

# Dr. André Weimerskirch

Ann Arbor, MI 48103, USA

Internet: [www.weimerskirch.org](http://www.weimerskirch.org)  
email: [andre@weimerskirch.org](mailto:andre@weimerskirch.org)

## EDUCATION

2008 - today

**Henley Management College**, Greenlands, England

- Executive MBA
- Part-time in parallel to full-time employment

2001 - 2004

**Ruhr-University Bochum**, Bochum, Germany

- Dr.-Ing. (Ph.D.), Electrical Engineering and Information Technology, July 2004
- Thesis: Authentication in Ad-hoc and Sensor Networks
- Advisor: Prof. Christof Paar; Reader: Prof. Jean-Pierre Hubaux

**Grade: 1.0**

1999 - 2001

**Worcester Polytechnic Institute**, Worcester, MA

- Master of Science, Computer Science, May 2001
- Thesis: The Application of the Mordell-Weil Group to Cryptographic Systems

**GPA: 4.0/4.0**

1995 - 1999

**Darmstadt University of Technology**, Darmstadt, Germany

- Double Major in Business Administration and Computer Science
- Second Major in Mathematics
- Pre Diploma October 1997 (BA/CS), Pre Diploma April 1998 (Mathematics)

**GPA: Ranked first (BA/CS)**

## EXPERIENCE

Mar. 2007 -  
today

**Chief Executive Officer and President, escript Inc.**, Ann Arbor, MI, USA

Successfully set up the US business of escript. Managing the company and responsible for all international business. Developed the future vehicle-to-vehicle safety communications security and privacy protocols and architecture for the USA deployment and worked on the European standard for secure and privacy preserving vehicle-to-vehicle and vehicle-to-infrastructure communication. Performed FIPS 140-2 security certifications and lead development of a vehicle-to-vehicle secure communication unit complying to the IEEE 1609.2 standard. Performed a large variety of risk assessments for industrial and high-tech customers, and designed legacy-aware cost-efficient secure systems.

<p>2004 - Feb. 2007</p>	<p><b>Chief Technology Officer, escript GmbH</b>, Bochum, Germany Co-founder and responsible for strategic planning and operative business. Set-up escript to become widely known in the embedded security market. Performed Common Criteria certifications and production-level code development for the automotive industry. Worked intensely to evaluate and secure computing platforms (e.g. smart-cards, TPMs, and standard embedded controllers) and performed forensic security evaluation of Pay-TV hacks for court.</p>
<p>Oct. 2001 - Aug. 2004</p>	<p><b>Research Assistant, Ruhr-University Bochum</b>, Bochum, Germany Doing my Ph.D. in pervasive and embedded security. Research in the area of security in mobile, ad-hoc and sensor networks, cryptographic protocols, efficient arithmetic, and applied cryptography. Performed teaching and student's supervising, and headed several industry projects.</p>
<p>Feb. 2003 - Aug. 2003</p>	<p><b>Researcher, Aarhus University</b>, Aarhus, Denmark (fellowship) European Union full-time fellowship to do research as part of my Ph.D.; Worked on security protocols for embedded systems and ad-hoc networks.</p>
<p>July 2002 - Sept. 2002</p>	<p><b>Researcher, Sun Microsystems Laboratories</b>, Mountain View, CA USA (internship) Did research in the area of efficient next generation cryptography; Implemented elliptic curve cryptography for a software library.</p>
<p>Jan. 2002 - June 2002</p>	<p><b>IT-Consultant, Josteit, Herten &amp; Partner</b>, Dusseldorf, Germany (part-time job) Consultancy in security related areas like PKI, Internet and application security, and vulnerability assessments.</p>
<p>June 2001 - Sept. 2001</p>	<p><b>Researcher, Accenture</b>, Sophia Antipolis, France (internship) Analyzed security of wireless networks; Modeled new security policies and developed a biometric access control mechanism.</p>
<p>Aug. 2000 - May 2001</p>	<p><b>Research Assistant, Worcester Polytechnic Institute</b>, Worcester, MA USA Doing my Master in cryptography. Worked on an industry project; helped organizing a large conference.</p>
<p>May 2000 - July 2000</p>	<p><b>Researcher, Philips Research</b>, Briarcliff Manor, NY USA (internship) Worked on copy protection method for digital music; Analyzed a hardware random number generator; Studied cryptanalysis methods for DES.</p>
<p>Feb. 97 - July 99</p>	<p><b>Web Developer, Deutsche Post AG</b>, Darmstadt, Germany (part-time job) Set up the Intranet with Lotus Notes; Designed and developed Workflow, Workgroup and Database applications; Consulted customers and in-house developers.</p>
<p>Dec. 98 - July 99</p>	<p><b>Notes Developer, Darmstadt University of Technology</b>, Darmstadt, Germany (part-time job) Planned and implemented a Novell Network and Lotus Notes system; Analyzed extant workflows and implemented them.</p>

