

## **KISHORE KUMAR SURAPATHI**

9411 Lee Highway, Apt# 1002,  
Fairfax,  
VA 22031

kishorekumar183@gmail.com  
ksurapat@gmu.edu  
571-308-4844

---

### **OBJECTIVE**

Computer Engineering graduate seeking an entry level position in a challenging environment that would utilize and enhance my technical skills and broaden my knowledge in the field of engineering.

### **EDUCATION**

**M.S., Computer Engineering, George Mason University, Fairfax, VA** Dec 2011

**Thesis:** Lightweight Implementations of SHA-3 hash functions on FPGAs

**GPA: 3.71**

**B.S., Electronics and Communications Engineering,** May 2009

Gayatri Vidhya Parishad College of Engineering, Vizag, India.

**GPA: 3.70**

### **WORK EXPERIENCE**

**Graduate Researcher,** Jan 2010-Dec 2011

**Cryptographic Engineering Research Group, George Mason University.**

Research interests include

- Cryptographic hardware implementations
- Hardware implementations of computer arithmetic
- Power measurements on FPGAs
- Low Power Implementations on ASICs

**Graduate Teaching Assistant,** Jan 2010-Dec 2011

**Electrical and Computer Engineering Department, George Mason University.**

- Courses: Digital System Design, Electric Circuit Analysis, Digital Electronics.
- Responsibilities include: conducting lab sessions, grading homework and exams and prepare question papers for Undergraduate class. Help students with hands-on lab session on projects.

### **PROJECTS**

- **Low area architectures of algorithms contesting in SHA-3 competition.**  
This project is supported by NIST which started the competition for developing new cryptographic hash algorithm SHA-3.  
Designed Compact Hardware architectures for four SHA-3 algorithms on FPGAs.
- **ASIC implementation of AES**  
Implemented AES(Advanced Encryption Algorithm) on ASICs using Synopsys Tools.
- **Verification of Designs using Assertions and Simulation tools.**  
Written test benches to test the digital hardware extensively.
- **Implementation of Adders and Multipliers on Xilinx and Altera FPGAs.**  
Implemented various adders like Carry save, Carry Look ahead and Hybrid adders.  
Implemented combinational, serial Multipliers and modular multipliers on both FPGAs.
- **Power Measurements of the SHA 3 Hash functions on an FPGA.**  
In this work, designs of SHA-3 final round functions implemented targeting low area were considered and their power is measured using an efficient methodology on an FPGA board.

- **Design of Full Adder using MicroWind.**  
Designed Full adder Schematic and Layout using Microwind and Post Layout simulations using Pspice.
- **Design of an LED display system.**  
Display of data on the LED display board with scrolling effect where data is sent from the PC to the controller (89C51ED2) via serial communication following RS232 protocol.

## TECHNICAL SKILLS

<b>Programmable Hardware</b>	Xilinx FPGA and Altera FPGA
<b>Assembly Programming</b>	8086 family, 89C51 , Msp430
<b>Languages</b>	VHDL, Verilog, C, C++, Perl
<b>Tools</b>	Xilinx ISE, ModelSim, Altera Quartus II, Active HDL, Synopsys Synplify Pro ,Pspice, Microwind , Synopsis tools for ASICs (Design Vision, Formality, Primetime, Astro)
<b>Applications</b>	Matlab , Microsoft Visio, Open office, MS Office, LaTeX
<b>Operating Systems</b>	Windows Xp, Vista, Linux

## AWARDS

- Best project award for the project "*Low-Area Implementations of Groestl, Luffa, BMW, and SHAvite-3*", George Mason University, Fall 2010.
- Best project award for the project "*LED display System*" by the department of ECE, GVP College Of Engineering, India, May 2009.

## RELEVANT COURSE WORK

**Graduate:** Microprocessors, Digital System Design w/ VHDL , Computer Arithmetic , Digital Integrated Circuits-CMOS technology, Cryptography and Network security, Advanced applied cryptography, VLSI Design for ASICs .

**Under-Graduate:** Electric Circuit Theory, Electronic Circuits & Devices, Digital Design, Signals & Systems, Microcontrollers, Digital Signal Processing, VLSI Design, Microwave engineering, Operational Amplifiers.

## 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), Springer, Dec, 2011