Aria Shahverdi

⌂ ECE Department Worcester Polytechnic Institute,
125 Salisbury Street, Worcester, MA 01609

☎ (508)250-7476
✉ ashahverdi@wpi.com
www.ashahverdi.com

Education

- **Worcester Polytechnic Institute** Worcester, MA
  Pursuing M.S. in Electrical and Computer Engineering *Class of 2015*
  - Current GPA: 4.0
- **Sharif University of Technology** Tehran
  B.S. in Electrical Engineering, Major: Digital Systems *Class of 2013*
  - Last two years major's courses GPA: 3.91 (Total GPA: 3.6)

Publications

"Silent SIMON: A Threshold Implementation under 100 Slices", Under Review.

"Enabling Fully Homomorphic Encryption via Trusted Hardware", Under Review.

"MACs Going Green: Same Security, Less Energy", To Be Submitted.

C. Chen, T. Eisenbarth, **A. Shahverdi**, X. Ye, "Balanced Encoding to Mitigate Power Analysis: A Case Study", Smart Card Research and Advanced Application Conference – CARDIS 2014. [pdf]

Y. Doröz, **A. Shahverdi**, T. Eisenbarth, B. Sunar, "Toward practical homomorphic evaluation of block ciphers using prince", Workshop on Applied Homomorphic Cryptography and Encrypted Computing – WHAC14, 2014. [pdf]

A. Shahverdi, C. Chen, T. Eisenbarth, "AVRprince - An Efficient Implementation of PRINCE for 8-bit Microprocessors", Technical Report, Worcester Polytechnic Institute, 2014. [pdf]

A. Shahverdi, S. Hashemi, "Effects of Adding a Filter Cache on Power and Performance", Technical Report, Sharif University of Technology, 2013. [pdf]

R. Rafiee, S. Mahdavian, **A. Shahverdi**, "Physics for Concours", Kelke Moallem Publication, 2009. [Book in Farsi]

Experience

- **Worcester Polytechnic Institute** Worcester, MA
  Research and Teaching Assistant *Since Fall 2013*
  - Teaching Assistant of the course "Introduction to Cryptography and Information Security", Instructor: Prof. Eisenbarth.
  - Teaching Assistant of the course "Computer Organization and Design", Instructor: Prof. Sunar.
- **Sharif University of Technology** Tehran
  Undergraduate Teaching Assistant *2011 - 2013*
  - Compiling lab manuals and coordinator for newly-offered course "Embedded System Laboratory", Supervisor: Prof. Hashemi.
  - Teaching Assistant of the course "Data Network" (Graduate Course), Instructor: Prof. Pakravan, 3 Semester.
  - Teaching Assistant of the course "Apl./Exp. Special Topics (Bluetooth)" (Graduate Course), Instructor: Prof. Vafaei.

  - Laboratory Assistant of the course "Microprocessor Systems Laboratory", Instructor: Prof. Tabandeh, 2 Semester.
  - Laboratory Assistant of the course "Computer Structure and Laboratory", Instructor: Prof. Jahed, 2 Semester.
  - Teaching Assistant of the course "Microprocessor System Design", Instructor: Prof. Sanaei.
  - Teaching Assistant of the course "Object Oriented Programming", Instructor: Prof. Vosughi Vahdat.

- **Telecommunication Company of Tehran (TCT), Access Section** Tehran
  Intern *Summer 2011*
  - Analysis of TCP/IP for LAN and Wireless LAN networks.
  - Evaluate the Behavior of IEEE 802.3 protocol and how different access methods such as Aloha and CSMA will affect a sample network.

Recent Selected Projects

- *Ongoing Projects*

Doing Studies on Leakage-Resilient Cryptography
The hardware implementation of SHA-3 and how it can be used for building a leakage-resilient encryption scheme.

Improving Fully Homomorphic Encryption Implementation using HW/SW Co-Design
The idea is to move costly operation of software to hardware in order to gain speedup.

- *During Graduate Studies*

7/2014 Analyzing The Power Performance of Proposed MAC Techniques
Proposed new Message Authentication Code (MAC) techniques suitable for low power environments such as WSN and BAN.

2/2014 Implementation of PRINCE – A Low-latency Block Cipher
This project started by implementing PRINCE cipher for microprocessor using parallel processing of states. We also proposed a way to secure the implementation against side-channel attacks. Finally, thanks to simple structure of non-linear level of this cipher we implemented homomorphic evaluation of this cipher. The results of each section has been published in different paper.

- *During Undergraduate Studies*

6/2013 Effects of Adding a Filter Cache on Power and Performance
Added a filter cache in SimpleScalar and observed its effect on power and performance by using SPEC CPU2000 benchmarks.

5/2013 Design and Simulation of an ARM7500 Processor
The structure of the processor consisted of 5-stage classic pipeline. A dedicated L1 cache for data and a dynamic branch prediction unit was also added.

