Steffi Roy

Gainesville, Florida | 352-222-9831 | steffiroy@ufl.edu | linkedin.com/in/steffiroy

About

Graduate Research student with instructional and research experience in cryptography, verification, architecture, and Hardware Security along with a zeal to work in a challenging research environment. Adept at grasping concepts with an ability to complete projects in the given time frame. Looking for Ph.D. positions starting Fall '23

Education

University of Florida **Jan 2021 – Present**
MS in Electrical and Computer Engineering *GPA: 3.7/4*

Mahindra Ecole Centrale, Hyderabad **July 2016 – Aug 2020**
Bachelor of Technology in Electrical and Electronics *GPA: 3.8/10*
Achivements: *Awarded scholarship of Rs. 100,000 for academic performance each year in bachelor's for 3 years*

FIITJEE Excel College, Hyderabad **June 2014 – May 2016**
Intermediate Schooling *Percent: 97.4%*
Achivements: *Awarded scholarship of Rs. 200,000 in virtue of performance in entrance examination.*

Relevant Coursework: *Computer Architecture, VLSI Circuits, Automated Hardware/Software Verification, Cad for Hardware Security Validation, Advance Hardware Security, Reconfig Computing, Applied ML, Quantum Computing, Machine Learning, Data Structures, Digital Signal Processing, Microcontrollers, and Microprocessors.*

Technical Skills

Programming: Python, MATLAB, System Verilog/Verilog, C++, Assembly, Tcl, SQL, CUDA
Tools: VCS, Pspice, Vivado, Virtuoso, Unix/Linux, Git, ModelSim, LATEX

Experience

Microsoft, Design Verification Intern **January 2023 – April 2023**

- Planning and creating a full chip test between SoC and Southbridge AXI Interconnect.
- Create the coverage, and SVA build, run regressions, and assist in UVM error debugging for Xbox. Using tools like Verdi, DVT eclipse, and Perforce.

University of Florida, Research Assistant **January 2021 – December 2022**

- Developed new paradigms for semiconductor IP protection based on secure and private function evaluation (SFE-PFE).
- Researched on Privacy-Preserving methods for Electronic Design Automation (EDA), Side-channel Resiliency for Neural Networks, and Hardware metering protocols.

Gallium Arsenide Enabling Technology, Chip Testing Intern **May 2019 – July 2019**

- Learned about design, fabrication, assembly, and testing processes/techniques involved in manufacturing of Gallium Arsenide (GaAs) wafers for satellite by working and interacting with scientists and engineers.
- Involved with testing unit and operating various qualification checks on the wafers.

Defense Research Development Laboratory, Autopilot Design Intern **April 2018 – July 2018**

- Simulated linear control Autopilot design for a 3-DOF model of a tactical guided missile using MATLAB. Designed compensators, PID controller and band pass filter.
- Achieved the best performance for the required phase margins, gain margins and best rise time with low noise.

Research Projects

Garbled EDA: Privacy-Preserving Electronic Design Automation

- M. Hashemi, **S. Roy**, F, Ganji, D. Forte, "Garbled EDA: Privacy-Preserving Electronic Design Automation", appeared on International Conference on Computer-Aided Design (ICCAD), November 2022: Garbled EDA, proposes an alternative direction through formulating the problem in a secure multi-party computation setting, where the privacy of IPs, CAD tools, and process design kits (PDKs) is maintained.
- Presents novel approach by formulating the problem in a multiparty context that protects IP, CAD tools, and process design kits (PDKs).

- Garbled EDA is evaluated in the context of simulation, where multiple IP description formats are supported (Verilog, C, S).

Active IC metering Protocol Security Revisited and Enhanced with Oblivious Transfer

- **S. Roy**, M. Hashemi, F. Ganji, D. Forte, "Active IC Metering Protocol Security Revisited and Enhanced with Oblivious Transfer", appeared on SRC TECHCON, September 2022.
- Investigated alternatives which employ 1-out of 2 oblivious transfer (OT), focusing on Bellare Micali OT and Naor Pinkas OT and guarantee protection against malicious adversaries.
- Using OT as an alternative helps with the need to protect the integrity of the private input generated by the chip compared to Maes et al.2009, also discuss possible attacks prevention.

HWGN2: Side-channel Protected Neural Networks through Secure and Private Function Evaluation

- "HWGN2: Side-channel Protected Neural Networks through Secure and Private Function Evaluation" presented in SPACE 22 introduces hardware garbled NN (HWGN2), an FPGA-based hardware accelerator for DL.
- Through a hardware-communication cost trade-off, HWGN2 also allows NN designers to protect their IP in real-time applications with limited hardware resources.
- HWGN2's side-channel resiliency has also been demonstrated using a test vector leakage assessment (TVLA) test against both power and electromagnetic side-channels.

Vulnerabilities and attacks possible on IC metering protocols

- Currently working on finding vulnerabilities related to an active metering protocol such as POCA

Relevant Projects

Implementation of 1D Time-Domain Convolution on the Zynq Zedboard | *VHDL, Vivado* **Dec 2022**

- Implemented a custom circuit on the zedboard using VHDL that exploits a significant amount of parallelism to improve performance when compared to a microprocessor.
- Used Vivado for running synthesis, implementation and generating the bitfile. Achieved a considerable speedup of 16.01 after various optimizations.

Concolic Testing for Identification of Trojans | *Pyverilog, Tcl* **May 2022**

- Created a tool to compare the data flow and control flow results of a given design with its golden model design to detect the presence of trojan. The RTL file (Verilog) of both the designs (golden and trojan inserted) are input to the tool.
- Used Pyverilog to generate the Data flow graph (DFG) and Abstract Syntax Tree (AST). The tool generates the mismatches, extra states, and paths in the data flow and control flow of the trojan design.

Simulation-based validation to find bug in AES | *SystemVerilog, UVM, JasperGold, SVA* **February 2022**

- Used Universal Verification Methodology (UVM) and SystemVerilog for Simulation-based validation, using the dumped simulation results from AES golden model that will be used as a comparison.
- Performed the formal verification of the given RTL implementation of the AES module. Wrote properties in SystemVerilog Assertions (SVA) and verified them using the JasperGold formal verification tool.

Design SRAM in Cadence | *Cadence, Virtuoso* **May 2021**

- Design, simulate, and layout an 8x2 SRAM array in Cadence using the 45 nm process and perform full array simulation.

Missile tracking | *VHDL, FPGA, Xilinx* **February 2020**

- Applied Constant Modulus Algorithm (CMA), an adaptive beam forming algorithm for phased array antenna written in VHDL and implemented it on FPGA using Xilinx and used Software-Defined-Radio (SDR) to measure the efficacy.

Application of Kalman Filter to Electric Drives on FPGA | *Verilog, QuartusPrime, ModelSim* **August 2019**

- Developed synthesizable Verilog code for Field Oriented Control of Permanent Magnet Synchronous Motor.
- Simulated the algorithms on Simulink, coded individual Verilog modules for the control system using Quartus Prime and ModelSim, tested the Verilog modules using Simulink co-simulation, and performed FPGA-in-the-loop testing.

Fire toxin alert system | *STM, GSM, GPS* **May 2019**

- The system uses ARM-STM32f3 microcontroller which can be installed at home, where any fire and gas leakage will be detected by the gas sensors.
- The alarm will alert, and the exhaust fans will dispel the gases and let the fresh air in. The fire department and user will be notified using a GSM module and the coordinates will be transmitted using GPS.

MOOCs

List of Digital Certificates here