Oct. 98 -  
Feb. 99

**Teaching Assistant, Darmstadt University of Technology**, Darmstadt, Germany  
Teaching Assistant for Operating Systems course. Advised, instructed and graded students.

March 96 -  
Nov. 96

**Network Administrator, Siemens AG**, Frankfurt am Main, Germany (part-time job)  
Administered a Windows NT network, maintained the e-mail system and performed troubleshooting of LAN computer systems.

May 95 -  
Jun. 95

**Network Administrator, Agrevo AG**, Frankfurt/Hoechst, Germany (internship)  
Administered the network, maintained a Microsoft Mail system, installed new PC equipment and upgraded software.

#### **AWARDS AND HONORS**

- Selected as expert by the European Telecommunications Standards Institute (ETSI) to define the European standard for vehicle-to-vehicle and vehicle-to-infrastructure secure communication.
- Transferpreis (Transfer Award) 2005 for technology transfer from academia to industry of rubitec (awarded with 10,000 €).
- European Union Marie Currie full-time fellowship for research visit at Aarhus University, Feb. 2003 - Aug. 2003.
- e-fellows.net scholarship 2001-2004.
- Selected by Sun Microsystems Laboratories for a full scholarship for the academic year 2000/2001.
- Full-time scholarship of German Academic Exchange Service (DAAD) 1999-2000.
- Best Pre Diploma out of 80 students in my field at Darmstadt University of Technology in the academic year 1997/98.

#### **PUBLICATIONS**

##### Journal Papers

- André Weimerskirch, "Secure Software Flashing", In Society of Automotive Engineers (SAE) International Journal of Passenger Cars — Electronic and Electrical Systems, October 2009, 2:83-86.
- Christof Paar and André Weimerskirch, "Embedded Security in a Pervasive World", Elsevier Science's Information Security Technical Report, vol 12, no 3, pp 155-161, 2007.
- Marko Wolf, André Weimerskirch, and Thomas Wollinger, "State-of-the-Art: Embedding Security in Vehicles", EURASIP Journal on Embedded Systems, Special Issue on Embedded Systems for Intelligent Vehicles, 2007.
- Bernd Lamparter, Christof Paar, André Weimerskirch, and Dirk Westhoff, "On Digital Signatures in Ad Hoc Networks", Wiley Journal European Transactions on Telecommunications, Special Issue on Self-Organization in Mobile Networking, September 2005.

##### Book Chapters

- André Weimerskirch, Jason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux, "Data Security in Vehicular Communications Networks", VANET – Vehicular Applications and Inter-Networking Technologies, Wiley Blackwell, 2010.
- Marko Wolf, André Weimerskirch, and Christof Paar, "Secure In-Vehicle

