

CURRICULUM VITAE

Dr. Torsten Schütze
Königsberger Str. 50
D-71696 Möglingen, Germany
Phone: +49 71 41 / 5 07 20 19
Mobile Phone: +49 1 73 / 6 51 45 22
E-Mail: torsten.schuetze@bosch.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: single

Professional background

Dr. rer. nat., Mathematician & Cryptographer

Möglingen, 2008-10-24

PROFESSIONAL EXPERIENCE

- research and development on embedded security and cryptography
- more than ten years of experience with applied and industrial cryptography
- expert on Smart Cards and Side Channel Resistance, theory and implementation
- involved in 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, Smart Cards
- strong background on mathematics and statistics
- teaching experience on cryptology, 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
- advanced Project Management and Moderation Techniques
- successful examination Common Criteria 3.1 BSI-Workshop: “Preparation of Protection Profiles / Security Targets”, “Introduction into Evaluation Methodology”

POSITION

- since 05/2007 Fachreferent (Senior Expert)
Corporate Sector Research and Advance Engineering, Software (CR/AEA),
Robert Bosch GmbH, Stuttgart
- Research and Development:
Cryptography and Security for Embedded Systems, especially in Automotive Industry
- Tasks and Mission:
Expert on Applied Cryptography, establish a Security and Cryptography Group, Project Management, Internal Lectures & Security Consulting for Business Units, perform internal security projects, increase security awareness
- 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
- Research and Development:
Cryptography and IT security; especially public key cryptography using elliptic curves, side channel attacks and countermeasures, smart cards and embedded systems, secure and efficient implementations, design of secure systems, Automotive Security applications (Digital Tachograph, Secure Odometers, Secure Access to Multifunction Instruments)
- 09/1997–10/1999 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,
large scale optimization/high performance computing

09/1993–08/1997 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”
Martin-Luther-University Halle/Wittenberg

09/1976–08/1986 Polytechnische Oberschule Klettenberg

WORKSHOPS

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 Wetzels, 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 Wetzels, Stevens Institute of Technology, Department of
Computer Science, Hoboken, NJ 07030 USA

IT-SKILLS

- | | |
|----------------|---|
| Administration | <ul style="list-style-type: none">• T_EX-Administration at the department (TU Dresden)• system administration Linux, Solaris, Windows NT/2000 (TU Dresden) |
| Organization | <ul style="list-style-type: none">• Foundation & management of Siemens CT IC 3 Krypto-Kolloquium (2000–2007)• member of AG Rechentechnik (TU Dresden) (1994–1999)• organizer of Dresdner T_EX-Anwendertreffen (1995–1999) |
| Skills | <ul style="list-style-type: none">• Linux and Matlab specialist• L^AT_EX specialist• programming languages C, Fortran, Pascal• quick adoption to new programming languages |

FURTHER SKILLS AND INTERESTS

- | | |
|-------------|---|
| Memberships | International Association for Cryptologic Research (IACR)
Society for Industrial and Applied Mathematics (SIAM), SIAG Optimization
Deutsche Anwendervereinigung T _E X e.V. (DANTE) |
| University | Active participation in academic administration (MLU Halle, TU Dresden, 1990–1999) |
| Languages | German (native language)
English (fluent in written and oral)
Russian (good) |
| Hobby's | Theater, Literature, L ^A T _E X |

- [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.