RESUME

Name: **Sandeep S. Kumar**
Address: HTC 34.6.027 (MS 61)
High Tech Campus 34
5656AE Eindhoven, Netherlands
Phone: +49-(0)234-3224080
E-mail: kumar @ sandeep. de

Sex: Male
Nationality: Indian
Marital Status: Married

EXPERIENCE

Philips Research Europe, Eindhoven, Netherlands

Senior Scientist – *"Information and System Security Group"* **Dec 2006 - present**

- Researched on Intellectual Property (IP) protection and anti-counterfeiting of electronic devices using Physcially Unclonable Functions (PUF). Technologies were developed for FPGA's to bind the programming code to each individual hardware chip to prevent cloning of the device. Also closely assisted the PUF related business initiative IntrinsicID within Philips.
- Presently working in the area of Digital Identity Management for consumer lifestyle applications. Emphasis is on trust and reputation management technologies which enables trustworthy transaction decisions.

Infineon Technologies Austria AG, Graz, Austria.

Internship – "Evaluation and Feasibility Study for application of Elliptic Curve Cryptography for RFID Systems" **Jan. 2006 – Mar. 2006**

Evaluation of energy requirements for various semi-custom designed co-processor and algorithmic alternatives for ECC on an RFID device. The project involved design and evaluation using the state-of-the-art ASIC tools.

Ruhr-University-Bochum, Germany

Research Assistant – *"Communication Security Group"* **Sep. 2002 –Nov. 2006**

- Low cost implementation of Elliptic Curve Cryptography (ECC) on 8-bit processors.
- Implementation of public key crypto algorithms based on elliptic curves on FPGAs.
- Hardware/Software co-design of ECC for 8-bit and 32-bit micro-controller.
- Implementation of symmetric block and stream ciphers on FPGAs.
- Guidance of BS thesis and MS thesis.
- Peer reviews for many established international conferences and journal publications.

Ruhr-University-Bochum, Germany

Teaching Assistant – "*Implementation of Cryptographic Algorithms*" **Winter Semester 2004, Winter Semester 2005**

Collaborated on curriculum and exam development, met with students upon request, graded all written work including various assignments for implementing cryptographic algorithms in C-programming.

Indian Institute of Technology-Bombay, India

Teaching Assistant – "*Digital Circuits Course*" & "*Digital Signal Processing Lab"* **2001- 2002**

Collaborated on curriculum and exam development, in charge of teaching students DSP programming, met with students upon request, graded all written work including various assignments for simulating digital circuits in C-programming.

EDUCATIONAL QUALIFICATIONS

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

Ph.D. (Dr.-Ing.) in Electrical and Computer Engineering **Sep. 2002 –July 2006**

Thesis title: ***"Elliptic Curve Cryptography in Constrained Devices"***

Supervisor: Prof. Dr.-Ing. Christof Paar

***Research Area**:*

- Elliptic Curve Cryptography.
- Low cost and constrained environment crypto-systems.
- FPGA implementation of Cryptographic Algorithms.
- Fast Software and Hardware Implementation of Cryptographic Algorithms.

Projects:

- *"Elliptic curve cryptography on constrained 8-bit processors",* sponsored by SUN Microsystems, California(USA), Sep 2002 – May 2003.
- *"Secure Wireless communication on constrained RF devices",* working model presented at SUN Networks 2003, sponsored by SUN Microsystems (USA), July 2003 – Sep 2003.
- *"ECDSA library for 8-bit smart card controller",* for a leading smart card manufacturer, Nov 2004 – Jan 2005.
- *"ABC stream cipher"*, implementation for eSTREAM – ECRYPT Stream Cipher Call, March 2005 – April 2005.
- *"COBRA – Cost Optimized BRute Force Attacker",* May 2005 – Feb 2006.
- *"Elliptic Curve Cryptography for RFID and sensor networks"*, Aug 2005 – present.

***Indian Institute of Technology-Bombay,** Mumbai, India*

Master of Technology, Communications and Signal Processing, Electrical Engineering **2001-2002**

Specialization in Cryptography
Thesis: "*Crypto Accelerator for IPsec on ARM core*"

Related Coursework:

- Advanced Internet Technologies
- Wireless and Mobile Communication
- Image Processing
- Adaptive Signal Processing
- Wavelets
- Digital Message Transmission
-

Other projects: *GPRS in Network Simulator(ns)*
The publicly available Network Simulator(ns) was extended to simulate General Packet Radio Service(GPRS).