- Communication”, Embedded Security in Cars, Springer Monograph Series, 2005.
- Marko Wolf, André Weimerskirch, and Christof Paar, “Automotive Digital Rights Management Systems”, Embedded Security in Cars, Springer Monograph Series, 2005.
  - André Weimerskirch, Dirk Westhoff, Stefan Lucks, and Erik Zenner, "Efficient Pairwise Authentication Protocols for Sensor and Ad-hoc Networks", Sensor Network Operations, IEEE Press, 2004.
  - André Weimerskirch, "Fixed-base exponentiation", Encyclopedia of Cryptography and Security, 2004.
  - André Weimerskirch, "Fixed-exponent exponentiation", Encyclopedia of Cryptography and Security, 2004.
  - André Weimerskirch, "Karatsuba algorithm", Encyclopedia of Cryptography and Security, 2004.
- Tim Güneysu, Igor Markov, and André Weimerskirch, “Securely Sealing Multi-FPGA Systems”, The 8<sup>th</sup> International Symposium on Applied Reconfigurable Computing (ARC 2012), March 21-23, 2012, Hong Kong.
  - André Weimerskirch, “V2X Security & Privacy: The Current State and its Future”, 18<sup>th</sup> ITS World Congress, October 16-20, 2011, Orlando, USA.
  - Hariharan Krishnan, André Weimerskirch, “Verify-on-Demand – A Practical and Scalable Approach for Broadcast Authentication in Vehicle-to-Vehicle Communication”, SAE 2011, World Congress, April 12-14, 2011, Detroit, USA.
  - André Weimerskirch, “Do Vehicles need Data Security?”, SAE 2011 World Congress, April 12-14, 2011, Detroit, USA.
  - Christof Paar, Kai Schramm, André Weimerskirch, and Marko Wolf, “Implementing Data Security and Privacy in Next-Generation Electric Vehicle Systems”, SAE 2010 World Congress, April 13-15, 2010, Detroit, USA.
  - Levente Buttyán, Tamás Holczer, André Weimerskirch, and William Whyte, “SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs”, First IEEE Vehicular Networking Conference 2009 (IEEE VNC 2009), October 28-30, 2009, Tokyo, Japan.
  - André Weimerskirch, Kai Schramm, Lars Wolleschensky, and Thomas Wollinger, “The Dilemma of Data Security, Privacy, Control and Liability in V2X”, ITS World Congress, September 21-25, 2009, Stockholm, Sweden.
  - André Weimerskirch, Kai Schramm, and Lars Wolleschensky, “Authentication and Privacy in Vehicular Networks: State-of-the-Art and Outlook”, ITS America’s 2009 Annual Meeting and Exposition, June 1-3, 2009, National Harbor, MD, USA.
  - Christof Paar, Andy Rupp, Kai Schramm, André Weimerskirch, and Wayne Burleson, “Securing Green Cars: IT Security in Next Generation Electric Vehicle Systems”, ITS America’s 2009 Annual Meeting and Exposition, June 1-3, 2009, National Harbor, MD, USA.
  - André Weimerskirch, Marko Wolf, and Thomas Wollinger, “Introduction to Vehicular Embedded Security”, SAE 2009 World Congress, April 20-23, 2009, Detroit, USA.
  - André Weimerskirch, “Secure Software Flashing”, SAE 2009 World Congress, April 20-23, 2009, Detroit, USA; selected for inclusion in SAE International Journal of Passenger Cars – Electronic and Electrical

Systems, 2(1): 83-86, 2009.

