# Harshit Kumar

Dept. of Electrical and Computer Engineering
Georgia Institute of Technology, Atlanta
www.kumarharshit.com

hkumar64@gatech.edu
harshitk11@gmail.com
+1-470-685-5060

## Education

| Year | Degree/Examination | Institute | CGPA |
|---|---|---|---|
| 2019 - 2023 (Exp.) | Ph.D. Electrical & Computer Engineering | Georgia Tech | 4.0/4.0 |
| 2014 - 2019 | B.S. & M.S. Dual Degree<br>Electronics and Electrical Communication | IIT Kharagpur | 9.04/10.0 |

## Publications [Google Scholar]

- "Towards Improving the Trustworthiness of Hardware based Malware Detector using Online Uncertainty Estimation" **Harshit Kumar**, Nikhil Chawla, and Saibal Mukhopadhyay. *DAC 2021.*
- "Machine Learning in Wavelet Domain for Electromagnetic Emission Based Malware Analysis" Nikhil Chawla, **Harshit Kumar**, and Saibal Mukhopadhyay. *IEEE Transactions on Information Forensics and Security.*
- "BiasP: a DVFS based exploit to undermine resource allocation fairness in Linux Platforms" **Harshit Kumar**, Nikhil Chawla, and Saibal Mukhopadhyay. *ACM/IEEE ISLPED 2020.*
- "Securing IoT Devices using Dynamic Power Management: Machine Learning Approach" Nikhil Chawla, Arvind Singh, **Harshit Kumar**, Monodeep Kar, and Saibal Mukhopadhyay. *IEEE Internet of Things Journal.*
- "Towards Increasing the Difficulty of Reverse Engineering of RSFQ Circuits" **Harshit Kumar**, Tahereh Jabbari, Gleb Krylov, Kanad Basu, Eby G Friedman, and Ramesh Karri. *IEEE Transactions on Applied Superconductivity.*
- "On Finding Suitable Key-Gate Locations in Logic Encryption" Rajit Karmakar, **Harshit Kumar**, Santanu Chattopadhyay. *International Symposium on Circuits and Systems (ISCAS)-2018* .
- "Efficient Key-gate Placement And Dynamic ScanObfuscation Towards Robust Logic Encryption" Rajit Karmakar, **Harshit Kumar**, Santanu Chattopadhyay. *IEEE Transactions on Emerging Topics in Computing.*

## Work Experience/Internships

**Graduate Research Assistant** Aug 2019 - present
*Supervisor: Prof Saibal Mukhopadhyay*
Georgia Institute of Technology, Atlanta, Georgia

- Exploring the impact of malware execution on the hardware stack in modern SoCs to devise robust malware detection strategies.
- Applied Bayesian inspired ML techniques for designing trustworthy hardware-based malware detectors.
- Proposed a kernel-level exploit that uses power-management as a backdoor for controlling resource allocation fairness in modern SoCs.

**Security Analysis of Superconducting Circuits** May 2018 - July 2018
*Supervisor: Prof Ramesh Karri & Prof Kanad Basu*
Tandon School of Engineering, New York University

- Performed security analysis of RSFQ circuits, a class of superconducting electronics, for preventing IP-Piracy.
- Developed a novel, low-overhead strategy for camouflaging RSFQ circuits which exploits similar structure of standard cells.
- Demonstrated the resilience of the aforementioned technique to SAT-based attacks by using a model-checking based attack framework.

**Single Channel Speech Enhancement** May 2017 - July 2017
TATA Power SED, Bangalore

- Implemented a single channel speech enhancement algorithm based on the masking properties of the human auditory system.
- Achieved an increase in SNR of 9.3 dB for noisy signals having SNR of 0dB.

## Other Research Experiences

**Logic Encryption (bachelor and master's thesis)** Sept 17 - April 18
*Supervisor: Prof Santanu Chattopadhyay, IIT Kharagpur*

- Formulated a strategy, for selection of key-gate location, which enhances the security of a logically encrypted chip, preventing IP piracy and scan-based side channel attacks.
- Developed an algorithm for preventing sensitization based attacks that finds key gate locations in linear time.
- Performed comprehensive security analysis demonstrating the defense's resilience against SAT attacks.

**Data Acquisition System** Oct 15 - July 16

*Team KART, Formula SAE Team, IIT Kharagpur*

- Implemented the Data Acquisition System project aimed at providing storage, wireless transmission as well as on-board real time display of vehicle data based on a 32-bit ARM Cortex M4 CPU based micro-controller.

## Selected Term Projects

**Reverse Engineering of Malware** Spring 2021

*Prof. Brendan Saltaformaggio, Georgia Institute of Technology*

- Reverse engineered malware : Michelangelo, DOS-7, SQLSlammer, Lucius, and Harulf using reverse engineering tools like IDAPro, OllyDbg, PEView.
- Got familiar with anti-debugging, anti-VM, anti-disassembly, polymorphic, and obfuscation techniques employed by malware authors while reverse engineering the malware.

**Computer Architecture** Spring 2020

*Prof. Thomas Conte, Georgia Institute of Technology*

- Designed a cache hierarchy simulator that simulates memory traces containing instruction and data addresses.
- Implemented a superscalar pipelined processor capable of performing out of order and speculative execution.
- Designed a cache-coherence simulator implementing MESI and MOESIF protocol for multi-core processors.

**Circuit Partitioning Using Graph Neural Networks** Spring 2020

*Prof. Sung-Kyu Lim, Georgia Institute of Technology*

- Implemented a deep-learning based fully differentiable approach to solve the problem of circuit partitioning using Graph Convolutional Networks.

## Positions of Responsibility

May 2016 - May 2017

**Head of Electronics Subsystem**

*Team KART, Formula SAE Team of IIT Kharagpur*

- Led a team of 6 students in developing numerous constituents of the electronic subsystem in a formula student car.

## Technical Skills and Expertise

- **Malware Analysis**: IDAPro, OllyDbg, PEView, Assembly
- **CAD Tools** : Cadence (Virtuoso Analog Design Environment), Synopsys ( Design & IC Compiler), Pspice
- **Micro-controllers**: ARM Cortex-M, AVR, Raspberry Pi
- **Other Softwares**: Proteus, EagleCAD, Atmel Studio, Coocox IDE, Xilinx
- **Tools** : Git, LaTex
- **Programming Languages**: C, C++, Python, MATLAB

## Academic Honors and Awards

- Member of the gold winning team at the Inter-IIT Tech Meet-2018 in "Technologies for Soldier Support".
- Offered fellowship by Indian Academy of Sciences, Bengaluru, during the summers of 2017. (*Surrendered due to internship at TATA Power SED*)
- Succeeded in being among the top 35 finalists out of 1500 teams of KPIT Sparkle 2017, a national design and development innovation contest for engineering.
- Ranked among the top 0.3% students in IIT-JEE (Advanced) Examinations, 2014 (air- 1059).

## Relevant Coursework

- **VLSI and Computer Architecture Related Courses:** Analog & Digital Electronic Circuits, Architectural Design of ICs, Analog & Digital VLSI, VLSI CAD, Advanced Computer Architecture, Advanced Operating Systems, Digital Systems Testing
- **Communications & Signal Processing Related Courses:** Analog Communications, Digital Communications, MIMO Communications, Network Theory, Signals and Systems, Digital Signal Processing, Introduction to Internet & Wireless Communications, Estimation & Detection Theory
- **Miscellaneous Courses:** Matrix Algebra, Probability and Stochastic Process, Mathematics I & II, Control Systems Engineering, Algorithms-I, Programming & Data Structures, Machine Intelligence & Expert System, Malware Reverse Engineering