In the name of God

Curriculum Vitae (as of Dec. 2010)

Personal

Sayyed Hamid Reza Ahmadi

Born in 1977, Tehran, Iran.
Married since 1999.

Contact:

Cellular: +98 912 6053505

Email : hrahmadi@ut.ac.ir and also, shr_a@hotmail.com

Honors

1. 2004
   Ranked **No. 1** in UT-ECE PhD entrance exam (Computer Engineering - Hardware).

2. 2001
   Ranked **No. 2** among M.Sc. graduate students in Electronics Engineering.

3. 1998
   Ranked No. 1 among all B.Sc. students in Electrical & Computer Engineering

4. 1994
   Ranked No. 2 (total ranking) and No. 4 (first part ranking)
   in nationwide university entrance exams among more than 300,000

Educational

- **2008-present**
  Ph.D. Candidate in Computer Engineering, University of Tehran

  Supervisor: Prof. A. Afzali-Kusha
  Research Subject: "Low-Power Hardware for Elliptic-Curve Cryptography"

- 2005-2007
  Ph.D. Student in Computer Engineering, University of Tehran

  GPA: 18.67 / 20

- 1999-2001
  M.Sc. Degree in Electrical and Electronics Engineering, University of Tehran

  Thesis Supervisor: Dr. Omid Shoaei
  M.Sc. Thesis title: "Design of Very High-speed Folding and Interpolating Analog-to-Digital Converters in CMOS"

  GPA : 18.15 / 20

  * Passed courses on VHDL and VerilogHDL, and a course on DSP
  * Designed an FIR filter from VHDL coding to final layout
  * Developed a full-functional synthesizable PAR-1 processor

- 1995-1998
  B.Sc. Degree in Electrical and Electronics Engineering, University of Tehran

  GPA : 18.65 / 20

  * Worked on a mixed analog-digital electronic kit for power measurements, including an Intel's 80C196 micro-controller.
  * Passed courses on Intel's 80x86 and Motorola's MIPS R3000 microprocessors

- 1994
  Diploma of Physics and Mathematics, Alavi High school

  GPA : 19.44 / 20

Publications

Journals

1- **H. R. Ahmadi**, A. Afzali-Kusha, and M. Pedram, "A Power-Optimized Low-Energy Elliptic-Curve Crypto-processor", *IEICE Electronics Express*, Vol. 7, No. 23, pp.1752-1759, Dec. 2010.

2- **H. R. Ahmadi**, and A. Afzali-Kusha, "A Low-Power and Low-Energy Flexible GF(p) ECC Processor," *Journal of Zhejiang University - Science C*, vol. 11, no. 9, pp. 724-736, Sep. 2010.

Conferences

1- **H. R. Ahmadi**, and A. Afzali-Kusha, "Low-Power Low-Energy Prime-Field ECC Processor Based on Montgomery Modular Inverse Algorithm," in Proceedings of 12th Euromicro Conference on Digital System Design, Patras, Greece on Aug. 27-29, 2009, pp. 817-822.

2- **H. R. Ahmadi**, and A. Afzali-Kusha, "Very Low-Power Flexible GF(p) Elliptic-Curve Crypto-Processor for Non-Time-Critical Applications," in Proceedings of 2009 IEEE International Symposium on Circuits and Systems, Taipei, Taiwan on May 24-27, 2009, pp. 904-907.

3- **H. R. Ahmadi**, and A. Afzali-Kusha, "Low-Power Flexible GF(p) Elliptic-Curve Cryptography Processor," in Proceedings of 3rd International Design and Test Workshop, Monastir, Tunisia on Dec. 20-22, 2008, pp. 182-186.

4- **S. Hamid R. Ahmadi**, and Omid Shoaei, "150 MS/s, 8-bits, Folding and Interpolating ADC in 0.25μm CMOS using Averaging", SCS, 2003.

5- N. Khosropour, **S. Hamid Reza Ahmadi**, and S.M. Atarodi, "A DSP Core for Telecommunication Applications," Eurasia, ICT, 2002.

6- B. Nejati, **S. Hamid R Ahmadi**, and Omid Shoaei, "Effect of Radix<2 on the Performance of Pipelined Analog-to-Digital Converters," SCS, 2001.

Research Interests

- Low-Power and Low-Energy Arithmetic Hardware Units
- Cryptography, Cryptography Algorithms, and Cryptanalysis
    - Low-Energy Hardware Implementations
    - SPA and DPA (Simple and Differential Power Analysis)
    - High-Throughput Hardware Implementations
- Hardware Units for Wireless Sensor Network Motes and RFID Tags
- FPGAs and Reconfigurable Hardware

Teaching Interests

Based on my experience in the field of cryptography and my industrial experiences in smart cards and also my experience in hardware design, I would like to teach the following courses at the graduate level:

- **Applied Cryptology** (Cryptography and Cryptanalysis)

- **E-commerce Security**
    - This course covers the area of E-payment systems. It is also possible to have a separate course on "**E-payment Systems**".

- **Data Security and Cryptography**

- **Cryptography and Communications Security**
    - This course would be better taught in collaboration with the "Communications" department in the school of ECE.

Skills and Experiences

- Extensive experience in VHDL- and VerilogHDL-based hardware design (both for modeling and synthesis)
- Experience in VHDL-based modeling of systems
- Extensive experience in the area of FPGA-based hardware implementation, working with FPGA-based minimum systems and using FPGAs in other systems
- Experience in digital hardware optimization for special applications
- Experience in digital ASIC synthesis
- Experience in Analog and Mixed-signal circuits design (integrated & board-level)

- Experience in the design of electronic circuits for use in Telephony Applications
- Experience in PCB design and laboratory testing of digital and analog circuits

- Experience in C++ programming and ASSEMBLY code developing
- Experience in many CAD tools:

  "Modelsim", "Leonardo Spectrum", "Quartus",
  "HSpice", "Tanner LEdit", "Protel",
  "SYNOPSYS Design Analyzer", etc.
- Working on SUN Microsystems's SOLARIS workstations

Industrial Experiences

- V. S. Co., Tehran branch (2000-2001)
  - Participated in the design of a pipelined analog-to-digital converter (8-bits, 50 MS/s) in 0.25µ CMOS to be used in a SOC application.
  - Design of a digital calibration block for the same pipelined ADC (HDL coded in VHDL).
    - This ADC was fabricated and worked in the SOC.

- Emad Semicon Co. (2001-2005)
  - Participated in the development of a DSP core based on the Motorola's 24-bit 56300 series processors (HDL coded in Verilog)
  - Design and optimization of an ASIC based on Intel's 8051 micro-controller, dedicated to communication applications
    - This ASIC was fabricated in both 0.5µ & 0.25µ CMOS.
    - The final product is used in a Telephone Central Switching System.
    - Also designed the testing algorithms and PCB and performed laboratory tests
  - Implementation and testing of many digital designs in ALTERA's FPGA cores
  - Participated in an "IC Layout Modification" procedure to introduce a special analog circuit into an already-fabricated digital IC
    - The resulting chip was fabricated and worked as desired.

- Others
  - Participated in the development of a DVBH Receiver Mixed-Signal ASIC Chip
  - Participated in the development and testing of a standard PCI-Express Interface Core, including the implementation of the core on Xilinx VirtexII and Xilinx VirtexIV FPGAs
  - Participated in the development of board-level Electronic circuits for use in Telephony Systems