

Bilal Habib-PhD

C: 571-224-5978, Email: bhabib@gmu.edu , Web: <http://mason.gmu.edu/~bhabib/>

Address: 1105 E. Ponderosa Pkwy, Apt 227, Flagstaff, AZ 86001. USA.

Goal: Looking for an interesting position in the areas of RTL design, Hardware Security, FPGA design, Firmware design, Low power design, Embedded Systems and Digital Logic Design.

Education

- PhD Computer Engineering, 2016, George Mason University, Fairfax, VA, USA.
- MSc Computer Engineering, 2010, George Washington University, Washington, D.C, USA.
- Bachelor of Computer Engineering, 2005, University of Engineering & Tech, Pakistan.

Selected Projects

- Firmware development for Automated Data Extraction, Analysis and developing Physical Unclonable Functions (PUF) and TRNG from CBRAM and ReRAM Nano devices. Platform used: Smartfusion SoC. http://www.hostsymposium.org/hwdemo/HOST_2017_hwdemo_6.pdf
- Design, Implementation and Analysis of Multi-core network on chip. Platform used: Virtex-5 FPGA. Performance analyses of different topologies were carried out.
- Characterization of FPGA devices for Physical Unclonable Functions (PUF). Design, development and testing of PUF circuits were performed. PUF quality metrics were analyzed under different voltage and temperature. Devices used: Spartan-3 and Spartan-6.
- Using Hardware-Software co-design concept, PUF circuits were designed and tested on System On Chip devices. Platform used Zynq.
- Designing low power Crypto (SHA-3) cores for FPGA devices. New Hash functions for SHA-3 competition were developed for NIST competition. Primary Target: Spartan-3
- Designing high speed Crypto (SHA-3) cores for FPGA devices. Primary Target: Spartan-3
- 32-bit MIPS single cycle processor implementation. Platform used: Basys-2
- Implementation of on-chip bus protocol (AXi-Lite)
- IP integration: Integration of hardware primitives to the ARM core on SoC devices.
- IP testing and simulation.
- Python projects for data analysis : <https://cryptography.gmu.edu/puf/>

Employment History

- **Post Doctoral Scholar** at the School of Informatics, Computing and Cyber Systems at Northern Arizona University at Flagstaff, AZ, USA. Aug 16, 2016 to date.
 - Firmware design for Developing Cyber Security Protocols.
 - Implementations of Hardware primitives using Nano-materials.

- Generating True Random Numbers using hardware primitives
- Analyzing Random Numbers using NIST Suite
- Design and implementation of authentication and identification protocols for internet security.
- Analyzing Nano devices for their respective use in developing PUF and/or TRNG
- Data extraction and error correction of CBRAM memory arrays using Smartfusion FPGA.
- Analyzing sensors for their use in IoT security
- Software development in C.
- **Research Assistant** in the Cryptographic Engineering Research Group, Sep. 2010-Jun 2016.
Job responsibilities include,
 - Design, Development and Implementation of FPGA cores for Xilinx devices using Vivado, SDK and chipscope.
 - Cryptographic Hardware design on FPGA
 - Efficient implementations of Low area and high throughput hardware designs for Xilinx devices.
 - Reliable and efficient code for simulation and synthesis, for Xilinx and Altera FPGAs.
 - FPGA design and validation in VHDL using Modelsim.
 - VHDL Simulations with ModelSim and Isim.
 - Synthesis, Placement and Routing using Vivado, ISE and Altera Quartus.
 - Post Place and Routing Timing simulations
 - Embedded Systems: MicroBlaze, Zynq based SoC design .
 - Python and Perl based scripting and data analysis.
 - Inter-processor communications: MPI (Message Passing Interface) based Inter processor communication protocols and implementation on hardware devices (FPGAs).
 - Design, Development, implementation and testing of Hardware primitives.
 - Hardware security.
 - Physical Unclonable Functions for FPGAs.
 - MSP430 micro-controllers protocols implemented: SPI, I2C, interfacing of sensors and displays. Serial and parallel interfaces.
 - Interfacing LCD with uC. TFT-LCD using SPI protocol.
 - Development, Prototyping and Testing of FPGA designs.
 - Algorithms development in C and C++.