- Stefan Lucks, Erik Zenner, André Weimerskirch, Dirk Westhoff, "Concrete Security for Entity Recognition: The Jane Doe Protocol", 9th International Conference on Cryptology in India (INDOCRYPT 2008), December 14-17, 2008, IIT Kharagpur, India.
- Andrey Bogdanov, Dario Carluccio, André Weimerskirch, and Thomas Wollinger, "Embedded Security Solutions for Automotive Applications", 11th International Forum on Advanced Microsystems for Automotive Applications, May 9-10, 2007, Berlin, Germany.
- Axel Poschmann, Dirk Westhoff, and André Weimerskirch, "Dynamic Code Update for the Efficient Usage of Security Components in WSNs", 4th Workshop on Mobile Ad-Hoc Networks (WMAN 2007), March 1-2, 2007, Bern, Switzerland.
- André Weimerskirch, Christof Paar, and Marko Wolf, "Cryptographic Component Identification: Enabler for Secure Inter-vehicular Networks", 62nd IEEE Vehicular Technology Conference, September 25-28, 2005, Dallas, TX, USA.
- André Weimerskirch, Katrin Höper, Christof Paar, and Marko Wolf, "Component Identification: Enabler for Secure Networks of Complex Systems", Applied Cryptography and Network Security (ACNS) 2005, June 7-10, 2005, New York City, NY, USA.
- Jonathan Hammell, André Weimerskirch, Joao Girao, and Dirk Westhoff, "Recognition in a Low-Power Environment", WWAN 2005, The 25th IEEE International Conference on Distributed Computing Systems (ICDCS-2005), Columbus, Ohio, USA, June 6-9, 2005.
- Marko Wolf, André Weimerskirch, and Christof Paar, "Security in Automotive Bus Systems", escar 2004 - Embedded Security in Cars Workshop, Bochum, 10.-11. November, 2004.
- Sandeep Kumar, Marco Girimondo, André Weimerskirch, Christof Paar, Arun Patel, and Arvinderpal S.Wander, "Embedded End-to-End Wireless Security with ECDH Key Exchange", 46th IEEE Midwest Symposium On Circuits and Systems, December 27-30, 2003, Cairo, Egypt.
- André Weimerskirch and Dirk Westhoff, "Identity Certified Authentication for Ad-hoc Networks", 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), October 31, 2003.
- André Weimerskirch and Dirk Westhoff, "Zero Common-Knowledge Authentication for Pervasive Networks", Selected Areas in Cryptography - SAC, August 14-15, 2003.
- André Weimerskirch, Douglas Stebila, and Sheueling Chang Shantz, "Generic  $GF(2^m)$  Arithmetic in Software and its Application to ECC", The Eighth Australasian Conference on Information Security and Privacy (ACISP 2003), 9-11 July 2003, Wollongong, Australia.
- Olivier Pelletier, André Weimerskirch, "Algorithmic Self-Assembly of DNA Tiles and its Application to Cryptanalysis", The Genetic and Evolutionary Computation Conference 2002 (GECCO 2002), July 9-13, 2002, New York City, USA.
- André Weimerskirch and Gilles Thonet, "A Distributed Light-Weight Authentication Model for Ad-hoc Networks", The 4th International Conference on Information Security and Cryptology (ICISC 2001), December 6-7, 2001, Seoul, South Korea.
- André Weimerskirch, Christof Paar, and Sheueling Chang Shantz, "Elliptic Curve Cryptography on a Palm OS Device", The 6th Australasian

National  
Conference Papers

Conference on Information Security and Privacy (ACISP 2001), July 11-13 2001, Sydney, Australia.

- Christof Paar, Jan Pelzl, Andy Rupp, Kai Schramm, André Weimerskirch "Green Car Security: IT-Sicherheit und Elektromobilität". DACH Security 2009, Ruhr-Universität Bochum, Bochum, Germany, May, 19-20, 2009.
- Stefan Lucks, Erik Zenner, André Weimerskirch, and Dirk Westhoff, "Entity Recognition for Sensor Network Motes", 2<sup>nd</sup> Workshop on Sensor Networks at Informatik 2005, Bonn, September 19-22, 2005.
- Marko Wolf, André Weimerskirch, and Christof Paar, "Digital Rights Management Systems (DRMS) als Enabling Technology im Automobil" (Digital Rights Management Systems (DRMS) as Enabling Technology in the Automobile), Sicherheit 2005: Sicherheit - Schutz und Zuverlässigkeit, Regensburg, April 5-8, 2005.
- Ulrich Kaiser, Christof Paar, Dörte Rappe, Werner Schindler, André Weimerskirch, and Thomas Wollinger, "Kriterien für die Auswahl der kryptographischen Algorithmen bei Low-Cost-RFID-Systemen" (Criteria for the Selection of Cryptographic Algorithms for Low-Cost RFID Systems), D-A-CH Security 2005, Darmstadt University of Technology, 2005.
- André Weimerskirch, Marko Wolf, and Christof Paar, "Komponentenidentifikation: Voraussetzung für IT-Sicherheit im Automobil" (Component Identification: Enabler for IT-Security in the Automobile), Automotive - Safety & Security 2004, Stuttgart, 6.-7. October, 2004.
- Marko Wolf, André Weimerskirch, and Christof Paar, "Sicherheit in automobilen Bussystemen" (Security in Automotive Bus Networks), Automotive - Safety & Security 2004, Stuttgart, 6.-7. October, 2004.
- André Weimerskirch, "Authentikation in Ad-hoc und Sensornetzwerken" (Authentication in Ad-hoc and Sensor Networks), GUUG-Frühjahrsfachgespräch 2004, Ruhr-Universität Bochum, 9.-12. März, 2004.
- Christof Paar, Jan Pelzl, Kai Schramm, André Weimerskirch and Thomas Wollinger, "Eingebettete Sicherheit: State-of-the-art" (Embedded Security: State-of-the-art), D-A-CH Security 2004, University of Basel, March 30-31, 2004.