***Indian Institute of Technology-Bombay,** Mumbai, India*

Bachelor of Technology, Electrical Engineering **1997-2001**

Related Coursework:

- Embedded Systems
- Digital Signal Processing
- Communication Networks
- Operating Systems
- Information Theory & Coding

Other projects: *Spectacles for the Blind*.

COMPUTER SKILLS

Programming Languages:	*C, C++, Java, Fortran, Tcl.*
Assembly Level:	*TI-DSP TMS320C50,* *Microprocessor (8085, ARM family),* *Microcontrollers (8051 family).*
Operating Systems:	*Linux, Windows, Solaris.*
Hardware Description Languages and Tools:	*VHDL, Xilinx ISE tools, Altera Quartus tools, Synopsis Design Compiler tools, Mentor Graphic tools.*
Misc. Packages and Simulator:	*Matlab, Maple, ARM SDK, Network Simulator (ns).*

SELECTED PUBLICATIONS

BOOKS & BOOK CHAPTERS

- Sandeep Kumar, "*Elliptic Curve Cryptography for Constrained Devices: Algorithms, Architectures, and Practical Implementations*", VDM Verlag, 2008.
- Sandeep Kumar, Thomas Wollinger, "*Fundamentals of Symmetric Cryptography*" in Embedded Security in Cars, Springer-Verlag, 2005.
- Thomas Wollinger, Sandeep Kumar, "*Fundamentals of Asymmetric Cryptography*" in Embedded Security in Cars, Springer-Verlag, 2005.

JOURNAL PUBLICATIONS

- Sandeep Kumar, Thomas Wollinger and Christof Paar, "*Optimum Hardware GF(2^m) Multipliers for Curve Based Cryptography*", IEEE Transactions on Computers, Volume 55, Issue 10, pp. 1306-1311, October 2006.
- Guajardo, S. S. Kumar, C. Paar, J. Pelzl, "*Efficient Software-Implementation of Finite Fields with Applications to Cryptography*", Acta Applicandae Mathematicae: An International Survey Journal on Applying Mathematics and Mathematical Applications, Volume 93, Numbers 1-3, pp. 3-32, Sept 2006.
- J. Guajardo, T. Güneysu, S. S. Kumar, C. Paar, J. Pelzl, "*Efficient Hardware Implementation of Finite Fields with Applications to Cryptography*", Acta Applicandae Mathematicae: An International Survey Journal on Applying Mathematics and Mathematical Applications, Volume 93, Numbers 1-3, pp. 75-118, Sept 2006.
- S. Baktir, S. Kumar, C. Paar, B. Sunar, "*A State-of-the-art Elliptic Curve Cryptographic Processor Operating in the Frequency Domain*", Mobile Networks and Applications (MONET) Journal, Special Issue on Next Generation Hardware Architectures for Secure Mobile Computing, vol 12, no 4, pp 259-270, Sept 2007.
- Thomas Eisenbarth, Sandeep Kumar, Christof Paar, Axel Poschmann, Leif Uhsadel, "*A Survey of Lightweight-Cryptography Implementations*," IEEE Design and Test of Computers, vol. 24, no. 6, pp. 522-533, Nov 2007.
- Guajardo, J., Škorić, B., Tuyls, P., Kumar, S., Bel, T., Blom, A. & Schrijen, G.-J. (2008), *"Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions"*, Information Systems Frontiers.

INTERNATIONAL CONFERENCES

- G. Bertoni, J. Guajardo, S. Kumar, G. Orlando, C. Paar, T. Wollinger, "*Efficient GF(p^m) Arithmetic Architectures for Cryptographic Applications",* Cryptographer's Track of the RSA Conference 2003, San Francisco, USA, April 2003.
- Sandeep Kumar, Marco Girimondo, André Weimerskirch, Christof Paar, Arun Patel, Arvinderpal S.Wander, "*Embedded End-to-End Wireless Security with ECDH Key Exchange*", 46th IEEE Midwest Symposium On Circuits and Systems 2003, Cairo , Egypt, December 2003.
- Sandeep Kumar, Christof Paar, "*Reconfigurable Instruction Set Extension for enabling ECC on an 8-bit Processor*", International Conference on Field-Programmable Logic and Applications (FPL) 2004, Antwerp, Belgium, August 2004.
- Johann Großschädl, Sandeep Kumar, Christof Paar, "*Architectural Support for Arithmetic in*

Optimal Extension Fields", IEEE 15th International Conference on Application-specific Systems, Architectures and Processors (ASAP) 2004, Galveston, Texas, September 2004.

