Proceedings

80) D. Demmler, T. Schneider, and M. Zohner, Hardware-assisted ad-hoc secure two-party computation on smartphones. In *19. Workshop der Fachgruppe Kryptographie in der Gesellschaft für Informatik (Kryptotag)*, Stuttgart, Germany, November 14-15, 2013.

81) T. Schneider and M. Zohner, Efficient secure two-party computation. In *17. Workshop der Fachgruppe Kryptographie in der Gesellschaft für Informatik (Kryptotag)*, Heidelberg, Germany, December 7, 2012.

82) 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.

83) 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.

84) 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.

85) 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.

86) 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.

87) V. Kolesnikov, T. Schneider, and V. Strehl, Practical secure function evaluation. In *8. Workshop der Fachgruppe Kryptographie in der Gesellschaft für Informatik (Kryptotag)*, vol. WSI-2008-02, Tübingen, Germany, April 11, 2008.

Posters/Demos and Short Talks

88) 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, Privacy-preserving speech processing via STPC and TEEs. 2. Privacy Preserving Machine Learning (PPML'19) – CCS 2019 Workshop, London, UK, November 15, 2019. Poster. To appear. Acceptance rate 63.2%.

89) D. Günther, A. Kiss, L. Scheidel, and T. Schneider, Framework for semi-private function evaluation with application to secure insurance rate calculation. **26. ACM Conference on Computer and Communications Security (CCS'19) Posters/Demos**, London, UK, November 11-15, 2019. Acceptance rate 67.2%. CORE rank A*.

90) A. Kiss, O. Schick, and T. Schneider, 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*.

91) F. Kerschbaum, T. Schneider, and A. Schröpfer, Automatic protocol selection in secure two-party computations. **20. Network and Distributed System Security Symposium (NDSS'13)**, San Diego, CA, USA, February 24-27, 2013. Short Talk. CORE rank A*.

92) E. Bangerter, S. Krenn, A.-R. Sadeghi, and T. Schneider, 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*.

93) A.-R. Sadeghi and T. Schneider, 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).

94) E. Bangerter, J. Camenisch, S. Krenn, A.-R. Sadeghi, and T. Schneider, Automatic generation of sound zero-knowledge protocols. **28. Advances in Cryptology – 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*.

95) T. Schneider, Practical secure function evaluation. In *Fachwissenschaftlicher Informatik-Kongress (Informatiktage 2008)*, vol. S-6 of *LNI*, pp. 37–40, GI, Bonn, Germany, March 14, 2008.

Technical Reports and Preprints

96) M. Y. Alhassan, D. Günther, A. Kiss, and T. Schneider, Efficient and scalable universal circuits. Cryptology ePrint Archive, Report 2019/348, 2019. `https://ia.cr/2019/348`. In submission.

97) 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.

Theses

98) 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.

99) T. Schneider, Practical secure function evaluation. Master's thesis, Friedrich-Alexander University Erlangen-Nürnberg, Germany, February 27, 2008.

100) 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

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**, *Technische Universität 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.

2015/06/08-12 **ABY - A Framework for Efficient Mixed-Protocol Secure Two-Party Computation**, *Securing Computation Workshop*, Berkeley, USA.

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.

2011/08/08 **Engineering Cryptographic Protocols (ENCRYPTO)**, *EC SPRIDE Colloquium, Technische Universität 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

I strongly encourage students to give the conference presentations of our papers whenever possible.

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.