Susheel C. Vadlamudi
3900 Moorpark Ave, Apt #100,
San Jose, CA 95117.

Phone: 732-789-0012
svadlamu@gmu.edu
http://www.cryptography.gmu.edu/team/svadlamu.php

Education

- **Master of Science in Computer Engineering** GPA - 3.54
  George Mason University, Fairfax, VA *Aug. 2009 - May 2012*
  - Course Work: Digital System Design with VHDL, Microprocessors, MOS Electronic Devices, VLSI Test Concepts, Cryptography and Network Security, Digital Integrated Circuits, Computer Network Architectures and Protocols, VLSI design for ASICs.
  - Thesis: Compact Implementations and Benchmarking of Two SHA-3 Finalists BLAKE and JH on FPGAs
- **Bachelor of Science in Electronics and Communication Engineering** GPA - 3.31
  Vignan Engineering College, Guntur, IND *Aug. 2005 - Aug. 2009*

Technical Skills

Programming Languages: C, Assembly level programming, VHDL, Verilog, SystemVerilog, Perl.

Operating Systems: Windows XP/Vista/7, Mac OS, Linux.

Tools: Xilinx ISE, Altera Quartus II, Synplify Pro, ModelSim, MultiSim, Matlab, Cadence Pspice, Microwind, Wireshark, TetraMax, Design Compiler, Prime Time, Formality, IC Compiler.

Other Softwares: Microsoft Office, Open Office, Microsoft Visio, LaTeX.

Miscellaneous: Excellent troubleshooting and debugging skills and also knowledge on Communication protocols (TCP/IP, FTP)

Work Experience

- **Cryptographic Engineering Research Group** George Mason Univ., VA
  Graduate Research Student *Jan. 2010 - Present*
  - Designed and implemented compact architectures of Two SHA-3 Finalists BLAKE and JH for Spartan-3 FPGAs. The different implementations include both distributed RAM version which uses pure logic and block RAM version which uses embedded elements for storage.
  - Benchmarking of all the implementations using hardware tool ATHENa for achieving maximum throughput/area ratio.
  - Other research interests include excessive study of architectural features of FPGA, Low-Area designing and True Random Number Generators.
- **George Mason University** Fairfax, VA
  Graduate Teaching Assistant(Digital System Design, Basic Electronics Lab & Microprocessors) *Aug. 2010 - May 2011*
  - Assist students in getting familiar with lab equipment, information about basic circuits and MSP430 debugging using IAR workbench.
  - Tutor students on weekly basis to help in ongoing course/lab work and assignments.
  - Responsible for grading lab assignments, course assignments and exams.

Projects Undertaken

- **ASIC Design - ASIC Implementation of Compact BLAKE-32**
  - Compact architecture of BLAKE-32 is optimized and implemented on ASICs using 90nm technology.
  - Implementation includes synthesis of the design, area optimization, timing analysis and floorplanning using Synopsys ASIC tools like Design Vision, PrimeTime, IC Compiler.
  - Test patters are generated and functionality is verified using TetraMax and VCS.
- **Digital Design with VHDL - Implementations of BLAKE**
  - Designed and simulated both 32-bit & 64-bit variants of BLAKE for FPGAs.
  - Designed two different architectures of both BLAKE-32 & BLAKE-64, which includes folded and unrolled architectures optimized for better throughput/area ratio.
  - Simulations are performed at different levels to achieve post place route functionality using Xilinx Design Suite and Modelsim SE.
- **Cryptography and Network Security - Low Area Implementations of BLAKE-32**
  - Designed and implemented area constraint designs of BLAKE-32 on Spartan3 FPGA using VHDL language.
  - Developed low area architectures of BLAKE-32, which uses minimal logic resources and an embedded storage element. All the designs were simulated and optimized for better throughput/area ratio.

  - The designs are implemented with Xilinx tools using VHDL and functionality is verified at block and unit level using simulation tools like Modelsim and Isim.

- **Microprocessors - Implementation of MSP430**
  - Implemented MSP430, a 16-bit low-power micro controller using Verilog open source code.
  - Analyzing the computer architecture of MSP430 and verifying the implementation by debugging with an assembly level program.

- **Implementation of Serpent Cipher Algorithm**
  - Designed and implemented Serpent Cipher Algorithm as a part of Final year project.
  - Responsible for implementation of key generation unit which produces 128/256-bit key for encryption and decryption.
  - VHDL language is used to develop the architecture of algorithm and implemented using Xilinx tools along with functional verification using Modelsim.

Publications

- J.-P. Kaps, P. Yalla, K.K. Surapathi, B. Habib, S. Vadlamudi, S. Gurung, and J. Pham, **Lightweight implementations of SHA-3 candidates on FPGAs**, Progress in Cryptology INDOCRYPT 2011, Lecture Notes in Computer Science (LNCS), volume 7107, Springer Berlin / Heidelberg, pages 270289, Dec, 2011.