Curriculum Vitae

Prof. Christof Paar

christof.paar@rub.de

Categories

- Personal
- Education
- Employment
- External Offers
- Chief Officer and Board Functions
- Fellowships and Awards
- Teaching-Related Awards
- External Funding
- Teaching
- Ph.D. Students Advised
- External Member in Ph.D. and Habilitation Committees
- Conference and Workshop Involvement
- University Service
- Other

Personal

DOB:	July 18, 1963, in Cologne, Germany
Martial status:	married, three children

Education

7.91-7.94	Digital Communications Group, Institute for Experimental Mathematics, Univ. of Essen, Germany, Dr.-Ing. (Advisor: Prof. Han Vinck) *Dissertation*: “Efficient VLSI Architectures for Bit-Parallel Arithmetic in Galois Fields”
1993, 1994	University of Massachusetts at Amherst, three research visits
11.90-5.91	Michigan Technological University, graduate research
8.89-5.91	University of Siegen, Germany, Dipl-Ing. Electrical Engineering
10.84-5.88	Cologne University of Applied Sciences, Dipl.-Ing. Electrical Engineering

Employment

7.2019–	Co-Founding Director of the Max Planck Institute for Cybersecurity & Privacy
10.01–6.2019	Chair for Embedded Security, Ruhr University Bochum
9.08-8.09 2.14-2.16	Research Professor at the University of Massachusetts at Amherst (sabbaticals)
9.09–	Affiliated Professor at the University of Massachusetts at Amherst
7.04-6.07 7.10-4.12 4.16-11.17	Director of the Horst Görtz Institute for IT Security, Ruhr University Bochum
7.02-6.07	Affiliated Professor, ECE Dept., Worcester Polytechnic Institute, USA
1.95-6.01	Assistant and Associate Professor (tenured), ECE Dept., WPI, USA (since 1998 joint appointment in the Computer Science Dept.)
1997–	Consultant in the area of information security for: Bosch, cryptovision, Fraunhofer Gesellschaft, Giesecke & Devrient, Greylock, NTRU, Philips Research, Polaroid, secunet AG, Ventizz, and others
6.88-5.89	Development engineer for embedded systems (part time)
9.88-12.89	Social service, research assistant in hearing disorder projects, Audiology Dept., University Hospital of Cologne, Germany
8.79-1.83	Apprenticeship as telecommunication technician

External Offers

2007	Offer of the Chair for Embedded System Security, Technical University of Eindhoven, The Netherlands (declined)
2005	Offer to become the founding director of the Fraunhofer Institute for Hardware Security, Munich, Germany (declined)

Fellowships and Awards

2017	IACR Fellow (International Association for Cryptologic Research)
2016	ERC Advanced Grant (2.5m €)
2016	Black Hat Conference “Pwnie Award for Best Cryptographic Attack” (with co-authors)
2013	*DHL Innovation Award 2013* (with G. Leander and A. Poschmann) (€10k)
2012	*Innovationspreis NRW 2012* by the state of North Rhine-Westphalia (€100k)
2012	Best Paper Award at the *IEEE Symposium on Security & Privacy*
2011	*IEEE Fellow*
2010	*Deutscher IT-Sicherheitspreis 2010* (with G. Leander and A. Poschmann), for the development of the lightweight cipher PRESENT (€100k)
2006	*RUBITEC Technology Transfer Award* (€10k)
1998	NSF *CAREER Award* ($210k)
1996	Satin Distinguished Fellowship Award for outstanding research and teaching ($18k)
1990	Fellowship from the Friedrich-Ebert Foundation

Teaching-Related Awards

2014	Advisor of the Eickhoff Dissertation Award (award for outstanding dissertations linking science and applications)
2012	Advisor of the 1st prize CAST Forum PhD Thesis Award (Germany /Austria/Switzerland-wide competition for dissertations in IT-Security)
2007	Advisor of the Eickhoff Dissertation Award (award for outstanding dissertations linking science and applications)
2006	in the Top 10 of the Germany-wide “Professor of the Year” competition, category Engineering and Computer Science.
2006	Advisor of the 1st prize of the CAST Forum MS Thesis Award (Germany/Austria/Switzerland-wide competition for theses in IT-Security)
2005	Advisor of the Gert Massenberg Foundation Dissertation Award (best engineering Ph.D. thesis at U. Bochum)
2000	Advisor of the Sigma Xi MS research award (best MS Thesis at WPI)
1999	Advisor of 1st ranked Major Qualifying Project (senior thesis), ECE Dept., WPI
1998	Advisor 1st ranked Major Qualifying Project (senior thesis), CS Dept., WPI

