

Aida Vosoughi

Office Address: Room 2045, Duncan Hall, Electrical and Computer Engineering
Department, Rice University, Houston, TX 77005, USA.

Email: vosoughi@gmail.com, aida.vosoughi@rice.edu, **Home Page:** www.vosoughi.info
Tel: 701-4468123

Areas of Interest

Embedded Systems Design, Hardware Software Co-design, Reconfigurable Computing, Computer Architecture, Cryptography, VLSI Design, CAD, Design for Manufacturability.

Education

1/2011 – present

PhD in Electrical and Computer Engineering

Department of Electrical and Computer Engineering, Rice University, Houston, TX 77005, USA

- Courses:
 - Computer-Aided Design for VLSI
 - Energy Efficiency in Modern Systems
 - Security Topics of Embedded Systems

9/2009 – 12/2010

Master of Science in Electrical and Computer Engineering

Department of Electrical and Computer Engineering, North Dakota State University, Fargo, ND 58102, USA

Advisor: Dr. Rajendra Katti

- GPA: 4.0
- Thesis: “**On the Security of Multimedia Encryption and Authentication Schemes**”. (full grade)
 - **Abstract:** In this thesis, two compression-combined encryption schemes for multimedia data, namely Randomized Arithmetic Coding and Key-based Interval Splitting Arithmetic Coding are proved to be insecure against ciphertext-only attacks. In addition, a novel Message Authentication Code for multimedia content is proposed and proved to be secure.
- Courses:
 - Computer-Aided Verification (A)
 - Research Methods (A)
 - Systems (A)
 - Hardware for Cryptography (A)
 - Cryptology (A)
 - Algorithm Analysis (A)

9/2006 – 12/2008

Master of Science in Computer Architecture

Department of Computer Engineering, Amirkabir University of Technology, Tehran, Iran

Advisor: Dr. Mehdi Sedighi

- GPA: 19.44/20 (3.89/4), Top Student
- Thesis: “**Hardware Software Co-design Considering Reconfigurability and its Application in Implementing EFM**”. (full grade)
 - **Abstract:** In this project, I have worked on an approach to Hardware Software Co-design, in which reconfigurability of the design is a criterion in partitioning it into Hardware and Software parts. In order to verify my approach, I have implemented an EFM (Ethernet in the First Mile)/ Ethernet reconfigurable module using this co-design partitioning approach.
- Courses:
 - VLSI Design Algorithms (20/20)
 - Advanced Computer Architecture (19/20)
 - Computers and Telecommunication Network Management (18/20)
 - Hardware Modeling and Design Methodologies (20/20)
 - Advanced Operating Systems (Distributed Systems) (20/20)
 - Test and Testability (20/20)
 - Fault Tolerant System Design (19/20)

- Digital Systems Synthesis (18/20)
- Seminar (on Ethernet in the First Mile-EFM) (20/20)

9/2002 – 9/2006

Bachelor of Science in Computer Engineering

Department of Computer Engineering, Amirkabir University of Technology, Tehran, Iran

Advisor: Dr. Morteza Saheb Zamani

- GPA: 16.89/20 (3.38/4), Top Student
- GPA of last four semesters (last 70 credits): 17.57/20 (3.5/4)
- Thesis: **“Implementation of Optical Proximity Correction for Deep Sub-Micron IC Manufacturing”**. (full grade)
 - **Abstract:** In my final thesis, a method for correcting pattern transfer effects was implemented which is on the basis of model-based Optical Proximity Correction (OPC). The solution is based on fragmenting edges of layout polygons to smaller pieces and moving these fragments to reach an optimal design. This project was implemented under the title of "atlasOPC", and was appended to "ATLAS", a Linux-based physical design tool implemented in CAD Laboratory of Computer Engineering Department, under the supervision of Dr. Saheb Zamani.
- Advanced Courses:
 - VLSI Systems Design (17.4/20)
 - Advanced topics in Hardware Engineering (19.63/20)
 - Advanced Logic Circuits (17/20)
 - Computer Interface Design (17/20)
 - Computer Networks (17/20)
 - Signals and Systems (19.25/20)
 - Information Technology Engineering (19/20)

Honors and Awards

- Graduation as the first rank student in MSc program, CEIT Dept., Amirkabir Univ. of Tech., 2008.
- Awarded with admission to MSc program at CEIT Dept. of Amirkabir Univ. of Tech. without taking MSc. national entrance examination, 2006.
- Graduation as the first rank student in Computer Hardware Engineering BSc program, CEIT Dept., Amirkabir Univ. of Tech., 2006.
- Ranked 298th among over 400,000 competitors in Iran national university entrance exam, 2002.
- Honored as dean student in National Organization for Development of Exceptional Talents (NODET) High school, Karaj, Iran, 2001.
- Reached first level of National Computer Olympiad, 2001.

