

Jamshid Shokrollahi

Address

Professional:

B-IT Center for Information Technology
University of Bonn
Dahlmannstr. 2
53113 Bonn
Germany

Private:

Draisstr. 11
76135 Karlsruhe



Phone: +49-228-269-9212 (o)
+49-174-177-1284 (m)
Fax: +49-228-2699241 (o)
Email: Jamshid@bit.uni-bonn.de

Personality

Name	Jamshid Shokrollahi
Birthday	29/12/1969
Marital Status	Married, no children
Nationality	Iranian
Immigration status	Unbefristete Aufenthaltserlaubnis

Education

<i>Ph.D.</i>	Computer science, University of Paderborn and University of Bonn, Germany	2000 - now
<i>M.Sc.</i>	Power engineering, Sharif University of Technology, Iran	1992-1996
<i>B.Sc.</i>	Control engineering, Sharif University of Technology, Iran	1987-1992

PhD Thesis

Efficient implementation of Elliptic Curve Cryptography on FPGAs (project supported by DFG).

Master's Thesis

Design and implementation of an induction motor speed controller by means of an 8031 based microcontroller system.

Bachelor's Thesis

Design and implementation of a PID-controller based on a Z80 microprocessor.

Research Interests

Digital hardware design (FPGAs and embedded systems), Cryptography, security, image processing, computer algebra (implementation in both software and hardware), efficient programming on different platforms, and coding theory.

Honors and Awards

- Rank 87 of ca. 3000 in M.Sc. entrance examination.
- Rank 90 of ca. 30000 in B.Sc. entrance examination.
- Preliminary rank in Iranian Mathematics Olympiad: 9.

Skills

- Digital hardware design, VHDL programming.
- Embedded system programming

- Programming in several programming languages such as C++, C, Matlab, Java, and PERL.
- Microsoft .NET, C++ applications, Internet applications (MFC and PERL).

Work Experience

- Design and development of “ECDSA Java Security Provider” for the “Raptor PCI Card”. (September 2003), SFB-376, computer science department, University of Paderborn.
- Design and development of an elliptic curve cryptography coprocessor using XCV2000E FPGA. (May 2000 - September 2003), SFB-376, computer science department, University of Paderborn.
- Research engineer, Fajr Electronic & Micro Computer Co. Ltd. (1998-2000)
- Development of a Persian ActiveX control for use on the Web, (August 1998 - December 1998), developed for Sharif University of Technology.
- Development of an industrial process monitoring system, (January 1998 - October 1998), developed for KALEH meat products company.
- Compulsory military service, Iranian Navy (1996-1998).
- Development of a train wheel fault detection system based on image finding and processing, (July 1997 - August 1998), developed for national Iranian railroad.

Research Assistance

- **January 2005 - now**, *towards Ph.D.*, computer security working group, B-IT Center for Information Technology, University of Bonn, Germany.
- **May 2000 - January 2005**, the algorithmic mathematics working group, computer science department, university of Paderborn, Germany.
- **March 1993 - March 1995**, Electronics research center, Sharif university of Technology, Tehran, Iran.

Talks

- 2005 SAC (Selected Areas in Cryptography) 2005, Kingstone, Canada, Efficient FPGA-based Karatsuba multipliers for polynomials over \mathbb{F}_2
- 2005 MINI SYMPOSIUM on CRYPTOGRAPHY, University of Zürich, Elliptic curve cryptography on FPGA
- 2003 Workshop über Algebraische Kodierungstheorie, Dortmund, Germany, FPGA-basierte Implementierung eines Karatsuba Multiplizierers in $\mathbb{F}_{2^{233}}$
- 2002 HGI Seminar, Bochum, Germany, Area/performance tradeoffs for reconfigurable elliptic curve coprocessors

Refereed Publications

1. Fast Arithmetic for Polynomials over \mathbb{F}_2 in hardware, Joachim von zur Gathen, Jamshid Shokrollahi, In IEEE Information Theory Workshop (ITW'2006), 107–111.
2. Efficient FPGA-based Karatsuba multipliers for polynomials over \mathbb{F}_2 , Joachim von zur Gathen, Jamshid Shokrollahi, In Selected Areas in Cryptography (SAC 2005), 359–369.
3. A High Performance VLIW Processor for Finite Field Arithmetic. C. Grabbe, M. Bednara, M. Daldrup, J. Teich, J. von zur Gathen, J. Shokrollahi, In Proc. of The 10th Reconfigurable Architectures Workshop (RAW-03).
4. FPGA Designs of parallel high performance $GF(2^{233})$ Multipliers. C. Grabbe, M. Bednara, M. Daldrup, J. Teich, J. von zur Gathen, J. Shokrollahi, In Proc. of the IEEE International Symposium on Circuits and Systems (ISCAS-03), volume II, 268-271. Bangkok, Thailand.
5. Tradeoff Analysis of FPGA based Elliptic Curve Cryptography, M. Bednara, M. Daldrup, J. Teich, J. von zur Gathen, J. Shokrollahi, IEEE International Symposium On Circuits and Systems (ISCAS 2002).

6. Reconfigurable Implementation of Elliptic Curve Crypto Algorithms. M. Bednara, M. Daldrup, J. von zur Gathen, J. Shokrollahi, J. Teich, Reconfigurable Architecture Workshop (RAW 2002).
7. An Image Processing Based System for Wheel and Flange Profile Measurement, Kambiz Nayebi, Jamshid Shokrollahi, World Congress on Railway Research (WCRR'99).

Technical Reports

1. Practical tests for Analyzing Pseudo Random Sequences and Block Cipher Systems, (Joint with S. Parsa, S. Sadeghian, J. Mohajeri), Technical Report, Electronic Research Center of Sharif University of Technology, 1994.
2. Design and Simulation of a Gearbox Controller, (Joint with S. Ghaem-Maghami, A. Shadravan), Technical Report, Electronic Research Center of Sharif University of Technology, 1994.
3. Hardware and Software Development for PLC, (Joint with A. Afsahi, M. Rastegar-Khojasteh, M. Saheb-Sara), Technical Report, Electronic Research Center of Sharif University of Technology, 1993.

Scientific Activities

- Review of papers for Workshop on Fault Diagnosis and Tolerance in Cryptography (2004).
- Review of papers for CHES 2002 (Cryptographic hardware and embedded systems).
- Review of papers for IEEE Transactions on Computers.

Teaching Experience

- Efficient Cryptography, Computer Security Group, B-IT, Bonn, 2005.
- Teaching assistant for the course Mathematics II for computer science students, Computer Science Department, University of Paderborn, 2004.
- Teaching assistant for the course Mathematics I for computer science students, Computer Science Department, University of Paderborn, 2003.
- Teaching assistant for the course Analysis I, Computer Science Department, University of Paderborn, 2003.
- Teaching assistant for the course Cryptography I, Computer Science Department, University of Paderborn, 2000.
- Teaching assistant for the course Power Electronics, Electrical Engineering Department, Sharif University of Technology, Tehran, 1994.

Languages

English	Fluent in reading, speaking, and writing
German	Fluent in reading and speaking, good in writing
Farsi	Mother tongue