Chief Officer, Advisory Functions and Spin-offs

2004	Co-founder of ESCRYPT GmbH – Embedded Security, Germany and USA ESCRYPT was acquired by Bosch in 2012
2003-2007	Managing Director of ESCRYPT *GmbH – Embedded Security*
2003-2006	CTO, *isits AG* – International School for IT Security, Germany
2006–2012	Board of Directors, *Card Factory*, Germany
2001–2003	Board of Directors, *Eracom Technologies*, Australia and Germany
2012–2018	Advisory Board, *Fraunhofer Institute for Applied & Integrated Security*, Munich
2008–	Technical Advisory Board, *Intrinsic ID*, USA and The Netherlands

2012–2018	Technical Advisory Board, *Chaologix*, USA
2000–2002	Technical Advisory Board, *rTrust Inc*., USA
1999–2003	Technical Advisory Board, *cv cryptovision*, Germany

2019	Co-founder emproof GmbH
2016	Co-founder of PHYSEC GmbH
2014	Co-founder of Kasper-Oswald GmbH
2008	Co-founder of SciEngines GmbH

External Funding: Research Grants
(Dollar and Euro amounts represent the share of C. Paar unless indicated otherwise)

Doctoral Schools

Fortschrittskolleg NRW “Brave New World: Security for Humans in Cyberspace (SecHuman)”, 2016 (3,000k €) and 2019 (2,000k €) (Spokesperson, with 13 co-PIs)

DFG Graduiertenkolleg “New Challenges for Cryptography in Ubiquitous Computing”, 2012, total: 4,200k € (Spokesperson, with 9 co-PIs)

ECRYPT-NET, European Innovative Training Network, 2015-2019, 498k € (total 3,900k €), (co-PI)

DFG (German National Science Foundation)

Cluster of Excellence "Cyber Security in the Age of Large-Scale Adversaries (CaSa)", 2019, total 35m € (with Th. Holz and E. Kiltz)

“Nano-Scale Side-Channel Analysis”, 2016, total: 476k € (with Dr. A. Moradi)

“CyPhyCrypt: Advanced Crypto for New and Next-Generation Cyber-Physical Systems”, 2016, total: 445k € (with Dr. Andy Rupp)

“Implementional Aspects of Alternative Asymmetric Crypto Algorithms”, 2010, total: 380k € (with Prof. T. Güneysu)

“Dedicated Architectures for Cryptanalysis of RSA and DL-Systems”, 2006-2008, 140k €

“Secure Data and Information Transmission”, Research Training Group Fellowship, 2003-2006, 42k € (co-PI)

NSF (US National Science Foundation)

“Designing Strongly Obfuscated Hardware with Quantifiable Security against Reverse Engineering”, 2016, total: $1,163k (PI, with D. Holcomb and S. Kundu)

“Investigating Stealthy Hardware Trojans”, 2014, total: $500k (PI, with S. Kundu)

“New Directions in Field Programmable Gate Arrays (FPGA) Security”, 2013, total: $432k (co-PI, with R. Tessier)

“Collaborative Research: Pay-as-you-Go: Security and Privacy for Integrated Transportation Payment Systems”, 2009, total: $845k (co-PI, with W. Burleson, J. Collura, K. Fu)

“Minimalist Hardware Trojans through Malicious Side-Channels”, 2009, total: $335k (PI, with W. Burleson)

“Security in Embedded Networks”, 2001, total: $460k
(co-PI, with B. Sunar and B. Martin)

“Instrumentation for Cryptographic Algorithms and Systems on Reconfigurable Hardware”, 1999, $83k (PI)

NSF CAREER Award: “Cryptography on Reconfigurable Hardware: Algorithmic and System Aspects”, 1998, $210k (PI)

European Directorate for Research

ERC Advanced Grant, “Exploring and Preventing Cryptographic Hardware Backdoors: Protecting the Internet of Things against Next-Generation Attacks (EPoCH)”, 2016, 2,499k €

“TETRAMAX, technology transfer for low energy”, 2017-2021, 163k € (total 7,000k €), (co-PI)

“ECRYPT NET European Integrated Research Training Network on Advanced Cryptographic Technologies for the Internet of Things and the Cloud”, 2015-2019, 498k € (share RUB, total 3,890k €), (co-PI)

