Curriculum Vitae

Dr. Torsten Schütze
Sturmfederstr. 26
D-74388 Talheim, Germany
Phone: +49 71 33 / 1 83 76 50
Mobile Phone: +49 1 73 / 6 51 45 22
E-Mail: torsten.schuetze@rohde-schwarz.com
torsten.schuetze@gmx.net
WWW: http://www.torsten-schuetze.de

Personal data
Date of birth: 1969-09-24
Place of birth: Nordhausen (Thuringia, Germany)
Marital status: married

Professional background
Development Principal
Dr. rer. nat., Mathematician & Cryptologist

Talheim, 2016-02-08

Professional Experience

- almost twenty years of experience with applied and industrial cryptography
- design of crypto systems and modules for high security classification levels
- research and development on embedded security and cryptography
- advanced project management and moderation techniques
- expert on smart cards and side-channel resistance, theory and implementation
- development of smart card long integer arithmetic unit for Infineon Technologies
- installation and commissioning of Siemens CT IC 3 side-channel laboratory
- security consulting and secure system design for business units, e. g., Automotive domain, Power Transmission and Distribution, Health care, Secure Smart Metering, and Smart Cards
- random number generator design and statistical evaluation
- strong background on mathematics and statistics
- teaching experience on cryptology, information securtiy, mathematics, and statistics
- regular participant of Workshop on Cryptographic Hardware and Embedded Systems (CHES), Workshop on Embedded Security in Cars (ESCAR), EUROCRYPT, CRYPTO, and several related conferences and workshops
- successful examination Common Criteria 3.1 BSI-Workshop: “Preparation of Protection Profiles / Security Targets”, “Introduction into Evaluation Methodology”

Positions

since 10/2010 Development Principal
Research and Development, Rohde & Schwarz SIT GmbH, Stuttgart

Responsibilities

- Developing crypto technology for mission critical environments (government, armed forces, critical infrastructures, and industry)
- Design of crypto systems and modules for high security classification levels
- Supervision of master thesis with topic "Efficient Implementation of a Generic Coprocessor for Elliptic Curve Cryptography on Reconfigurable Hardware"

05/2007–09/2010 Senior Expert (Fachreferent)
Corporate Sector Research and Advance Engineering, Software (CR/AEA),
Robert Bosch GmbH, Stuttgart

Responsibilities

- Research and development: cryptography and security for embedded systems, especially in automotive industry
- Expert on applied cryptography, establish a security and cryptography group within Bosch, project management, RB-wide lectures and training, security consulting for business units, perform internal security projects (e. g. secure rail pressure sensor, tuning protection, feature activation, flash protection, secure audio transmission, etc.), increase security awareness
- Supervision of master thesis and internships with topics "Efficient AES Implementation" and "Side-Channel Resistant AES-Implementation"
- BMBF project "Side-Channel Analysis for Automotive Security (SCAAS)"

11/1999–04/2007 Senior Research Scientist & Project Manager
(Research Scientist/Development Engineer 11/1999–10/2001)
Corporate Technology, Information & Communications Division, Security Technologies (CT IC 3), Competence field Cryptography, Siemens AG, Munich

Responsibilities

- Research and development: cryptography and IT security; especially public key cryptography using elliptic curves, smart cards and IT security
- Selected projects:
  - Construction of cryptographically strong elliptic curves [1999/2000]
  - Analysis of long integer arithmetic unit ACE, design of new smart card long integer arithmetic unit Crypto2000 for Infineon Technologies AG [2000/2001]
  - ECC signature solution for BMWi project SELMA (Secure Electronic Metering) [2001/2002]
  - Digital tachograph: cryptographic methods, code review, security concepts, project management [2003–2005]
  - Security for odometers and secure access to multi-function instruments: consulting, requirements and specification documents, security concepts [2004/2005]
  - Project management: "Secure and Efficient Implementation of Cryptographic Methods – Side-Channel Lab", installation and commissioning of Side-Channel Lab [01/2004–04/2007]
    Specialist side-channel attacks and countermeasures
  - Security consulting for Boeing Phantom Works (Seattle): strong cryptography on RFID tags, secure long-term archiving of digitally signed documents [2006]

  - EU project “Secure Middle-ware in Embedded Peer to Peer (SMEPP)” [11/2006–04/2007]
- Establishment and management of CT IC 3 Colloquium “Cryptography and Applications” [01/2000–04/2007]
- Supervision of master thesis/bachelor thesis/internships with topics side-channel attacks, long integer arithmetic units, elliptic curves, and smart cards
- IT-Security consultant for Siemens Business Units, lectures and training for Siemens and Infineon, Representation in national and international working groups, workshops, and conferences