5/2103 Design DQPSK Encoder and Decoder on ASIC Chip
Implemented DQPSK encoder and decoder in hardware and verified the design by using Simulink, this is called MATLAB Simulink/ModelSim co-simulation, and also generated its sample chip using Design Compiler and SOC Encounter.

5/2013 Design and Simulation of IEEE 802.11a Wireless Transmitter
Based on IEEE 802.11 standard, simulated the physical layer of this standard and verified the results with standard's test vectors. The whole process has been done in MATLAB Simulink.

2/2013 Design and Simulation of an ARM7500 Processor, Single-Cycle and Multi-Cycle
Designed a single-cycle and multi-cycle processor and verified its functionality by running the programs assembled by my assembler.

2/2013 Design and Simulation of a Cache Controller
Wrote a Verilog code for a direct mapped and set associative cache and verified its functionality in ModelSim.

1/2013 Physical Layer Simulation of The IEEE 802.15 Bluetooth Standard
Simulated the mentioned standard step by step using Simulink and verified each part with the test vectors provided in the standard.

7/2012 Implementation of Monitoring and Security Remote System (B.S. Project)
Changes in remote site should be sensed (such as temperature, gas leakage and changes in level of Infrared light) and then transmitted to near site in order to conduct appropriate reactions. In the sender site, the data to be transmitted first goes through AES encryption function and then will be encoded using Reed-Solomon function.

2/2012 Design a Dynamic Routing Agent for a Three-Layered Network Using OPNET
Simulated a whole network from packet field to MAC and network layer of each node using OPNET.

1/2012 Implementation of MAC Layer of The IEEE 802.3 Ethernet Standard on NIOS II
Implemented the MAC layer of IEEE 802.3 standard i.e. Ethernet, on DE2 board and handled its connection with DHCP.

7/2011 Implementation of The Gorillas Game in Assembly
The game consisted of one server which was programmed to conduct calculation and sending the results to two terminals which were programmed to show the results on the monitor and interface appropriately with user.

6/2011 Design Frame Synchronizer ASIC Chip for an OFDM system
Produced a ready-to tape-out ASIC chip by using Design Compiler after evaluating its performance in ModelSim.

Related Courses & Grades

Computer Security	Current	Software Security	Current
Adv. Crypt. (Graduate)	A	Inf. Theory & Coding (Graduate)	A
Crypt. & Data Security (Graduate)	A	Abstract Algebra (Graduate)	A
Computer Architecture	20.0 / 20	Computer Interface Circuits	19.0 / 20
Adv. Microprocessor (Graduate)	18.5 / 20	Microprocessor System Lab	18.8 / 20
Apl./Exp. Special Topics (Graduate)	20.0 / 20	Computer Structure	17.4 / 20
Adv. Data Networks (Graduate)	19.0 / 20	Signals & Systems	18.5 / 20
Data Networks (Graduate)	19.0 / 20	Fundamental of Electronics	17.0 / 20
IEEE 802.11a TX Simulation	20.0 / 20	Principles of Elec. Eng.	19.0 / 20

Awards and Honors

2014 Research/Teaching Assistantship in ECE Department at Worcester Polytechnic Institute.

2013 Ranked 7 among undergraduate students in Digital Systems at Sharif University of Technology.

2008 Ranked 50 in university entrance exam (among 350,000+ students).

2009 Awarded dean's honorary award from Dr. Sohrabpour, former dean of Sharif University of Technology, for exceptional performance in national university entrance exam.

2008 5 years fellowship award and member of National Elite Foundation of Iran.

2008 Ranked 165 in university entrance exam for foreign language majors.

2007 Successfully passed the 1st round of Iranian National Physics Olympiad.

Technical Skills

Professional Software: Quartus II, Xilinx ISE, Vivado Design Suite, Nios II, Modelsim, Design Compiler, SOC Encounter, CodeVision AVR, Atmel Studio, Keil μVision, Code Composer Studio, OPNET, NS3, NS2, Pspice, Proteus, Altium Designer, SimpleScalar, MATLAB, Simulink, LabVIEW,

Programming Language: C, C++, C#, Tcl, Python, Sage, Verilog, OpenGL, 8085/x86 Assembly, HTML

Basic Software: LaTeX, Microsoft Office, Dreamweaver, Microsoft Expression Web, AutoCAD, Adobe Photoshop

Operating Systems: Unix/Linux based OS's, Windows, Mac OS

Languages: Fluent in English, Farsi(Native), Basic Spanish, Familiar with Arabic

Leadership and Service

2013-Present Member of WPI's Iranian Volleyball Team

2008-2012 Organizing Yearly Reunion of Danesh High School Class of 2008 (Approx. 70 Students)

2009-2011 Teaching Advanced Math to Freshman Students in Danesh High School

2012 Volunteer Teacher for Freshman Student at Sharif University of Technology During Summer

2010 Student Volunteer in The First Iranian Conference on Smart Grid

Interests and Hobbies

Playing Soccer, Tennis, Volleyball

Archiving Iranian Classic Songs

Watching Movies