Publications

Theses:

- **“On the Security of Multimedia Encryption and Authentication Schemes,”** MSc Thesis, Dept. of Elect. and Comp. Eng., North Dakota State Univ., Fargo, ND, 2010.
- **“Hardware Software Co-design Considering Reconfigurability and its Application in Implementing EFM,”** MSc Thesis, Dept. of Comp. Eng., Amirkabir Univ. of Tech., Tehran, Iran, Sep. 2008.
- **“Implementation of Optical Proximity Correction for Deep Sub-micron IC Manufacturing,”** BSc Thesis, Dept. of Comp. Eng., Amirkabir Univ. of Tech., Tehran, Iran, Aug. 2006.

Journal papers:

- Raj S. Katti, Sudarshan S. Srinivasan, Aida Vosoughi, **“On the Security of Randomized Arithmetic Codes against Ciphertext-only Attacks,”** *IEEE Trans. on Information Forensics and Security*. vol. 6, issue 1, pp. 19-27, March 2011.
- Raj S. Katti, Aida Vosoughi, **“On the Security of Arithmetic Coding with Key-based Interval Splitting,”** submitted for publication in *IEEE Trans. on Information Forensics and Security*.

Conference papers:

- Aida Vosoughi, Farinaz Koushanfar, Marten VanDijk, and Ari Juels, “**Doing the Limbo: Ultra-Low-Power Cryptography for Kill Switches**,” submitted to the *workshop on Cryptographic Hardware and Embedded Systems (CHES)* 2011.
- Aida Vosoughi, Raj S. Katti, “**Fast Message Authentication Code for Multiple Messages with Provable Security**,” *53rd IEEE Global Communications Conference (GLOBECOM)*, Miami, FL, USA, Dec. 2010.
- A. Vosoughi, K. Bilal, S. U. Khan, N. Min-Allah, J. Li, N. Ghani, P. Bouvry, and S. Madani, “**A Multidimensional Robust Greedy Algorithm for Resource Path Finding in Large-Scale Distributed Networks**,” in *7th ACM/IEEE International Conference on Frontiers of Information Technology (FIT)*, Islamabad, Pakistan, Dec. 2010.
- Aida Vosoughi, Mehdi Sedighi, “**A Reconfigurable Hybrid Hardware/Software Architecture for EFM/Ethernet**,” *International Symposium on Telecommunications (IST)*, Tehran, Iran, Aug. 2008.
- Aida Vosoughi, Mehdi Saeedi, Mehdi Sedighi, Morteza Saheb Zamani, “**Hardware Implementation of TC-Encapsulation in the EFM Standard**,” *13th Computer Society of Iran Computer Conference (CSICC)*, Kish Island, Iran, Mar. 2008.

Academic Activities**Selected Academic Projects:**

- **Advanced Programming Course Project** (Jul. 2003 – Sep. 2003)
A strategic game with graphical interface was developed in C++ (team project).
- **Information Retrieval** (Jun. 2004 – Sep. 2004)
A search engine was developed in C++.
- **Computer Architecture Lab. Project** (Apr. 2005 – Jun 2005)
A Simple processor was implemented and tested using MAXPLUSII (team project).
- **VLSI Design Project** (Jun. 2005 – Jul. 2005)
A low power, four input multiplexer layout was designed using LEdit8.0 software (team project).
- **Route Finder Mini Robot** (May 2006 – Jul. 2006)
A small robot with the capability of finding its way through a maze and moving toward its destination was designed and made using ATmega16 microcontroller and step motors (team project).
- **Steiner Tree Problem** (Mar. 2007 – Apr. 2007)
Heuristic algorithms for Minimum Rectilinear Steiner Tree problem were implemented in C++.
- **Hardware Modeling Project** (Jul. 2007 – Sep. 2007)
A TC 64/65-Octet Encapsulation Module for IEEE802.3ah (EFM Standard) was designed and modeled in VHDL. The model was then synthesized using QuartusII synthesis tool. It led to a conference paper.
- **Using ACL2 Theorem Proving to Verify a Pipelined Processor** (Sep. 2009 – Dec. 2009)
A three-stage pipelined processor was modeled at micro-architecture and instruction set levels and verified using ACL2 language and theorem proving system.