09/1997–10/1999 Scientific Research Assistant, Post Doc
DFG-funded research group “Identification and optimization of complex models based on the calculation of analytical sensitivities”
Dresden University of Technology, Institute of Scientific Computing/Numerical Mathematics

Development and application of optimization methods, interdisciplinary research
large scale optimization/high performance computing/automatic differentiation

09/1993–08/1997 Scientific Research Assistant
DFG-Project “Shape Preserving Spline Approximation”
Dresden University of Technology, Institute of Numerical Mathematics

Numerical methods of approximation theory, numerical linear algebra,
nonlinear optimization and parameter estimation

Education and Degrees

January 1998 Dr. rer. nat. (Ph.D. in Mathematics/Theoretical Physics)
Thesis: “Diskrete Quadratmittelapproximation durch Splines mit freien Knoten”
(Discrete least squares approximation by splines with free knots)
Dresden University of Technology, Faculty of Mathematics and Natural Sciences

09/1993–09/1997 Ph.D. student (Supervisor Prof. Dr. H. Schwetlick)
Dresden University of Technology

June 1993 Diplom-Mathematiker (M.Sc. in Mathematics)
Thesis: Quadratmittelapproximation durch B-Splines mit freien Knoten

09/1988–06/1993 Study of mathematics and theoretical physics
Martin-Luther-University Halle/Wittenberg, Dept. of Mathematics

Primary and Secondary Education

09/1986–08/1988 Abitur, “Spezialklassen für Mathematik und Physik” (special classes for mathematics and physics), Martin-Luther-University Halle/Wittenberg

09/1976–08/1986 Polytechnische Oberschule Klettenberg

Workshops and Teaching

03/2010–09/2010 Teaching appointment: Einführung in die Informationssicherheit (Introduction to information security), Heilbronn University

September 2009 Invited Lecturer, Sommerakademie der Studienstiftung des Deutschen Volkes, La Colle-sur-Loup, France, September 20–Oktober 3, 2009
Applied Cryptography and Security Engineering,
together with Prof. Susanne Wetzel, Stevens Institute of Technology, Department of Computer Science, Hoboken, NJ 07030 USA

August 2006 Invited Lecturer, Max Weber-Programm der Studienstiftung des Deutschen Volkes, Sommerakademie Neubeuern, August 6–19, 2006
Security and Privacy in a Networked World
together with Prof. Susanne Wetzel, Stevens Institute of Technology, Department of Computer Science, Hoboken, NJ 07030 USA and Dr. Bernd Meyer, Siemens AG, CT IC 3

August 2005 Invited Lecturer, Sommerakademie der Studienstiftung des Deutschen Volkes, Salem, August 14–27, 2005
Kryptographie: Theorie und Praxis
together with Prof. Susanne Wetzel, Stevens Institute of Technology, Department of Computer Science, Hoboken, NJ 07030 USA

Academic and University Engagement

April 2010 offer on W2-professorship “Angewandte Informatik, insbesondere IT-Sicherheit und Softwareentwicklung”, Heilbronn University, refused

continuously Peer review for scientific journals and conferences

01/1999–10/1999 Member of committee for IT development at Dpt. of Mathematics, Dresden University of Technology

1994–1997 Member of faculty committee at Institute of Numerical Mathematics, Dresden University of Technology

1992–1993 Member of appointment committees at Dpt. of Mathematics and Computer Science, Martin-Luther-University Halle/Wittenberg

1991–1993 Member of committee of ministry of higher education in Sachsen-Anhalt, Martin-Luther-University Halle/Wittenberg

04/1990–06/1993 Member of faculty committee at Dpt. of Mathematics and Computer Science, Martin-Luther-University Halle/Wittenberg

IT-Skills

Administration

- TeX-administration at the department (TU Dresden)
- System administration Linux, Solaris, Windows (TU Dresden)

Organization

- Establishment & management of Siemens CT IC 3 Colloquium Cryptography and Applications [01/2000–04/2007]
- Installation and commissioning of Side-Channel Lab [01/2004–04/2007]
- Member of AG Rechentechnik (TU Dresden) (1994–1999)
- Organizer of Dresdner TeX User Group (1995–1999)