- **Design Engineer** (Embedded Systems) at AND OR Logic Pvt Ltd, Islamabad
(<http://www.andorlogic.com/>) Jan. 2005 to Dec. 2007.
 - Software development C
 - Board level testing, debugging and power analysis.
 - Securing E1 and D1 streams with cryptographic algorithms for Radio Communication.
 - Design and Development of Tamper Proof Digital Energy Meter.
 - Behavioral and RTL Design for Xilinx FPGAs.
 - Simulation and Optimization of Verilog HDL.
 - Designing Firmware for PIC and ARM Microcontrollers.
 - Circuit Design and Testing.

Selected Research Publications

- B. Cambou, R. Chipana and B. Habib. “**PUF with dissolvable conductive paths**”. Patent filed (US Patent Application No.: 62/541,005. Filing Date: August 3, 2017).
- B. Cambou, R. Chipana and B. Habib. “**Securing Physically Unclonable Functions with Additional Random Ternary States**”. Patent filed (US Patent Application No.: 62/480,151. Filing date: March 31, 2017)
- B. Habib and K. Gaj. “**A Comprehensive Set of Schemes for PUF Response Generation,**” Journal of Microprocessors and Microsystems, Vol 51 (2017), pp-239-251.
- B. Habib, J.-P. Kaps and K. Gaj . “**Implementation of Efficient SR-Latch PUF on FPGA and SoC devices,**” Journal of Microprocessors and Microsystems, 2017.
- B. Habib and K. Gaj . “**A Comprehensive Set of Schemes for PUF Response Generation,**” 12th International Symposium on Applied Reconfigurable Computing, Rio de Janeiro, Brazil, 22-24 March, 2016.
- B.Habib, J.-P. Kaps and K.Gaj . “**Efficient SR-Latch PUF,**” 11th International Symposium on Applied Reconfigurable Computing, 2015, Bochum, Germany, April 15-17. 2015.
- B.Habib, K.Gaj and J.-P. Kaps . “**FPGA PUF Based on Programmable LUT Delays,**” Proc. 16th EUROMICRO Conference on Digital System Design, 2013, Santander, Spain, Sep. 2013.
- J.-P. Kaps, P. Yalla, K.K. Surapathi, B. Habib, S. Vadlamudi, and S. Gurung, “**Lightweight Implementations of SHA-3 Finalists on FPGAs**”, Proc. 3rd SHA-3 Candidate Conf., Washington, D.C., Mar. 2012.
- Bilal Habib, Ahmed Anber and Sultan Daud Khan. “**The Effect of Multi-core Communication Architecture on System Performance** ” (Accepted), Sixth International Symposium on Embedded Multicore SoCs, 20-22 September 2012, Aizu-Wakamatsu, Fukushima, Japan.

- 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), vol. 7107, Springer, Dec. 2011.
Google Scholar Citations: [Google Scholar](#)

Relevant Courses

- Digital System Design with VHDL
- VLSI Design for ASICs
- Microprocessors
- Data structure
- Cryptography and Computer Network Security
- Cryptographic Engineering
- Computer Arithmetic
- VLSI Test Concepts
- Advanced Applied Cryptography
- High Performance Computing
- Theory and Applications of Data Mining

Achievements

- Dissertation Completion Grant from the ‘Office of Provost’. George Mason University.
- Ministry of Science & Technology Merit Scholarship for four consecutive years of graduate engineering studies. Sponsor www.hec.gov.pk
- Nationwide selection and then participation in International Congress, Sydney, Australia Sep. 2004, based on my essay and presentation. Sponsor www.worldenergy.org.
- Merit Scholarships in College and School.

Software Skills

VHDL, C, C++, Verilog, Assembly, Python, Perl, Tcl scripts , Java, MPI, UPC.

Tools

Source and Measurement Unit (SMU), Logic Analyzer, Oscilloscope, Vivado, Xilinx ISE, Xilinx Plan Ahead, ModelSim, Altera Quartus , Matlab, MPLAB, PSPICE, Weka, Arena, audacity, Code Composer, IAR workbench, Libero SOC, MicroSemi SoftConsole.

Embedded Platforms

MicroBlaze, Zynq (SoC).

Office: Microsoft Excel, Microsoft PowerPoint, Microsoft Word.

Academic Service

Reviewer Conference: CHES-(2012, 13, 14, 15), DSD-(2012, 2014), ReConFIG-(2012, 13, 15).

Reference

Marcin Rogawski (408) 893-0859 Email: marcin@cadence.com [Principal Software Engineer at Cadence]

Umar Shareef (703) 622-4666 Email: malik.umar.sharif@gmail.com [Ixia]

Kris Gaj (703) 993-1575 Email: kgaj@gmu.edu [Associate Professor, George Mason University]