RAHUL KANDE

rahulkande@tamu.edu | https://www.rahulkande.com | www.linkedin.com/in/rahulkande | +1 979-739-8914

DOCTORAL RESEARCH

Functional and Security Verification of CPUs and SoCs using Fuzzing

- Pioneered coverage-guided hardware fuzzer, TheHuzz (a scalable and automated regression testing technique), achieving 3.33x faster coverage closure vs. random regression testing. **(Paper Link)**
    - Automated generation of RISC-V programs to use as initial inputs.
    - Extracted coverage from Synopsys VCS simulator, enabling coverage-guided dynamic test generation.
    - Implemented a differential tester to compare RTL simulation and software model. Detected 8 new vulnerabilities and demonstrated privilege escalation and arbitrary code execution attacks.
- Integrated Synopsys VCS (simulation tool) and Cadence JasperGold (formal tool) to boost verification of hard-to-reach design regions in a hybrid hardware fuzzer, HyPFuzz. **(Paper Link)**
    - Detected 3 new vulnerabilities. Achieved 41.24x speedup in coverage achievement.
- Modified traditional fuzzer to use multi-armed bandit (MAB) engine for selecting testing inputs. **(Paper Link)**
    - Detected vulnerabilities 56.49x faster and achieved 3.05x speedup in coverage achievement.

Functional and Security Verification Using SystemVerilog Assertions (Paper Link)

- Developed an LLM-based framework to automate SystemVerilog assertion generation, streamlining prompt engineering, RTL compilation, and evaluation workflows.
- Created 10 benchmarks and 7 evaluation metrics, generated 220k+ assertions using OpenAI code generation LLM. Achieved 93.55% peak accuracy.

Security of System-On-Chips (SoCs) (Paper Link) (Competition Website)

- Developed RISC-V-based buggy SoC designs using CVA6, OpenPiton, and OpenTitan for Hack@EVENT hardware security competition (1500+ participants so far).
- Implemented security features (like AES, secure boot, access control, and register locks) and inserted 150+ bugs mimicking 20+ hardware common weakness enumerations (CWEs).

EXPERIENCE

Offensive Security Researcher, *Intern*, Intel, Hillsboro, Oregon — Dec. 2020 – May 2021

- Built a static analysis tool to automate reset logic vulnerability detection in RTL verification workflows.
- Engineered a TCL script leveraging Synopsys Verdi Interoperable Apps (VIA) interface to extract reset domains of signals from SystemVerilog code.
- Scaled the solution to parse reset logic across Intel's commercial SoC with 1.8 million RTL modules in <2 hours.

RTL Design and Verification Engineer, Samsung Research Institute, Delhi, India — July 2017 – Aug. 2018

- Optimized redundant data paths in the RTL design of an image CODEC IP to reduce the gate count by 10%.
- Automated RTL verification flow and test generation using bash scripts and SystemVerilog test benches, achieved >85% code coverage, and detected four bugs in under 72 hours.
- Built a UVM verification environment to verify a security IP.
- Created the scoreboard with reference model integration by modifying a legacy C model.
- Identified functional coverage points, developed UVM test sequences, and verified the IP for all tests.

RTL Design and Verification Engineer, *Intern,* Semi-Conductor Laboratory, Punjab, India — May 2016 – June 2016

- Designed and verified Verilog modules for UDP and Ethernet stack implementation.
- Implemented and verified internal cache for MAC address. Achieved 14% speedup in packet transmission.
- Built test benches, simulated designs using Xilinx Vivado, and synthesized using Synopsys Design Compiler.

SKILLS

Languages: Verilog, SystemVerilog, C, C++, Python, bash script, TCL script
Tools: Synopsys VCS, Siemens Modelsim, Synopsys VC Formal, Cadence JasperGold, Xilinx Vivado
Hardware Security: Fuzzing, Common Weakness Enumerations (CWEs), SoC security features
Hardware Verification: SystemVerilog assertions, Universal Verification Methodology (UVM), differential testing

EDUCATION

Texas A&M University, College Station, Texas July 2018 – Aug. 2025

Doctor of Philosophy in Computer Engineering (Advisor: Dr. Jeyavijayan Rajendran) GPA: **3.90/4**

Indian Institute of Technology, Guwahati, India May 2013 – May 2017

Bachelor of Tech. in Electronics and Communication Engineering (Minor in Computer Science) GPA: **8.91/10**

ACADEMIC PROJECTS

Architecture and Design of Deep Neural Network Hardware Accelerator Jan. 2019 – May 2019

- Created the architecture and implemented a SystemVerilog-based convolution layer supporting 7-dimensional data with variable-length tensor dimensions, enabling flexible model deployment.
- Incorporated a scheduling algorithm that reduced computation time by 20% and engineered a LUT-based MAC unit that replaced 16 additions with a single lookup table.