“ECRYPT CSA – European Coordination and Support Action in Cryptology”, 2015-2018,
172k € (share RUB, total 1,000k €), (co-PI)

“ECRYPT II – European Network of Excellence for Research in Cryptography”, 2008-2012, 200k € (share RUB, total 3,000k €), (co-PI)

“ECRYPT – European Network of Excellence for Research in Cryptography”, 2004-2008, 340k € (share RUB, total 5,400k €), (co-PI)

“STORK – Strategic Roadmap for Cryptography”, 2002, 60k €
(share RUB, co-PI)

“Ubiquitous Sensing and Security in the European Homeland”, 2005-2008, 250k €
(co-PI, with NEC Labs Heidelberg et al.)

BMBF (German Federal Ministry for Research and Education) and
BMWi (German Federal Ministry for Economics and Technology)

BMBF, „Incubator for start-ups in the area of cyber security“, 2017, 1500k €

BMBF, „Computerunterstützte Erzeugung und Verifikation von Maskierungen in kryptographischen Implementierungen”, 2016, 746k €
(co-PI, with NXP, University of Bremen)

BMBF, „Development tools for application-optimized security hardware for Industrie 4.0 Applications”, 2016, 243k €
(co-PI, with NXP, FZi, IMST, Hierschmann, Hochschule Aalen)

BMBF, „INSPECT: Organisierte Finanzdelikte”, 2014, 256k €
(co-PI, with BKA, Wincor-Nixdorf, SBSK GmbH, Uni Magdeburg, TU Darmstadt)

BMBF, “PhotonFX: Photonische Fehler- und Angriffsanalyse von Sicherheitsstrukturen und Sicherheitsfunktionen”, 2013, 358k €,
(co-PI, with TU Berlin, NXP)

BMBF “UNIKOPS: Universell konfgurierbare Sicherheitslösung für Cyber-Physikalische heterogene Systeme”, 2013, 373k €,
(co-PI, with IHP, ESCRYPT, Hochschule Furtwangen)

BMBF “Prophylaxe: Providing Physical Layer Security for the of Things 2013, 152k €,
(co-PI, with Heinrich Hertz Inst., TU Dresden, TU Kaiserslautern, Bosch)

BMWi “Secure eMobility”, 2012, 195k € (total 4,050k €)
(PI, with Daimler, Elmos, ESCRYPT, Smart Labs and Univ. of Applied Sciences Gelsenkirchen)

BMBF “Excellence in Security Evaluation Testing”, 2010, 510k € (total 850k €)
(PI, with T-Systems, TÜV, and Univ. of Applied Sciences Bonn Rhein-Sieg)

BMBF, “Side-Channel Analysis for Automotive Security”, 2010, 288k € (total 1,140k €)
(PI, with Bosch, ESCRYPT, and Univ. of Applied Sciences Bonn Rhein-Sieg)

BMBF, “Methods and Tools for Securing Embedded and Mobile Applications against Next-Generation Attacks”, 2010, 305k €
(co-PI, with BSI, Giesecke & Devrient, Fraunhofer SIT, Infineon, TU Darmstadt et al.)

BMBF “Secure Ad-hoc On Demand Virtual Private Storage”, 2010, 238k €
(co-PI, with Jörg Schwenk, Utimaco, Adesso Mobile Solutions, and TU Dortmund)

BMBF “High Security Intelligent Copyright Protection for Software”, 2010, 113k €
(co-PI, with ESCRYPT)

BMWi “Trusted Computing and Digital Rights Management”, 2005-2007, 240k €
(co-PI, with Ahmad Sadeghi)

BSI (German Federal Agency for IT Security)

“Hardware-supported Factoring”, 2007-2008, 87k (PI)

“High-Performance Reconfigurable Computing”, 2006, 60k (PI)

“Cryptographic Hardware”, 2003, 160k (PI)

„Interdependencies between Critical Infrastructures”, 2002, 40k (PI)

„Evaluation of Reconfigurable Hardware for Cryptographic Applications”, 2002, 35k (PI)

Industry and other funding sources

NXP, “Memory Encryption”, 2011, 300k € (PI, with TU Denmark)

SRC, “Sub-45nm Circuit Design for True Random Number Generation and Chip Identification, 2010, total: $300k (co-PI, with Wayne Burleson)

CISCO, “Alternate Public Key Cryptosystems”, 2009, $60k (PI, with Wayne Burleson)

