RAHUL KANDE

rahulkande@tamu.edu | https://www.rahulkande.com | www.linkedin.com/in/rahulkande
Bryan, Texas, 77801, Ph: +1 979-739-8914

EDUCATION

Texas A&M University, College Station, Texas — July 2018 – Aug 2025
Doctor of Philosophy in Computer Engineering — 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**

Related Coursework :

Advanced Computer Architecture | Intro. to Formal Verification | Software Security | Advanced Design Verification
Microprocessor System Design | Microarchitecture Prediction | Secure Computer Systems and Arch

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 (access control, register lock, FUSE memory, secure BOOT, cryptographic engines)
Hardware Verification: SystemVerilog assertions, Universal Verification Methodology (UVM), differential testing

EXPERIENCE

Graduate Research Assistant, *Hardware Security Group,* Texas A&M University — Sept. 2018 – Present
Advisor: Dr. Jeyavijayan Rajendran

- *Developed Hardware Fuzzers to detect vulnerabilities in open-source processors and SoCs*
  - TheHuzz, a coverage-feedback based smart regression testing technique:
    - Extracted coverage from RTL simulators to provide feedback for input generation.
    - Automated generation of RISC-V programs to use as testing inputs.
    - Implemented a differential tester to compare output of RTL simulation and software ISA simulator.
    - Detected 8 new vulnerabilities, leading to arbitrary code execution and privilege escalation attacks.
    - Achieved 3.33x speedup compared to random regression on RISC-V ISA-based Rocket Core processor.
  - HyPFuzz, a hybrid hardware fuzzer that combines simulation-based testing with formal verification:
    - Automated interfacing of simulation-based tool with formal tool.
    - Detected 3 new vulnerabilities. Achieved 41.24x speedup in coverage achievement.
  - MABFuzz, a hardware fuzzer that uses optimization algorithms to speedup verification:
    - Modified traditional fuzzer to use multi-armed bandit (MAB) engine for selecting testing inputs.
    - Detected vulnerabilities 56.49x faster and achieved 3.05x speedup in coverage achievement.
- *Evaluated the capability of LLMs in generating hardware assertions*
  - Automated generation of prompts, querying LLMs, compiling SystemVerilog assertions, and evaluation.
  - Created 10 testing benchmarks, generated 220k+ assertions, and evaluated across 7 metrics.
- *Organized Hack@EVENT, a set of hardware security CTF competitions (1500+ participants so far)*
  - Created three buggy designs based on RISC-V SoCs CVA6, OpenPiton, and OpenTitan.
  - Added security features (like AES crypto engine, access control, register locks, secure boot, and FUSE memory) and security vulnerabilities resembling 20+ hardware common weakness enumerations (CWEs).

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

- Developed automated static analysis tool to aid verification engineers in detecting reset logic bugs.
- Automated parsing of reset logic information using Synopsys Verdi Interoperable Apps (VIA) interface.

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

- *CODEC IP project*: Enhanced the RTL design to reduce design area. The gate count has been reduced by 10%.
  - Upgraded a bash script and a Verilog based testbench to automate the process of design verification.
- *Security IP project:* Modified a C model of the IP to obtain a reference model for verification.
  - Developed a UVM based verification environment to verify the IP; identified functional coverage points, generated corresponding test cases and verified the IP for all test cases.

Undergraduate Research Student, IIT Guwahati July 2016 – May 2017

- *5-stage 32-bit Microprocessor:* Converted single stage microprocessor to 5 stage microprocessor.
  - Implemented Instruction/Data caches, branch prediction, and early branch evaluation features.
  - Designed Co-processor with custom instruction extension for machine learning.
  - Verified working on a Xilinx Virtex-6 FPGA for 100 programs each having 50-100 instructions.

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

- Developed hardware design IP for the UDP and Ethernet internet protocols with support for ARP protocol and an internal cache for temporary MAC address storage using Xilinx ISE Design and simulation tool.

AWARDS & HONORS

- *WhisperFuzz* paper received distinguished paper award at USENIX Security, 2024.
- *TheHuzz* paper shortlisted 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.
- ACM/IEEE Design Automation Conference, best Research Video Award in 2020.
- Department Graduate Merit scholarship, TAMU 2018.
- USENIX Security Student Grant award in 2020 and 2021, IEEE Hardware Oriented Security and Trust Student Grant award in 2020, 2022, and 2023, and ACM/IEEE DAC, Young Fellowship award in 2020 and 2021.
- Qualified Samsung's Professional programming test (only ~20% are Professional qualified world-wide).

PUBLICATIONS

- **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 for Finding Software-Exploitable Vulnerabilities*, USENIX Security Symposium 2022 (**Acceptance rate: 18%**)
- **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 **(Acceptance rate: 29%)**

Please refer to my Google Scholar profile for the full list of publications:
https://scholar.google.com/citations?user=4X6V5rwAAAAJ&hl=en&oi=ao

LEADERSHIP & ACTIVITIES

Texas A&M University

- Mentored three junior PhD students and four Masters students with their thesis projects.
- Assisted my advisor with creating and teaching two Hardware Security courses.
  - Designed five class projects on hardware security, mentored 150+ undergraduate and graduate students.
- Volunteering at Aggieland Humane Society, TX, USA. Dec. 2022 to Present

Samsung Research Institute *(Great work place agent)* Aug. 2017 – Aug. 2018

- Planned and organized various team building activities on monthly and quarterly basis.

Indian Institute of Technology, Guwahati *(Head of Entrepreneurship Development Cell)* April 2015 – April 2016

- 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 Post Graduate students.
- Member of National Sports Organization (NSO), Athletics.