SHASHI PRASHANTH KARANAM

skaranam@gmu.edu 9409 Lee HWY, Fairfax, Virginia-22031 (703) 342-8992

OBJECTIVE

To be a part of an energetic team in the field of Computer Engineering with special interest in Secure Embedded systems, Digital System Design and Verification, seeking a Full-time position for self and organization growth.

EDUCATION

M.S., Computer Engineering, expected Graduation May 2009 GPA: 3.6
George Mason University, Fairfax, VA
Thesis: Design and Implementation of True random number generator on an FPGA.

B.S., Electronics and Communications Engineering, May 2006 Grade: First Class
Kamala Institute of Technology and Sciences, Huzurabad, India

WORK EXPERIENCE

Computer Engineer, Microwave Technologies Inc., Burke, VA June 2008- August 2008

- Designed and Optimized a Pulse analyzer to measure the Radar emitter parameters such as frequency, pulse width, pulse amplitude, time of arrival and pulse repetition interval(PRI) using VHDL and Verilog.
- Accomplished on-chip debugging using ChipScope Pro to view internal signals. The design is targeted onto Virtex 5 FPGA and finds applications in defense emitter environments.

Hardware Support Engineer, Wireless Ventures, McLean, VA January 2008-May 2008

- Implemented a Hardware Gaussian Noise generator based on Box-Muller method in VHDL targeting Altera Stratix II FPGA family. Project also involved piecewise polynomial approximation and determination of polynomial coefficients using Octave.
- Testbench in VHDL to simulate the Noise generator, Octave scripts to cross verify the simulated results and to plot the generated noise are written. Obtained improved results in terms of area and memory utilization to all previously published results.
- Testbench to interface and debug the memory and data register access commands of Sidense SiPROM OTP through JTAG is written in Verilog.

Graduate Student Researcher, Cryptographic Engineering Research Group, Fairfax, VA May 2007-Present

- Research interests include true random number generators for cryptographic applications, also concerns hardware implementations in the areas of efficient cryptographic algorithms and computer arithmetic's.

Teaching Assistant, George Mason University, Fairfax, VA Spring 2007, Fall 2007 and Fall 2008

- Taught the following courses and labs: Introduction to VHDL (Graduate), Digital system design, Digital electronics and logic design lab.
- Responsibilities included teaching at hands on sessions, recitations and labs, preparing midterms and final exams for labs and giving out final grades, also involved weekly homework and lab reports grading.

Undergraduate Student Intern, Indian Space Research Organization, India Decemeber 2005-March 2006

- Simulated an algorithm for measuring gain of the satellite signal and developed a graphical window panel that captures real time plot and saves data as offline content using CVI.
- The project makes a real time application for analysis of quantity and quality of signal, detection of data loss and to study the behavior of satellites.

PUBLICATIONS

- D. Hwang, M. Chaney, S. Karanam, N. Ton, and K. Gaj**,** "Comparison of FPGA-Targeted Hardware Implementations of eSTREAM Stream Cipher Candidates," Proc. State of The Art of Stream Ciphers Workshop (SASC 2008),pp. 151-162 Feb 2008.

- B. Zhou, *S. Karanam, *S. Shah, M. Chaney, N. Ton, D. Hwang and K.Gaj, "eSTREAM candidates vs. AES: Comparative study of Hardware performance in Resource-Restricted Environments" poster presentation in 10th annual workshop on Cryptographic Hardware and Embedded systems (CHES 2008), Aug 10-13, 2008, Washington DC, USA. (*Presenters)

TECHNICAL SKILLS

Programming Languages : VHDL, Verilog, MATLAB, Octave, TCL, RC Toolbox, C, CVI, Assembly, PSpice
Tools : Xlinx ISE, Xilinx EDK, Synplicity Synplify Pro, Altera Quartus II, Active HDL, ModelSim, PrimeTime, Formality, Design Compiler, Chipscope Pro, Simulink, Simplescalar, DSPlogic RC Toolbox, CrypTool, Kryptos
Programmable Hardware : FPGA
Applications : LaTeX, HTML, Gimp, Jfig, Microsoft Visio, Openoffice, MS Office
Operating Systems : Mac OS X , GNU/Linux, Windows

ADDITIONAL SELECTED EXPERIENCE

- Excellent Programming skills in VHDL gained by implementing projects like True random number generators, hardware gaussian noise generator, eSTREAM Phase 2 ciphers Phelix & Trivium, pulse analyzer, high radix sequential multiplier, fast adders and by optimizing eSTREAM Phase 3 profile 2 candidates targeting onto FPGA devices and Semi Custom ASIC's.
- Experienced in debugging and creating testbenches to simulate digital circuits using VHDL and Verilog.
- Proficient at floorplanning and programming FPGA, completed as part of implementing various true random number generators on Virtex 2 FPGA.
- Created a hardware system with a Co-processor to store generated random bits into external memory using Xilinx EDK (Embedded Development Kit) tools.
- Skilled in Matlab/Octave programming, achieved by writing scripts to open and digitize captured analog output of TRNG, for post-processing of TRNG output, to perform piecewise polynomial approximation and determine polynomial coefficients of logarithmic, exponential and square root functions.
- Experienced in using Synopsys Design Compiler and Primetime for ASIC Chip synthesis, and design verification using Formality and TCL.
- Extensively used CAD tools and great hands on experience with oscilloscopes, logic analyzers and other laboratory modules.
- Good programming skills in C and high level languages like RC Toolbox and CVI.
- Practical knowledge of transistor level operation of circuits. Fabricated an N-MOSFET and transistor characteristics were observed.

OTHER INFORMATION

- Member, International Association for Cryptologic Research, August 2008-Present.
- Member, Cryptographic Engineering Research Group, George Mason University, May 2007-Present.

References: Available upon request