Sharath Pendyala

Raleigh, NC, USA

spendya@ncsu.edu
sharathpawan@gmail.com
linkedin.com/in/sharathpawanp
https://sharathpend.github.io

FPGA AND HARDWARE SECURITY ENGINEER

FPGA and RTL Design Engineer with over a decade of industry and research experience in digital hardware architecture, secure algorithm implementation, real-time signal processing, and high-speed data communication. Combines industry experience in FPGA design, integration, and timing optimization with research in cryptographic hardware acceleration, LLM-aided hardware co-design methodologies, and hardware security education. Currently pursuing a PhD in Hardware Security at NC State, focusing on secure and efficient post-quantum cryptography hardware, including FALCON (FN-DSA) and Frodo-KEM.

TECHNICAL SKILLS

Design and Research: FPGA Architecture | RTL Design | Hardware Security | Post-Quantum Cryptography | Algorithm Development | Timing and Area Optimization | Digital Signal Processing
Languages and Design Methods: Verilog | SystemVerilog | VHDL | HLS | Python | TCL | C
Design and Simulation Tools: Vivado | QuestaSim | ModelSim | MATLAB
Test and Measurement: Signal Studio | Wavejudge | Vector Signal Analyzer | Signal Generator | Wireshark
Version Control: Git | ClearCase

RESEARCH EXPERIENCE

Research Assistant and PhD Candidate at NC State University, Raleigh, NC, USA August 2024 – current
PhD Candidate with research in post-quantum cryptography (PQC), secure hardware design, hardware security, and LLM-based hardware design and optimizations for cryptographic algorithms with a focus on FALCON (FN-DSA) and Frodo-KEM.

- Developed an open-source custom floating-point unit for FALCON signature generation; *accepted at FPT 2026*.
- Developed open-source teaching material for cryptography and hardware security, covering correlation power analysis on AES-128, fault injection attacks on AES-128, physical unclonable functions, hardware trojans, and malware detection using zero-cost online software; *published at GLS-VLSI 2026*.
- Explored FPGA and ASIC architectures for 64-bit multipliers targeting FALCON, including two-stage Karatsuba, asymmetrical Tiling, and Comba (symmetrical tiling); *published at LightSec 2025.*
- Investigated LLM-based HLS generation for FALCON's discrete Gaussian sampler; *published at IEEE VLSI-SoC 2025.* Developed a framework for LLM-based HLS and RTL generation for PQC hardware.
- Developed an FPGA-based hardware accelerator for FALCON's discrete Gaussian sampling; *IACR archive 2025.*
- Served as a teaching and lab assistant for the undergraduate course Design of Complex Digital Systems on FPGA and the graduate course Cryptographic Engineering and Hardware Security.

INDUSTRY EXPERIENCE

Independent FPGA Contractor October 2023 – June 2024

- FPGA RTL Design of scanning control and safety electronics on a Zynq UltraScale+ based AMD K26-SOM board for Scanning Laser Ophthalmoscopy and Optical Coherence Tomography.
- M8000 BERT FPGA RTL design at Keysight Technologies.
  - Implemented Partial Reconfiguration (PR) on the FPGA for quick feature reconfiguration.
  - Floorplanning and timing optimization for various features planned in the PR.
  - Designed a novel cascaded PLL structure for precise clock generation with limited resources.
  - Designed parts of IEEE 802.3 (Ethernet) 100-G, 200-G, 400-G FEC at Physical Layer, integrated into the PR.

R&D IC Engineer at Keysight Technologies, Morrisville, NC, USA November 2018 – June 2023
Designed baseband RTL of 5G-NR and 802.11ax/be physical layer on Xilinx FPGAs, performed RTL simulations, analysis, and hardware tests. 5G-NR millimeter-wave over-the-air (OTA) testbed bring-up.

