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	Institute for Experimental Mathematics, Digital Communications Group 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 (FH Köln), Dipl.-Ing. Electrical Engineering

Employment

10.2001–	endowed chair for Embedded Security (W3), ECE Dept., Ruhr University Bochum and founding director of the Horst Görtz Institute for IT Security
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-	Director of the Horst Görtz Institute for IT Security at the 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.)
6.88-5.89	Development engineer for embedded systems (part time)
6.88-7.89	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 (€100,000)
2006	*RUBITEC Technology Transfer Award* (€10,000)
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 award 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" award, category Engineering and Computer Science.
2006	Advisor of the 1st prize of the CAST Forum MS Thesis Award (Germany/Austria/Switzerland-wide award 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, Board Functions and Spin-offs

2003	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
2012–	Advisory Board, *Fraunhofer Institute for Applied & Integrated Security*, Munich
2012-	Technical Advisory Board, *Chaologix*, USA
2008–	Technical Advisory Board, *Intrinsic ID*, The Netherlands
2000–2002	Technical Advisory Board, *rTrust Inc*., USA

1999–2003 Technical Advisory Board, *cv cryptovision*, Germany

2006–2012 Board of Directors, *Card Factory*, Germany

2001–2003 Board of Directors, *Eracom Technologies*, Australia and Germany

Research Grants

Doctoral Schools

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

DFG Graduiertenkolleg “New Challenges for Cryptography in Ubiquitous Computing”, 2012, total: 4,200k € (Spokesperson, with 10 co-PIs)

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

DFG (German National Science Foundation)

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

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

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

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

“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 Dan Holcomb and Sandip Kundu)

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

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

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

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

“Security in Embedded Networks”, 2001, total: $460k (co-PI, with Berk Sunar and Bill 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 €

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

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

“STORK – Strategic Roadmap for Cryptography”, 2002, 60k €
(co-PI, with KU Leuven and ENS Paris)

“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, „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)

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

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

Since 2002, I have graduated 25 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, Germany, Singapore and the USA.

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

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

Elif Kavun (RUB, 1/15), Resource-efficient Cryptography for Ubiquitous Computing, Infineon

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

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, Infineon

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

Thomas Eisenbarth (RUB, 7/09), Cryptography and Cryptanalysis for Embedded Systems, University of Lübeck (Full Professor 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. NXP

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

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. University of Michigan

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

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

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

Teaching: Higher Education

Graduate courses:

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

Undergraduate courses:

Introduction to Cryptography and Data Security I and II (U. Bochum)
Programing Languages: C and Assembly (U. Bochum)
Introductory Physics (Cologne College for Nurses)
Introduction to VLSI Design (WPI)
Continues-Time Signal and System Analysis (WPI)

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
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

Founding of Conference and Workshops

- Co-founder of the conference “CHES – Cryptographic Hardware and Embedded Systems”, 1999
- Founder of the workshop “escar – Embedded Security in Cars”, 2003
- Co-founder of “RFIDsec – Workshop on RFID Security and Privacy”, 2005
- Co-founder of the workshop “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, 2011-2016
- Associate Editor of the IEEE Trans. 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

Program Committee

- International conference on security and privacy on Vehicular Area Networks 2016
- ACM CCS Workshop on Smart Energy Grid Security, 2013
- CyCAR 2013
- EUROCRYPT 2011
- CRYPTO 2009, 2013
- 3rd Workshop on Embedded Systems Security (WESS '2008), USA
- PQCrypto 2008 (Workshop on Post-Quantum Cryptography), USA

- IEEE International Workshop on Hardware-Oriented Security and Trust (HOST) 2008, 2009, 2012, 2016USA
- TRUST 2008, Austria
- CHES, since 1999
- Selected Areas in Cryptography – SAC, Canada, 2007
- VANET – ACM Workshop on Vehicular ad-hoc Networks, USA, 2007
- ACM EMSOFT Workshop on Embedded Systems Security, Asia and Europe, 2006-2007
- State-of-the-Art of Stream Ciphers, Belgium, Germany, Switzerland, 2006- 2008
- 2007 International Workshop on Service, Security and its Data Management for Ubiquitous Computing – SSDU-07, China, 2007
- IT-Solutions for Physical Security, Sweden, 2007
- RFIDSec Workshop, Austria and Spain, 2005-2007, 2012, 2015
- Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC, 2004 -2007
- ESAS – European Workshop on Security in Ad-Hoc and Sensor Networks, Hungary, 2005
- RSA Conference – Cryptographer´s Track, USA, Silicon Valley, 2002
- Advisory Board, Conference on Field Programmable Technology, Hong Kong, 2002
- Workshop Alternative Public-Key Algorithms, Germany, 2002
- Conference on Information Security and Cryptology – ICISC 2002, Korea, 2002
- Workshop Complexity-theoretical and Algebraic Methods in Cryptography, Germany, 2002

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 foundation of our childrens' school (2006-2012)
	interest in social psychology