

CURRICULUM VITAE
December 2010

Full name

Babak Zakeri

Date & Place of Birth

Dec 6th, 1981, Sheffield, UK

Contact Information:

2319 McNeill Ave, Victoria, BC, Canada
Postal Code: V8S 2Z1
Phone: +1-250-885-7509
Email address: babak.zakeri@gmail.com

Currently involved:

MASc in Electrical Engineering in ECE department of University of Victoria, Victoria, BC, Canada,
Started in Sep 2009.
ReCoEng Lab, University of Victoria: Laboratory of Reconfigurable Computing Engineering
Supervisor: Dr. Mihai Sima

Education:

MSc in Digital-Electronics from Sharif University of Technology, Tehran, Iran, June 2005 to February 2008
Project: *Differential Power Analysis Attack Resistant Implementation of AES Algorithm on FPGA using Masking Methods*
Supervisor: Dr. M. Salmasizadeh

BSc in Electrical Engineering-Electronics from University of Tehran, Tehran, Iran, June 2000 to June 2005
Project: *Testing, debugging and implementation of two CPU cores, designing of a MPEG video decoder and implementation and testing the code as a golden model on Virtex II and Virtex IV FPGAs.*
Supervisor: Dr. M. Movahedin

Summary of Experience:

- Very well experienced in Xilinx and Altera FPGA's simulation, implementation and emulation.
- Strong theoretical and practical experience in HDL languages: VHDL and Verilog.
- Very well experienced on hardware design tools, packages and architectures:
 - o FPGA simulators and synthesis tools: Modelsim, Synplify, Leonardo Spectrum and ...
 - o Xilinx ISE suite's various design tools: XST, ISim, XPower, Core Gen, and ...
 - o Altera Quartus software
- Very well experienced (and already involved in) Side-Channel Attacks regarding FPGA implementation of encryption algorithms (Developing attacks, Setting up measurement and ...).
- Good experience in processor design issues, HDL coding, software compilation, design process, design partitioning, design testing and ...
- Good experience with Sparc Architecture and assembly.
- Good experience on software and hardware implementations of MPEG algorithm on FPGA.

- Experience on different FPGA architecture issues: Manual P&R, Adder dedicated and optimized blocks, Dynamic Partial Reconfiguration, Improvement of compilers
- Experience on implementation of Fuzzy-Nero controllers on FPGAs.
- Experience of working with the tools, standards, architectures and languages:
 - o Analog Circuit Simulators: PSPICE , HSPICE
 - o Programming languages: Visual C++, C# .NET
- Experience of working on Micro-controllers and Micro-processors.
- Very strong algebraic background in finite group theory, field theory, vector spaces and

Research Interests:

Side Channel Attacks regards FPGA implementations of encryption algorithms.
 FPGA architecture, Dynamic Partial Reconfiguration, FPGA compilers
 Optimized implementation of MPEG and encryption standards on FPGAs.

Work Experience:

- Parseh semiconductor, March 2005 to April 2006

Testing, debugging and implementation of two CPU cores. Designing of an MPEG video decoder and implementation and testing the code as a golden model on Virtex II and Virtex IV FPGAs.

- o Simulation and debugging of two CPU cores
- o Preparing a compatible MPEG video decoder C code for Sparc architecture
- o Implementation, designing and debugging of external peripherals for the CPU cores.
- o Emulation of the MPEG decoder as a golden model for CPUs.

- Micro-Controller lab of Sharif University of Technology, September 2006 till December 2006
Lab TA

- Electronics Research Centre, Sharif University of Technology, Dec. 2006 to March. 2008

Researching on AES algorithm, attacks against it and improving the resistance of the implementation against attacks.
 Implementation and optimization of a secure AES encryption algorithm in a compact way on Xilinx FPGA series

- Alborz Sanat Kavir Co., July 2007 till July 2008

Digital designer of a high voltage inverter design project for traction motor control for Tehran's underground railway.

- o HDL code development on Altera FPGA series.

- SAMA Co., Dec. 2007 till May 2008

Digital designer of a digital TV design project.

- o HDL code development on Actel anti-fuse FPGA series.

- University of Victoria, October 2009 till December 2009
TA (Introduction to Computer Architecture)

- University of Victoria, February 2010 till April 2010
TA (Electronic Circuits)

Published Papers:

B. Zakeri, M. Salmasizadeh, A. Moradi, M. Tabandeh, and M.T. Manzuri Shalmani. Compact and Secure Design of Masked AES S-box. In Sihan Qing, Hideki Imai and Guilin Wang, editors. *International Conference on Information and Communications Security – ICICS 2007, 9th International Conference, Sofitel Zhengzhou, Zhengzhou, China, 12-15, Dec 2007, Proceedings*, volume 4861 of Lecture Notes in Computer Science, pages 216-229. Springer, 2007.

Presentations:

- FPGA and VHDL workshop, two 24 hours workshops in IEEE branch of University of Tehran, summer 2005 “FPGAs and HDL codes”.
- Sharif University of Technology, Fall 2005 “PCI Express implementation using Hardware Description languages”.
- Fall 2005 “PA-RISC architecture”, Sharif University of Technology.
- Winter 2005 “Things to be concerned in developing HDL codes to be synthesized”, Sharif University of Technology, Fall 2006
- Fall 2009, “Implementation of Carry-Save adders on Altera Stratix FPGAs”, University of Victoria
- Spring 2010, “Implementing parts of MPEG encoder standard on FPGA”, University of Victoria
- Summer 2010, “Motion Estimation: Developing optimized pure software solution, software-hardware solutions and comparing their performances”.

Project (Thesis) Currently Involved:

Study the Vulnerability of a specific Stream-Cipher Implementation regarding Side Channel Attacks.

Nationality

I am Persian (Iranian) from Iranian parents who are from the Turkish part of Iran (Azarbayjan) which makes me capable of understanding Azari other than my native language Farsi :].
I'm also a British Citizen since I was born and lived in UK for a few years.

Interests and Hobbies:

Thinking, Work, Music, Movies, Hanging out with Friends , Analytical and Archetypal Psychology, DotA of Warcraft, and pretty soon painting maybe :]