Major Previous Research:

- **OPC for Deep Sub-micron IC manufacturing** (Apr. 2006 – Sep. 2006)
Working on Resolution Enhancement Techniques (RETs) in IC manufacturing process, Mask Engineering, and especially Optical Proximity Correction (OPC) led to an implementation of OPC in C++. This work is published as my BSc thesis.
- **Multi Threshold CMOS** (Feb. 2007 – Mar. 2007)
Working on MTCMOS, and reviewing several papers on it led to a lecture review document and a presentation.
- **Integer Linear Programming** (Apr. 2007 – Jun. 2007)
It consisted of researching on how to use ILP in clustering graphs for VLSI Design Algorithms.
- **Hardware Software Co-synthesis** (Oct. 2007 – Dec. 2007)
Researching on HW/SW co-synthesis and reviewing several papers on it led to a lecture review document and a presentation.
- **Ethernet in the First Mile** (Oct. 2006 – Mar. 2009)
EFM standard was studied thoroughly and an Ethernet/EFM reconfigurable architecture was proposed. It led to two research papers and a presentation.
- **Hardware Software Partitioning** (Jul. 2007 – Mar. 2009)

We researched on HW/SW co-design methodologies, and we proposed a HW/SW partitioning approach in which reconfigurability is a concern. It led to my MSc thesis and a research paper.

- **Robust Resource Allocation in Distributed Networks** (Sep. 2009 – May. 2010)
A robust greedy algorithm for path allocation in distributed networks is proposed and implemented.
- **Multimedia Encryption and Compression** (Sep. 2009 – Dec 2010)
The vulnerabilities of the existing multimedia compression/encryption methods are analyzed and new solutions for secure compression of multimedia contents are explored.
- **Quantum Dot Cellular Automata Design Using Null Convention Logic** (Nov. 2009 – May 2010)
Efficient QCA threshold gates are designed for implementing QCA asynchronous registers.
- **Power consumption characterization of the final hash function candidates for SHA-3 competition** (Sep. 2010 – Apr. 2011)
Five final SHA-3 hash algorithms were implemented for low power applications in ASIC and they were compared in terms of energy per cycle metric.

Qualifications

Hardware Description Languages

- VHDL, Familiar with Verilog and systemC

Tools

- Practical Experience with:
 - Simulation tools: Synopsys VCS and PrimeTime PX, ModelSim, MaxPlusII, and Spice
 - Synthesis tools: Synopsys Design Compiler, Leonardo Spectrum, QuartusII, and Xilinx ISE
 - Design tools: Active HDL, and FPGA Advantage
 - Layout editor: LEdit
 - Board level layout design tools: Orcad, and Protel
 - Development Environment: CodeVisionAVR, MPLAB, Eclipse, Microsoft Visual Studio, Adobe Dreamweaver

Hardware Interfaces

- Familiar with USB, FireWire, I2C, SPI, ISA, SCSI, and PCI buses.

Microcontrollers

- ATmega16 microcontroller
- PIC microcontroller

Programming

- C, C++, MATLAB, Pascal, Visual Basic, SQL, ACL2

Web Developing

- PHP, HTML, Familiar with XML

English Language

- Diploma in English Language Proficiency from Iranian Academic Center for Education, Culture, & Research, Tehran, Iran, 2003.
- iBT TOEFL score (October 2007): 112/120
 - Reading: 29/30, Listening: 29/30, Speaking: 27/30, Writing: 27/30
- GRE General Test Scores (October 2007):
 - Verbal: 410/800, Quantitative: 800/800, Analytical Writing: 4.0/6.0

Teaching Experience

Circuit Analysis (I) TA, ECE Dept., NDSU, Fall 2010.

Embedded Systems TA, ECE Dept., NDSU, Fall 2009 and Spring 2010.

Digital Electronics TA, CEIT Dept., Amirkabir Univ. of Tech., Fall 2008.

Computer Interface Design TA, CEIT Dept., Amirkabir Univ. of Tech., Spring 2007.

Work Experience

Research Assistant

Dept. of Electrical and Computer Engineering, NDSU, Fargo, ND (Sep. 2009-present)

Dept. of Computer Engineering and IT, Amirkabir University of Technology, Tehran, Iran (Sep. 2006-Mar. 2009)

Part-time Hardware Designer/Tester

Data Processing Co., Tehran, Iran (Jul. 2005- Dec. 2005)

Part-time VB and SQL Programmer

Arman Samaneh Novin Co., Tehran, Iran (Sep. 2003-Jul. 2004)

Part-time Web Developer

Amirkabir University of Technology, Tehran, Iran (Jun. 2003-Sep.2003)

Memberships

IEEE: Computer Society, Circuits and Systems Society, Reliability Society, Signal Processing Society

IEEE Women in Engineering

ACM: SIGDA, SIGMETRICS, SIGSAC, SIGBED

References

Available Upon Request.

To see the most recent version of this document please visit: <http://www.vosoughi.info/resume.php>