Baseband RTL development and testing 5G-NR End-User Emulator

- Verilog RTL design of Resource Mapping module to support SRS 8x8 MIMO on Virtex UltraScale+ FPGA.
- Brought up 5G-NR millimeter-wave OTA setup in Keysight's lab and at customer sites like Verizon.
- Demonstrated and evaluated over-the-air capabilities of 5G-NR UE chassis at FR2 frequency ranges.
- Independently evaluated throughput against UXA Signal Analyzer at OTA distances of up to 16 feet.
- Generated specific 5G-NR waveforms using Signal Studio and evaluated against customer requirements.

Baseband RTL migration and integration of IEEE 802.11ax (WiFi) MAC and Physical-Layer FPGA from Keysight WiFi Test Platform (AXE) to Keysight 5G Test Platform (UXM) as a proof of concept

- Reduced RTL functionality of Keysight AXE (Wi-Fi Test Platform) baseband codebase and integrated it with Keysight UXM codebase while maintaining core baseband 802.11ax Single-User SISO functionality.
- Achieved 802.11ax MAC and IQ sample loopback on Keysight UXM chassis with modified FPGAs for WiFi.

Baseband RTL development of IEEE 802.11ax/be Physical Layer Receiver on Keysight WiFi Test Platform (AXE)

- Reduced RTL baseband receiver end-to-end latency (SIFS time) in Rx MIMO subsystem to meet IEEE specs, including changes to CDC logic and FFT IP.
- Added RTL support for 160MHz signal bandwidth and characterized the radio performance for edge cases with waveforms created using Signal Studio.
- Created multi-FPGA and multi-PPDU RTL simulation testbenches, test tools and scripts to evaluate and analyze baseband receiver RTL bugs.
- Ported RTL design of 802.11ax OFDMA non-MU-MIMO to Keysight UXM platform (5G Test Platform) while reducing functionality to 2x2 MIMO.
- Designed RTL to decode 802.11be EHT PPDU and user-specific signaling symbols.

Hardware Engineer 3 at Hughes Network Systems, Germantown, MD, USA July 2015 – November 2018

Architected and designed baseband modem RTL for Hughes' satellite-based 3G base station on Xilinx FPGA.

Designed the next-generation Satellite Base Station Sub-system on a Virtex-7 FPGA.

- Created and maintained High-Level and Low-Level FPGA Baseband design documents.
- Modelled the DDR interface throughput along with the Xilinx Memory Interface Generator IP Core in its Native and AXI4 form (with a DMA) when combined with a DDR3 and the specific transaction patterns.
- Developed a novel DDR memory organization and arbitration scheme to interface with a modified Native-interface Xilinx MIG to achieve an average efficiency >70% and peaks of 93% in a live system.
- Designed DDR arbiter to perform offset-address burst reads and writes with minimal penalty, when compared to default AXI4 based MIG, to compensate for sample offsets caused by Doppler effect.
- Designed BIST and memory rotation scheme in the DDR arbiter, to minimize memory degradation under continuous use, and DFT logic to test parts of the rest of the design through the DDR arbiter and memory.
- Designed custom logic to interface with AXI4 I/O submodules to the native DDR arbiter.
- Designed asynchronous-width clock-crossing First-Word-Fall-Through FIFO wrappers for a single BRAM slice supporting multiple individual FIFOs to improve timing closure and area utilization.
- Designed Digital Interpolators and FIR filter paths for various burst types and the surrounding arbiter logic.
- Created Vivado-Implementation optimization TCL and Bash scripts for better FPGA build success rate.
- Created and executed block-level and end-to-end FPGA test plans.
- Performed subsystem and end-to-end integration and testing, rack designs, and agency testing.

EDUCATION

Third-Year Doctor of Philosophy (PhD) – Computer Engineering - Hardware Security
North Carolina State University, Raleigh, NC, USA. 2024 – 2028 (expected)

Master of Science (M.Sc.) - Computer Engineering
North Carolina State University, Raleigh, NC, USA. Graduated: 2015. GPA 3.83/4

Bachelor of Technology (B.Tech.) - Electronics and Communication Engineering
National Institute of Technology, Trichy, TN, India. Graduated 2013. GPA 8/10