

Curriculum Vitae

Education

- 7.91-7.94 Institute for Experimental Mathematics, University of Essen, Germany
degree: Ph.D. (Dr.-Ing.), Electrical Engineering
- 1993, 1994 University of Massachusetts Amherst, three research visits
- 11.90-5.91 Michigan Technological University, graduate research
- 8.89-5.91 University of Siegen, Germany
degree: M.S. (Dipl.-Ing.)
- 10.84-5.88 Cologne University of Applied Sciences, Germany
degree: B.S. (Dipl.-Ing. FH)

Employment

- 10.01- Head of the endowed chair “Embedded Security” (W3), ECE Dept., Ruhr-University Bochum, Germany
- 9.09- Affiliated Professor at the University of Massachusetts Amherst
- 8.08-8.09 Research Professor at the University of Massachusetts Amherst
- 04-07/10-12 Director of the Horst Görtz Institute for IT Security at the Ruhr-University of Bochum
- 1.95-6.02 Assistant Professor and later Associate Professor (tenured), ECE Dept., WPI
- 97- Consultant in the area of embedded security in the US and Europe: Bosch, cryptovision, DAFCA, Greylock, Nagravision, NTRU, Philips, Polaroid ID, secunet and others
- 6.88-5.89 Development engineer for embedded microcontroller systems, Engel & Co Telecommunication, Germany (part time)
- 8.79-1.83 Apprenticeship as telecommunication technician

Fellowships and Awards

- 2012 Best paper award at the IEEE Conference on Security & Privacy
- 2012 *Innovations Preis NRW 2012*, for technical innovation by the federal state of North Rhine-Westphalia, Germany’s largest state (€100,000)
- 2011 *IEEE Fellow*
- 2010 *IT Security Award* (with Gregor Leander and Axel Poschmann) for the development of the lightweight cipher PRESENT (€100,000)
- 1998 *CAREER Award* by the National Science Foundation (NSF)
- 1996 *Satin Distinguished Fellowship Award* for outstanding teaching & research, WPI

Teaching Awards

- 2012 Advisor of the 1st prize *CAST Forum PhD Thesis Award*
- 2006 Top 10 of the Germany-wide *Professor of the Year* competition, Engineering & CS
- 2006 Advisor of the 1st prize of the *CAST Forum MS Thesis Award*
- 2005 Advisor of the *Gert Massenbergs Foundation* dissertation award
- 1999 Advisor of 1st prize *senior thesis competition* (MQP), ECE Dept., WPI
- 1998 Advisor of 1st prize *senior thesis competition* (MQP), CS Dept., WPI

Board and Chief Officer Functions

2003	co-founder of <i>ESCRYPT GmbH – Embedded Security</i> (Germany) and <i>escrypt Inc.</i> (USA) <i>ESCRYPT</i> was acquired by Bosch in 2012
2006-2012	Board of Directors, <i>Card Factory</i> , Germany
2001-2003	Board of Directors, <i>Eracom Technologies</i> , Australia and Germany
2014-	Scientific Advisory Board, <i>Chaologix</i> , USA
2000-2002	Scientific Advisory Board, <i>rTrust Inc.</i> , USA
1999-2003	Scientific Advisory Board, <i>cv cryptovision</i> , Germany

Research Funding

Christof Paar has received major research grants from organizations such as the US National Science Foundation (NSF), German National Research Foundation (DFG), BMBF, BMWi, Blaupunkt, BSI, Cisco, GTE, Lockheed Martin, NXP, Sun, Texas Instruments and others. He is Spokesperson for the Research Training Group (Graduiertenkolleg) *Cryptography in Ubiquitous Computing*.

Publications

Christof Paar has more than 150 peer-reviewed scientific publications in applied security, and he is the editor of eight conference proceedings and special issues dealing with cryptographic engineering. He holds three patents in the area of applied cryptography. He was invited speaker at TrustEd 2014, CCS 2013 (tutorial), Indocrypto 2011, CHES 2009, HotChips 2003, ECC 2003, IEEE Communication Theory Workshop 2002, FPGA 2000, and ECC '99. He co-authored (with Jan Pelzl) the textbook "Understanding Cryptography", published by Springer.

Invited Talks

Christof Paar has given invited talks in the US and Europe, including presentations at MIT, Yale, Stanford University, UCLA, University of Illinois U-C, IBM T.J. Watson Labs, Sun Labs, NEC Labs, Infineon, EPFL Lausanne (Switzerland), University of Linköping (Sweden), University of Essen, Darmstadt University of Technology and others.

Conference Organization

In 1999 Christof Paar was co-founder (with Cetin Koc) of the CHES conference series "CHES – Cryptographic Hardware and Embedded Systems", which he has helped to organize since '99. In 2003 he founded "escar – Embedded Security in Cars". He was involved in launching the RFIDsec workshop series in 2005. He is member of the steering committees of CHES, ECC (Workshop on Elliptic Curve Cryptography) and RFIDsec.

Industry Teaching

Christof Paar has taught industry courses in security at NASA, Motorola Research, Philips Research, GTE, General Dynamics, CAMP Consortium (Ford, GM, Honda, Mercedes, Toyota) and EPFL Lausanne.

University Teaching

Christof Paar has taught undergraduate and graduate courses in Cryptography, Cryptographic Implementations, Computer Networks, VLSI Design, Programming Languages and Linear Systems. He taught at Ruhr-University Bochum, University of Massachusetts, WPI and the University of Lugano (Switzerland).