- Sandeep Kumar, Kerstin Lemke, Christof Paar, "*Some Thoughts about Implementation Properties of Stream Ciphers*", SASC - State of the Art of Stream Ciphers Workshop, Belgium, October 2004.
- Sandeep Kumar, Christof Paar, Jan Pelzl, Gerd Pfeiffer, Andy Rupp, Manfred Schimmler, "*How to Break DES for Euro 8,980*", Special-purpose Hardware for Attacking Cryptographic Systems (SHARCS 2005), Cologne, Germany, April 2006.
- S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer, M. Schimmler, "*A Configuration Concept for a Massive Parallel FPGA Architecture*", Int. Conference on Computer Design (CDES 2006), USA, June 2006.
- Sandeep Kumar, Christof Paar, *"Are standards compliant elliptic curve cryptosystems feasible on RFID"*, to be presented at Workshop on RFID Security 2006, Graz, Austria, July 2006.
- Sandeep Kumar, Christof Paar, Jan Pelzl, Gerd Pfeiffer, Manfred Schimmler, "*Breaking Ciphers with COPACOBANA - A Cost-Optimized Parallel Code Breaker*", Cryptographic Hardware and Embedded Systems (CHES 2006), Japan, October 2006.
- Jorge Guajardo, Sandeep S. Kumar, Geert-Jan Schrijen, Pim Tuyls, "*Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection*", Int. Conference on Field Programmable Logic and Applications (FPL), Aug 27-29, 2007, Amsterdam, The Netherlands.
- Jorge Guajardo, Sandeep S. Kumar, Geert-Jan Schrijen, Pim Tuyls, "*FPGA Intrinsic PUFs and Their Use for IP Protection*", Workshop on Cryptographic Hardware and Embedded Systems (CHES), Sep 10-13, 2007, Vienne, Austria.
- Guajardo, J., Kumar, S., Schrijen, G.-J. & Tuyls, P. (2008), *"Brand and IP protection with physical unclonable functions"*, In IEEE International Symposium on Circuits and Systems, 2008. ISCAS 2008. May 2008., pp. 3186-3189.
- Kumar, S., Guajardo, J., Maes, R., Schrijen, G.-J. & Tuyls, P. (2008), *"Extended abstract: The butterfly PUF protecting IP on every FPGA"*, In IEEE International Workshop on Hardware-Oriented Security and Trust, 2008 -- HOST 2008.. June 2008., pp. 67-70.

INVITED PRESENTATIONS

- *"Accelerating IPsec using ARM core"*, July 2002, Cirrus Logic, Pune, India.
- *"Elliptic Curve Cryptography for sensor networks"*, NEC-Lab, Heidelberg, Germany.
- *"ECC implementation using 8-bit processor instruction set extension on FPGA"*, June 2004, CryptArchi-2004, Abbey La Bussière, France.
- *"Reconfigurable Instruction Set Extension for Enabling ECC on an 8-bit Processor*", July 2004, ECRYPT-VAMPIRE Meeting, Graz, Austria.
- *"Physically Unclonable Functions (PUFs) for IP Protection on FPGA",* June 2008, CryptArchi-2008, Trégastel, France.

AWARDS AND RELATED ACTIVITIES

- Scholar of the prestigious National Talent Search Exam held by N.C.E.R.T., India in 1995.
- Stood 1st in the Web Design Contest organized by IIT-Bombay.
- Held the post of Computer Secretary of the Department for the year 2000-01 and was actively involved in the revamping of the EE-Department homepage & database setup with an easily updateable facility, and automation of some routine procedures like Project allotment, Teaching Assistant allotment and Time-Table generation.
- Participated in Yantriki-98, the annual robotics competition of IIT-Bombay.
- Was coordinator of Competitions, Mood Indigo-98, the annual cultural festival of IIT-Bombay.

LANGUAGES

Fluent in English, German and Hindi

Dutch beginners level