IT Department of the German Armed Forces, “RFID Security in Defense Applications”, 2009, 209k € (PI)

NXP, “Analysis of Contactless Payment Tokens”, 2009, 25k € (PI)

Hörmann KG, “Secure Keyless Entry Systems”, 2009, 23k € (PI)

Printed Systems GmbH, “Security of printed electronics”, 2008, 20k € (PI)

Cynops GmbH, “Hardware-based Password Search”, 2008, 7,500 € (PI)

Novoferm GmbH, “Secure Keyless Entry Systems”, 2008, 15k € (PI)

Scienengine GmbH, “FPGA-based Supercomputers”, 2008, 45k € (PI)

Undisclosed Sponsor, “Hardware-based Reverse Engineering”, 2008, 45k € (PI)

ESCRYPT GmbH, „Pay-TV Security“, 2007, 30k € (PI)

State of North-Rhine Westphalia, Staatskanzelei “IT Security in NRW: State-of-the-art and Development Opportunities“, 2007, 28k € (PI)

NTRU, “High Speed Elliptic Curve Cryptography”, 2007, undisclosed funding

Research Ministry of the State of North-Rhine Westphalia “GRID Computing for Small and Medium Industries”, 2004-2006, 40k € (PI)

BKA (German Federal Bureau of Investigation), Data Recovery, 2004-2005, undisclosed funding

Infineon, “Security for Mobile Devices”, 2004, undisclosed funding

Blaupunkt/Bosch, “Cryptography in Infotainment Applications”, 2003, undisclosed funding

Research Ministry of the State of North-Rhine Westphalia “CHES Portal and other IT Security Coordination Tasks”, 2002, 60k € (PI)

SUN Labs, “Efficient Hardware and Software Algorithms for Pervasive Computing Applications”, 2002-2005, $150k (PI)

Eracom Technologies, “Future Trends in Data Security”, 2002, 5k € (PI)

SUN Labs, “Software Library for eCommerce Applications between Servers and PDAs”, 2000, $30k (PI)

General Dynamics, “GD Trusted Network Systems Centre at WPI”, 1999-2001, $80k (PI)

Texas Instruments DSP University Research Program: “Security Library for TI Digital Signal Processors”, 1998, $150k (PI)

Technical Communications Corporation, “Design and Implementation of a Public-Key System on Embedded Systems”, 1998, $92k (PI)

Bosch Backnang, “FPGAs as cryptography components”, 1997, $15k (PI)

GTE Government Systems, “Protocol Aspects of Elliptic Curve Cryptosystems”, 1996, $18k (PI)

Lockheed Martin, “Security in ATM Networks”, 1996, $42k (PI)

External Funding: Graduate Fellowships

Bosch, “Security Aspects of FPGA-Designs and Embedded Software“, Hans L. Merkle doctoral research program, 135k €

GTE CyberTrust , “GTE Graduate Fellowship for Research in Cryptography”, 1996-2000, $80k

USENIX, “Graduate Fellowship for Research in Security for Embedded Internet Devices“, 2000, $31k

Secunet AG, “Secunet IT Security Fellowship”, 1998, $25k

Teaching: Higher Education

Undergraduate courses:

Introductory Physics (Cologne College for Nurses)

Introduction to VLSI Design (WPI)

Continues-Time Signal and System Analysis (WPI)

Introduction to Cryptography and Data Security I and II (U. Bochum)

Programing Languages: C and Assembly (U. Bochum)

Graduate courses:
Computer and Communication Networks (WPI)
Advanced VLSI Design Techniques (WPI)
Cryptography and Data Security (WPI)
Selected Topics in Cryptography (WPI)
Implementation of Cryptographic Algorithms I (U. Bochum)
Implementation of Cryptographic Algorithms II (U. Bochum)
Security Engineering (UMass Amherst)
Cryptographic Engineering (UMass Amherst)
Introduction to Cryptography (UMass Amherst)

Teaching: Continuing Education

since 2002 annual MEAD-Course „Cryptographic Engineering“, *EPFL Lausanne*, Switzerland

2003–2012 annual course “Introduction to Cryptography”, ALaRI International Master’s Program, *University of Lugano*, Switzerland

9.04 Summer School “Elliptic Curve Cryptography”, *Ruhr University Bochum*, 5 day course, coordinator and lecturer

11.02 “Mobile Security”, 3 day course, *Motorola Research*, Paris, France

2002, 2003 “Kryptographie und Datensicherheit“, 3 day course, *Center for IT Security*, Germany