International  
Magazine Articles

- Andrey Bogdanov, Christof Paar, André Weimerskirch and Thomas Wollinger, "Embedded Security in Next-Generation Civilian and Government Systems", Safety and Security International, 2008.
- André Weimerskirch and Christof Paar, "Embedded Security in Geoinformation Systems", Geoinformatics Magazine, 2004.

National Magazine  
Articles

- André Weimerskirch and Christof Paar, „Was der ISM über Embedded Security wissen sollte“, Information Security Management – Das Praxishandbuch, TÜV Media, 2007.
- Marko Wolf, André Weimerskirch, and Christoph Wegener, "Rechte für Kleine – Digital Rights Management in mobilen und eingebetteten Geräten“, iX, 1/2006.
- Marko Wolf, André Weimerskirch, and Christof Paar, "Digitale Rechteverwaltung" (Digital Rights Management), Elektronik Automotive,

2/2005

- André Weimerskirch and Christof Paar, "Sicherheit schlicht verpennt" (Security Simply Overslept), Automobil Elektronik, 02.2005.
- André Weimerskirch and Prof. Paar, "Der digitale Goldesel - DRM im Automobil" (The Digital Cash Cow - DRM in the Automobile), Automobil Elektronik, December 2004.
- André Weimerskirch and Christof Paar, "IT-Sicherheit in Geoinformations-Systemen" (IT-Security in Geoinformations Systems), GeoBit, 2004.

#### Technical Reports

- Stefan Lucks, Erik Zenner, André Weimerskirch, and Dirk Westhoff, "Concrete Security for Entity Recognition: The Jane Doe Protocol (Full Paper)", IACR ePrint Archive, 2009/175, 2009.
- André Weimerskirch and Christof Paar, "Generalizations of the Karatsuba Algorithm for Efficient Implementations", 2003.

#### Theses

- André Weimerskirch, "Authentication in Ad-hoc and Sensor Networks", Ph.D. Thesis, Ruhr-University of Bochum, Germany, July 2004.
- André Weimerskirch, "The Application of the Mordell-Weil Group to Cryptographic Systems", MS Thesis, Worcester Polytechnic Institute, Worcester, MA, USA, May 2001.

#### Other Publications (not related to data security)

- Armin Scholl and André Weimerskirch, "Robuste Projektplanung auf der Grundlage des Linear Time-Cost Tradeoff-Problems" (Robust Project Scheduling Based on the Linear Time-Cost Tradeoff Problem), Schriften zur Quantitativen Betriebswirtschaftslehre, 10/99, November 1999.

#### Patents

- André Weimerskirch, "Method and apparatus for preventing noise from influencing a random number generator based on flip-flop meta-stability", United States Patent Application 20030101205.
- André Weimerskirch, "Method and apparatus to prevent the unauthorized copying of digital information", United States Patent Application 20030088775.
- Laslo Hars, Antonius Staring, and André Weimerskirch, "Apparatus and methods for attacking a screening algorithm based on partitioning of content", United States Patent Application 20020152172.

#### **PUBLIC PROJECTS**

- VSC-3 – Vehicle Safety Communications 3, funded by the US Department of Transportation: Responsible for escrypt Inc.
- VSC-2 – Vehicle Safety Communications 2, funded by the US Department of Transportation: Responsible for escrypt Inc.
- UbiSec&Sens – Ubiquitous Sensing and Security in the European Homeland, Sixth Framework Program of the European Union: Representative and Task Leader for Bochum Ruhr-University
- EMSCB – European Multilaterally Secure Computing Base, partly funded by the German Federal Ministry of Economics and Technology: Responsible for escrypt GmbH