Functional Verification of MESI protocol based Cache Coherence system Jan. 2019 – May 2019

- Devised a verification test plan and implemented a UVM verification environment with interfaces, sequences, driver, and scoreboard to validate the cache system. Analyzed the code coverage using the Cadence Incisive tool and created constrained-random tests to maximize the coverage.
- Identified 15 design bugs via SystemVerilog Assertions and performed root-cause analysis.

Undergraduate Research Student, IIT Guwahati July 2016 – May 2017

- Converted the Verilog code of a single-stage microprocessor to a 5-stage processor. Implemented forwarding unit, data hazard handler, 32KB Instruction/Data cache, branch prediction, and early branch evaluation features.
- Designed a Co-processor with a custom instruction extension for machine learning.
- Verified the working on an Xilinx Virtex-6 FPGA for 100 programs, each having up to 100 instructions.

AWARDS & HONORS

- *WhisperFuzz* paper received the distinguished paper award at USENIX Security, 2024.
- *TheHuzz* paper selected for Top Picks in Hardware and Embedded Security, 2023.
- Quality Graduate Student Award, Department of Electrical and Computer Engineering, TAMU, 2023.
- Third place, in Hardware Demonstration, IEEE Hardware Oriented Security and Trust, 2022.
- Multiple student Grant awards from USENIX Security, IEEE HOST, and ACM/IEEE DAC.

PUBLICATIONS (Please check Scholar for full list: https://scholar.google.com/citations?user=4X6V5rwAAAAJ&hl=en&oi=ao)

- R. **Kande**, A. Crump, G. Persyn, P. Jauernig, A.-R. Sadeghi, A. Tyagi, and J. Rajendran, *TheHuzz: Instruction Fuzzing of Processors Using Golden-Reference Models*, USENIX Security Symposium 2022
- **R. Kande**, H. Pearce, B. Tan, B. Dolan-Gavitt, S. Thakur, R. Karri, and J. Rajendran, *(Security) Assertions by Large Language Models*, in IEEE Transactions on Information Forensics and Security, 2024
- V. Gohil*, **R. Kande***, C. Chen, A.-R. Sadeghi, and J. Rajendran, *MABFuzz: Multi-Armed Bandit Algorithms for Fuzzing Processors*, Design, Automation and Test in Europe Conference (DATE) 2024 (* equal contribution)
- P. Borkar, C. Chen, M. Rostami, N. Singh, **R. Kande**, A.-R. Sadeghi, C. Rebeiro, and J. Rajendran, *WhisperFuzz: White-Box Fuzzing for Detecting and Locating Timing Vulnerabilities in Processors*, in USENIX Security, 2024
- M. Rostami, M. Chilese, S. Zeitouni, **R. Kande**, J. Rajendran, and A.-R. Sadeghi, *Beyond Random Inputs: A Novel ML-Based Hardware Fuzzing*, Design, Automation and Test in Europe Conference (DATE) 2024
- C. Chen, **R. Kande**, N. Nguyen, F. Anderson, A. Tyagi, A.-R. Sadeghi, and J. Rajendran, *HyPFuzz: Formal-Assisted Processor Fuzzing*, USENIX Security Symposium 2023

LEADERSHIP & ACTIVITIES

- Mentored 3 junior PhD students and 4 Masters students with their thesis projects at Texas A&M University.
- Designed five class projects on hardware security, and mentored 150+ undergraduate and graduate students.
- Lead a team of 150 members to conduct lectures & workshops including the Annual E-summit of IIT Guwahati.
- Organized TEDx for the first time in IIT Guwahati along with a team of Graduate students.