1997-2001 “Introduction to Cryptography and Data Security”, annual 4-day course, *WPI* Continuing Education Department

11.96 “Cryptography and Data Security”, 4-day course, *Philips Research*, NY

9.97 “Cryptography and Data Security”, 4-day course, *NASA Lewis Research Center*, OH

1998 “Applied Cryptography”, 2 months, *Technical Communications Corporation*, MA

Teaching: Ph.D. Students Advised (with thesis title and current employer)

Since 2002 I have graduated 28 Ph.D. students at Ruhr Univ. Bochum, Univ. of Massachusetts Amherst and Worcester Polytechnic Institute. Six of them have become assistant or associate professors in Denmark, England, Germany, Singapore and the USA.

Falk Schellenberg (RUB, 11/2018), Novel Methods of Passive and Active Side-Channels Attacks, Postdoc Ruhr-Universität Bochum

Pawel Swierczynski (RUB, 9/2017), Bitstream-based Attacks against Reconfigurable Hardware, Senior Researcher ESMT Berlin

Christian Zenger (RUB, 1/17), Physical-Layer Security for the Internet of Things
CEO PHYSEC GmbH, a technology start-up

Gesine Hinterwälder (Univ. of Massachusetts, 3/15), Privacy-Preserving Payments for Transportation Systems, NXP

Elif Kavun (RUB, 1/15), Resource-efficient Cryptography for Ubiquitous Computing, University of Sheffield (Assistan Professor)

Daehyun Strobel (RUB, 10/14), Novel Applications for Side-Channel Analyses of Embedded Microcontrollers, ESCRYPT GmbH

Georg T. Becker (Univ. of Massachusetts, 12/13), Intentional and Unintentional Side-Channels in Embedded Systems, Digital Society Institute of the EMST Berlin

Stefan Heyse (RUB, 11/13), Post Quantum Cryptography: Implementing Alternative Public Key Schemes on Embedded Devices, NXP

David Oswald (RUB, 9/13), Implementation Attacks: From Theory to Practice, University of Birmingham (Assistant Professor)

Benedikt Driessen (RUB, 7/13), Practical Cryptanalysis of Real-World Systems, Consultant

Timo Kasper (RUB, 9/11), Security Analysis of Pervasive Wireless Services
CEO Kasper-Oswald GmbH, a technology start-up

Thomas Eisenbarth (RUB, 7/09), Cryptography and Cryptanalysis for Embedded Systems, University of Lübeck (W3)

Andrey Bogdanov (RUB, 7/09), Analysis and Design of Block Cipher Constructions, TU Denmark (Associate Professor)

Martin Novotny (RUB, 4/09), Time-Area Efficient Hardware Architectures for Cryptography and Cryptanalysis. Technical University of Prague (Instructor)

Axel Poschmann (RUB, 4/09), Lightweight Cryptography – Cryptographic Engineering for a Pervasive World. Dark Matters

Tim Güneysu (RUB, 2/09), Cryptography and Cryptanalysis on Reconfigurable Devices. Ruhr University Bochum (Full Professor)

Andy Rupp (RUB, 11/08), Computational Aspects of Cryptography and Cryptanalysis. KIT (post-doc)

Marko Wolf (RUB, 4/08), Security Engineering for Vehicular Systems -- Improving Trustworthiness and Dependability of Automotive IT Applications, ESCRYPT GmbH.

Kerstin Lemke-Rust (RUB, 6/07), Models and Algorithms for Physical Cryptanalysis. University of Applied Sciences Bonn-Rhein-Sieg (Associate Professor)

Kai Schramm (RUB, 7/06), Advanced Methods in Side Channel Cryptanalysis. Credit Swiss, Switzerland

Sandeep Kumar (RUB, 6/06), Elliptic Curve Cryptography for Resource Constraints Devices. Philips Research, The Netherlands

Jan Pelzl (RUB, 5/06), Practical Aspects of Curve-Based Cryptography and Cryptanalysis. University of Applied Sciences Hochschule Hamm-Lippstadt (Associate Professor)

Thomas Wollinger (RUB, 7/04) Software and Hardware Implementation of Hyperelliptic Curve Cryptosystems. CEO of ESCRYPT GmbH

André Weimerskirch (RUB, 7/04), Authentication in Ad-hoc and Sensor Networks. Head of Cybersecurity, LEAR

Jorge Guajardo Merchan (RUB, 7/04), Arithmetic Architectures for Finite Fields GF(p^m) with Cryptographic Applications, Bosch Research, PA, USA