#### **COMMITTEE**

- VEHICULAR 2012 (The First International Conference on Advances in

## MEMBER

- Vehicular Systems, Technologies and Applications), in conjunction with InfoWare 2012, June 24-29, 2012, Venice, Italy.
- Technical Program Committee of VANET 2011 (The Eighth ACM International Workshop on Vehicular Inter-Networking), in conjunction with ACM Mobicom 2011, September 23<sup>rd</sup>, Las Vegas, USA.
  - Technical Program Committee of the 4<sup>th</sup> International Symposium on Wireless Vehicular Communications (WIVEC 2011), September 5-6, San Francisco, USA.
  - Technical Program Committee of the 73<sup>rd</sup> Vehicular Technology Conference 2011 (VTC 2011), May 15-18, Budapest, Hungary.
  - Technical Program Committee of Second IEEE Vehicular Networking Conference 2010 (IEEE VNC 2010), December 13-15, Jersey City, NJ, USA.
  - General Co-Chair of VANET 2010 (The Seventh ACM International Workshop on Vehicular Inter-Networking), In conjunction with ACM Mobicom 2010, Chicago, USA.
  - General Co-Chair of VANET 2009 (The Sixth ACM International Workshop on Vehicular Inter-Networking), In conjunction with ACM MobiCom 2009, Beijing, China.
  - Industry Track Organization Committee of The First Annual International Symposium on Vehicular Computing Systems (ISVCS 2008), July 22, 2008, in conjunction with MobiQuitous 2008, Dublin, Ireland.
  - Program Committee of The Fourth IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'08), September 29, 2008, in conjunction with The 5th IEEE International Conference on Mobile Ad-hoc and Sensor Systems, Atlanta, Georgia, USA.
  - Technical Program Committee of the Fifth ACM International Workshop on Vehicular Inter-Networking (VANET) 2008, in conjunction with ACM MobiCom, San Francisco, USA.
  - Program Committee of WiSP 2008 (Workshop on Wireless Security and Privacy), Beijing, China, June 20, 2008.
  - Program Committee of SPEED 2007 (Software Performance Enhancement for Encryption and Decryption), Amsterdam, The Netherlands, June 11-12, 2007.
  - Program Committee of escar 2006 (Embedded Security in Cars), Berlin, Germany, November 14-15, 2006.
  - Program Committee of WSNS'06 (The Second International Workshop on Wireless and Sensor Networks Security), in conjunction with MASS 2006 (The 3rd IEEE International Conference on Mobile Ad-hoc and Sensor Systems), Vancouver, Canada, October 9-12, 2006.
  - Program Committee of ESAS 2006 (3rd European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks), in conjunction with ESORICS 2006 (European Symposium on Research in Computer Security), Hamburg, Germany, September 20-21, 2006.
  - Program Committee of ESAS 2005 (2nd European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks), Visegrad, Hungary, July 13-14, 2005.
  - Program Committee of MADNES 2005 (Secure Mobile Ad-hoc Networks and Sensors Workshop), in conjunction with ISC 2005 (Information Security Conference), Singapore, September 20-22, 2005.
  - Program Committee of ESAS 2004 (1st European Workshop on Security in Ad-Hoc and Sensor Networks), Heidelberg, Germany, August 5-6,

2004.

## REVIEWER

- Evaluator for the European commission as well as for European ministries.
- Peer review:
  - ACM Transactions on Information and System Security (ACM TISSEC)
  - Elsevier Computer Communications
  - Embedded Security in Cars (escar)
  - European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS)
  - IEEE Communications Letters
  - IEEE Globecom
  - IEEE Transactions on Computers
  - IEEE Transactions on Information Forensics and Security
  - Information Processing Letters (IPL)
  - Journal of Cryptology
  - Journal of Systems and Software (JSS)
  - Mobile Ad-hoc and Sensor Networks (MSN)
  - New Security Paradigms Workshop (NSPW)
  - Secure Mobile Ad-hoc Networks and Sensors Workshop (MADNES)
  - The Sixth ACM International Workshop on Vehicular Inter-Networking (VANET 2009)
  - Workshop on Cryptographic Hardware and Embedded Systems (CHES)
  - Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)

## PRESENTATIONS

### INVITED PRESENTATIONS

- SAE 2011 Intelligent Vehicle Systems Symposium, Detroit, MI, November 8-9, 2011
- Invited presentation and panel member, COMeSafety 7<sup>th</sup> International Workshop on Vehicle Communications for Safety and Sustainability, Orlando, FL, October 21, 2011.
- Keynote presentation WIVEC 2011, San Francisco, USA, September 5-6, 2011.
- Pitney Bowes, Seventh Annual Conference on Information Security and Communication, Stamford, CT, USA; June 14, 2011
- 9<sup>th</sup> Annual Wireless Telecommunication Symposium (WTS 2010), Tampa, FL, USA, 21-23 April, 2010.
- ITS World Congress 2008, New York City, NY, November 18, 2008.
- Pitney Bowes, Fourth Annual Conference on Information Security and Communication, Stamford, CT, USA, June 25, 2008.
- IES Industry Forum, Santa Clara, CA, USA, June 5-6, 2008.
- SECSI – Secure Component and System Identification, Berlin, Germany, March 17-18, 2008.

