RAHUL KANDE

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

EDUCATION

Texas A&M University, College Station, Texas — July 2018 – Aug 2025
Ph.D. in Computer Engineering — GPA: **3.90** on scale of **4**

Indian Institute of Technology, Guwahati, India — May 2013 – May 2017
Bachelor of Tech. in Electronics and Communication Engineering (with minor in Computer Science) — GPA: **8.91** on scale of **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	Design Laboratory

EXPERIENCE

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

- *Hardware Fuzzing of open-source processors and SoCs*
  - TheHuzz, a coverage-feedback based smart regression testing technique.
    - Detected 8 new vulnerabilities, leading to arbitrary code execution and privilege escalation attacks.
    - 3.33x speedup compared to random regression.
  - HyPFuzz, a hybrid hardware fuzzer that combines simulation-based testing with formal verification
    - Automated the interfacing of simulation-based tool with formal tool.
    - Detected 3 new vulnerabilities. Achieved 41.24x speedup in coverage achievement.
  - MABFuzz, a smart fuzzer that uses multi-armed bandit (MAB) algorithms to speedup verification
    - Developed a hardware fuzzer that uses MAB engine to schedule testing input selection.
    - Detected vulnerabilities 56.49x faster and achieved 3.05x speedup in coverage achievement.
- *Evaluated the capability of LLMs in generating hardware assertions*
  - Automated the 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 that resemble 20+ hardware common weakness enumerations (CWEs).

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

- Developed automated static analysis tool to aid verification engineers in detecting the reset logic bugs.
- Used Synopsys Verdi Interoperable Apps (VIA) interface to automatically parse reset logic information.

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

- *CODEC IP project*: Enhanced the RTL design to reduce the design area. The gate count has been reduced by 10%.
  - Upgraded a bash script and a Verilog based test bench 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 the functional coverage points, generated the corresponding test cases and verified the IP for all the test cases.

Department of Electronics and Communication Engineering, IIT Guwahati — July 2016 – May 2017
Undergraduate Research Student

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

Semi-Conductor Laboratory, Punjab, India *(Internship)* — 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.

TECHNICAL SKILLS

Languages: Verilog, C, C++, Python, bash script
Methodologies: Universal Verification Methodology (UVM)
Tools: VCS (Synopsys), irun (Cadence), Jaspergold (Cadence), VC Formal (Synopsys), Vivado (Xilinx)

AWARDS & HONORS

- *WhisperFuzz* paper received the 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.
- *MABFuzz* paper featured on IEEE Spectrum, IEEE's flagship publication.
- USENIX Security Student Grant award in 2020 and 2021, IEEE Hardware Oriented Security and Trust Student Grant award 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.
- Volunteer 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 organize 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.

WORK AUTHORZATION

Eligible to work in the U.S for a period of 12 months under Curricular Practical Training (CPT) program.