Skills

- Detailed knowledge of cryptographic methods, Internet protocols, and cryptographic libraries
- Practical experience with intrusion detection systems and vulnerability scanners; Consulting for operating system security for Siemens CERT
- Linux and Matlab specialist, specialist for typesetting system LaTeX
- Programming languages C, Fortran, Pascal
- Detailed knowledge about secure programming techniques and relevant tools
- Quick adoption to new programming languages

Further Interests

Memberships	International Association for Cryptologic Research (IACR) Society for Industrial and Applied Mathematics (SIAM) Deutsche Anwendervereinigung TeX e.V. (DANTE) Gesellschaft für Informatik (GI)
Languages	German (native language) English (fluent in written and oral) Russian (good)
Hobby's	Theater, literature, typography and typesetting with LaTeX

Talheim, 2016-02-08

External Publications

[1] T. Schütze. Quadratmittelapproximation durch B-Splines mit freien Knoten. Diplomarbeit, Martin-Luther-Universität Halle/Wittenberg, Fachbereich Mathematik und Informatik, 1993.

[2] H. Schwetlick and T. Schütze. Least squares approximation by splines with free knots. *BIT*, 35(3):361–384, 1995.

[3] T. Schütze. Quadratmittelapproximation durch B-Splines mit freien Knoten und Ungleichheitsnebenbedingungen an Ableitungen. Forschungsbericht im Rahmen des DFG-Projektes Schm 968/2-1, 1995.

[4] T. Schütze. FREE – A program for constrained approximation by splines with free knots. Preprint MATH-NM-04-1996, Technical University of Dresden, 1996.

[5] T. Schütze and H. Schwetlick. Constrained approximation by splines with free knots. *Z. Angew. Math. Mech.*, 77 Suppl. 2:S 669–S 670, 1997.

[6] T. Schütze and H. Schwetlick. Constrained approximation by splines with free knots. *BIT*, 37(1):105–137, 1997.

[7] T. Schütze. *Diskrete Quadratmittelapproximation durch Splines mit freien Knoten.* Dissertation, Technische Universität Dresden, 1997.

[8] E. Hess, N. Janssen, B. Meyer, and T. Schütze. Information leakage attacks against smart card implementations of cryptographic algorithms and countermeasures—a survey. In *Proceedings of EUROSMART Security Conference, June 2000, 13–15*, pages 55–64, Marseille, France, 2000.

[9] H. Schwetlick and T. Schütze. Estimates for Kaufman's Approximation in Constrained Semi-Linear Least Squares. GAMM-Jahrestagung 2001, February 12 – 14, 2001, ETH Zürich, Schweiz, 2001.

[10] T. Schütze and H. Schwetlick. Bivariate free knot splines. *BIT. Numerical Mathematics*, 43(1):153–178, 2003.

[11] C. Ruland, L. Lo Iacono, T. Schütze, and M. Kahmann. SELMA AP 1.5 – Sicherheitskonzept, Version 4.2.3. In N. Zisky, editor, *Das SELMA-Projekt. Konzepte, Modelle, Verfahren*, volume PTB-IT-12, pages 165–246. Physikalisch-Technische Bundesanstalt, March 2005.

[12] M. Angele, C. Ruland, and T. Schütze. SELMA AP 1.4 – Sicherheitsanalyse. In N. Zisky, editor, *Das SELMA-Projekt. Konzepte, Modelle, Verfahren*, volume PTB-IT-12, pages 117–164. Physikalisch-Technische Bundesanstalt, March 2005.

[13] T. Schütze. Side-Channel Analysis – a comparative approach on smart cards, embedded systems, and high security solutions, December 2010. Talk at Workshop on Applied Cryptography: Lightweight Cryptography and Side-Channel Analysis Nanyang Technological University, Singapore, December 3, 2010.

[14] T. Schütze. Automotive security: Cryptography for Car2X communication, March 2011. Talk at Embedded World Conference 2011, Nürnberg, Germany, March 1-3, 2011, Workshop on Cryptography and Embedded Security, March 1, 2011, 26 slides, 16 pages paper.

[15] Manfred Lochter, Johannes Merkle, Jörn-Marc Schmid, and Torsten Schütze. Requirements for standard elliptic curves. Cryptology ePrint Archive, Report 2014/832, 2014. `http://eprint.iacr.org/`.

[16] Manfred Lochter, Johannes Merkle, Jörn-Marc Schmid, and Torsten Schütze. Requirements for elliptic curves for high-assurance applications. Technical report, NIST Workshop on Elliptic Curve Cryptography Standards, 2015. `http://www.nist.gov/itl/csd/ct/ecc-workshop.cfm`.