- The 9th Workshop on Elliptic Curve Cryptography (ECC 2005), Copenhagen, Denmark, September 19, 20 & 21, 2005.
- "Datensicherheit für Location Based Services" (Data Security for Location Based Services), esgeo (embedded security in geoinformation systems) 2005, Bochum, Germany, June 2nd, 2005.
- "IT-Sicherheit im Automobil" (IT-Security in the Automobile), Autokongress der Ruhr-Universität Bochum, Bochum, Germany, June 1st, 2005.
- "Datensicherheit im Fahrzeug" (Data Security in Vehicles), Cebit, Hannover, Germany, March 11, 2005.
- "Embedded Security im Automobil" (Embedded Security in the Automobile), Entwicklerforum "Drahtlose und drahtgebundene Netzwerke 2004", Munich, Germany, July 7, 2004.
- "Cryptographic Performance in Practical Applications", TransFIT Workshop, Berlin, Germany, June, 2001.

Held further invited presentations at

- Accenture Technology Labs
- Embedded World, Nuremberg
- NEC Europe Network Laboratories
- Philips Research
- Ruhr-University of Bochum
- Sun Microsystems Laboratories
- Worcester Polytechnic Institute

Further Presentations

- "Why do we need Data Security in ITS", ITS World Congress (World Congress on Intelligent Transport Systems), New York City, USA, November 16-20, 2008.

## TEACHING

- Held several courses and workshops for industry including DaimlerChrysler, TUV, Ford, and Toyota:
  - Introduction to Cryptography
  - Elliptic Curve Cryptography
  - Secure Car-to-Car Communication
  - Trusted Hardware in Embedded Systems
- Teaching assistant of "Asymmetric Cryptography" course. Organized homework and exercises, and held several classes.
- Supervised diploma theses:
  - Daniel Hamburg, "Implementing Public Key Algorithms on Embedded Systems", 2004.
  - Michael Holzt, "Penetration of Infotainment Devices", 2005 (external Masters Thesis).
  - Katrin Höper, "Cryptographic Protocols for Component Identification and Applications", 2002.
  - Hakim Izaamriouane, "Erstellung eines drahtlosen kryptographischen Identifizierungstokens" (Development of a Wireless Cryptographic Identification Token), 2005.
  - Makoto Miyamoto, "Security in Ad-hoc Networks - Survey and

Implementation", 2003.

- Ingo Riedel, "Security in Ad-hoc Networks: Protocols and Elliptic Curve Cryptography on an Embedded Platform", 2003 (thesis was awarded with 2nd place of the CAST forum).
- Lars Wolleschensky, "Efficient Cryptographic Protocols for Secure Vehicle-to-Vehicle Communication", 2009.
- Zheng Wu, "Secure Hardware Platforms for Embedded Applications", 2006.
- Supervised seminar term work:
  - Marko Borrmann, "Steganographie" (Steganography), 2003.
  - Tim Güneysu, "CD/DVD Copy Protection", 2004.
  - Marius Hilckmann, "Quantum Cryptography", 2003.
  - Lijun Liao, "Kryptographie in der Praxis" (Cryptography in Practical Applications), 2003.
  - Egmont Semmler, "Schnelle Faktorisierung" (Fast Factorization), 2004.
  - Christof Schmits, "e-Voting", 2004.
  - Marcel Selhorst, "Die Geldkarte - Eine "sichere" elektronische Geldbörse?!" (The Electronic Money Card - A Secure Electronic Wallet?!), 2002.

## COMPUTER EXPERIENCE

**Certifications:** Microsoft Certified Systems Engineer, Lotus Notes Administrator

**Operating Systems:** UNIX/Linux, MS Windows, Novell Networks

**Programming Languages:** C/C++, Java, Visual Basic/Notes Script, JavaScript, HTML

**Misc. Packages:** MS Office, Star Office, Lotus Notes 4.x, LATEX

## LANGUAGES

Fluent in German and English, basic Spanish knowledge