Adam J. Elbirt (Worcester Polytechnic Institute, 5/03), Reconfigurable Computing for Symmetric-Key Algorithms, Draper Laboratory, MA, USA

Gerardo Orlando (Worcester Polytechnic Institute, 3/02), Efficient Elliptic Curve Processor Architectures for Field Programmable Logic, General Dynamics, MA, USA

External Member in Ph.D. and Habilitation Committees

5.2000, EE Dept., *Massachusetts Institute of Technology (MIT),* USA
2.2002, EE Dept., *University of Linköping*, Sweden
2.2002, EE Dept., *University of Siegen,* Germany
8.2003, Mathematics Dept., *University of Toulouse,* France (habilitation)
9.2003, CS Dept., *Darmstadt University of Technology,* Germany
12.2003, CS Dept., *Ecole Normale Superieur (ENS),* France (habilitation)
4.2004, EE Dept., *Polytechnico di Milano*, Italy
5.2004, EE Dept., *Universite catholique Louvain-la-Neuve*, Belgium
9.2004, Mathematics Dept., *Université de Versailles*, France
6.2005, EE Dept., *University of Dortmund*, Germany
7.2005, EE Dept., *University of Siegen,* Germany
3.2007, EE Dept., *University of Siegen,* Germany
6.2007, EE Dept., *Katholieke Universiteit Leuven*, Belgium
8.2007, EE Dept., *Universite catholique Louvain-la-Neuve*, Belgium
11.2007, Mathematics Dept., *Université de Versailles*, France
5.2009, ECE Dept., *WPI*, USA
9.2010, CS Dept., *Université de Grenoble*, France
1.2011, EE Dept., *Katholieke Universiteit Leuven*, Belgium
3.2012, EE Dept., *ETH Zürich*, Switzerland
6.2012, EE Dept., *Universite catholique Louvain-la-Neuve*, Belgium
7.2013, ECE Dept., *Technische Universität München*, Germany
11.2013, CS Dept., *Technische Universität Darmstadt*, Germany
12.2014, Economics Dept., *Université Paris II Panthéon-Assas*, France
12.2014, CS Dept., *Université Paris I Sorbonne*, France
2.2017, CS Dept, *Technical Universiteit Eindhoven*, The Netherlands

Conference and Workshop Organization

- Co-founder of the workshop series “CHES – Cryptographic Hardware and Embedded Systems”, 1999
- Founder of the workshop series “escar – Embedded Security in Cars”, 2003
- Co-founder of RFIDsec – Workshop on RFID Security and Privacy, 2005
- Co-founder of the workshop series “SHARCS – Special-Purpose Hardware for Attacking Cryptographic Systems”, 2005
- Co-founder of the workshop “SECSI – Secure Component and System Identification”, 2008

Steering Committees and Editorship

- IACR Board of Directors, since 2011
- Associate Editor of the IEEE Transactions on Information Forensics and Security, 2008-2010

- Permanent member of the CHES Steering Committee, since 2002 (Chair 2007-2009)
- Member of the Workshop on Elliptic Curve Cryptography Steering Committee, 2003-2014
- Member of the escarUSA Steering Committee
- Member of the eSTREAM (Future Stream Cipher Algorithms) Steering Committee, 2005-2008
- Member of the International Workshop on the Arithmetic of Finite Fields (WAIFI) Steering Committee, since 2007

Conference Chair

- Program Co-Chair for RFIDsec 2011
- Program Co-Chair for CHES, USA and Europe,1999-2003
- Publicity Co-Chair for CHES, USA, Europe, Asia, 2004-2005
- Program Co-Chair for "ESAS – European Workshop on Security in Ad-Hoc and Sensor Networks", Germany, 2004
- Program Co-Chair for escar – Embedded Security in Cars, Germany, 2003-2013
- Organizing Committee, "Workshop on Special Purpose Hardware for Cryptography: Attacks and Applications", USA (UCLA), 2006
- General Co-Chair, "SASC 2007 – State-of-the-Art of Stream Ciphers", Germany, 2007
- Program Co-Chair for "Secure Component and System Identification (SECSI)", Germany, 2008 and 2010

Other

Languages	fluent in English and German, basic knowledge of Dutch and French
Other activities	traditional Okinawa karate (founder of *Okinawa Köln e.V*.)
	head of the support association of our childrens' school (2006-2012)
	interested in social psychology