ANTHONY ETIM

Address: Yale University, 10 Hillhouse Avenue, New Haven, CT, 06511 Email: anthony.etim@yale.edu
Webpage: https://anthonyedemetim.com/ Phone Number: +1 (215) 485-8250
https://www.linkedin.com/in/anthony-etim/

EDUCATION

Yale University, New Haven, CT August 2021 – May 2027
Ph.D. in Electrical Engineering
Research Assistant, Computer Architecture and Security Lab (CASLAB).
Advisor: Prof. Jakub Szefer

Yale University, New Haven, CT August 2021 – May 2024
M.S., M.Phil. in Electrical Engineering

Villanova University, Villanova, PA August 2017 – May 2021
B.S. in Electrical Engineering,
Minors in Computer Science and Computer Engineering

TECHNICAL SKILLS

Programming: Python, C++, C, MATLAB, Java, SQL, VHDL, Verilog， SystemVerilog, Haskell.
Tools: AWS, Xilinx Vivado/ISE, Quartus, GitHub, PyTorch, Tensorflow, Hugging Face, Git.
Technological Devices: Raspberry Pi, Arduino.
Expertise: FPGA, Computer Architecture, Hardware Security, AI Security, Machine Learning, Deep Learning, Hardware Architecture, AI HW/SW Co-design, Neural Network Architecture, Large Language Models, Reinforcement Learning.

RESEARCH EXPERIENCE

Yale University, *Graduate Researcher*, New Haven, CT August 2021 – Present

- Pioneered attacks and defenses in ML accelerators — first to recover full-color inputs from ML accelerators on multi-tenant cloud FPGAs via ML-enhanced TDC side-channel analysis.
- Engineered adversarial attacks and defenses — deployed sticker perturbations on traffic-sign CNNs (92 % outdoor success) and implemented a "time-traveling" defense using historical image ensembles for 100% robustness against attacks.
- Fortified Tiny ML algorithms — induced near-100% misclassification via voltage glitches on four models; restored accuracy with random self-reducibility and majority voting.
- Secured Q-Learning and Deep Q-Learning systems — evaluated voltage-glitch and bit-flip attacks, revealed defense gaps, and developed a fault-resilient implementation for dynamic control environments.
- Built self-correcting fault-injection defenses — applied randomized perturbations and majority-voting to detect and correct faults in ML and cryptographic accelerators, optimizing robustness via error-distribution analysis.

Scale AI, *Gen AI Intern,* New York, NY June 2025 – Present

- Designed domain-specific and adversarial evaluations for frontier LLMs; performed failure-mode analyses and delivered recommendations adopted in model updates.
- Oversaw end-to-end training and fine-tuning of a code-reasoning LLM; developed C++/Python solutions for top-3% Olympiad problems, applied LoRA/PEFT to enhance chain-of-thought, and benchmarked Olympiad-level reasoning to surface failure modes that informed architecture improvements.

Villanova University, *Undergraduate Researcher*, Villanova, PA Fall 2020

- Used Matrix Singular Value Decomposition (SVD) technique to optimize the deep neural network (DNN) on the AVNET Ultra96-V2 FPGA development board.
- Evaluated the performance, accuracy, and energy consumption of the optimized system.

Electrical Engineering Intern, National Grid, Albany, NY, Remote Summer 2020

- Collaborated with a team of 4 engineers to help reorganize and plan the grid network using various tools.
- Modelled data to fit various design requirements and constraints of the power system.
- Assisted in the management and creation of a SharePoint Setting Repository for the handoff of smart control settings to the field device engineers.
- Collaborated with other engineers to build a database of DMX and control house plans for the grid network.

Villanova University, *Undergraduate Researcher*, Villanova, PA March 2018 – May 2019

- Conducted research on the development of the flow network modeling tool Villanova Thermodynamic Analysis of Systems (VTAS), which models the energy flows throughout a data center.
- Upgraded the Graphical User Interface (GUI) for the Villanova Thermodynamic Analysis of Systems (VTAS) data center flow network modeling tool.
- Developed the GUI for the VTAS electrical system layout.

PUBLICATIONS

- **Anthony Etim** and Jakub Szefer. "Fall Leaf Adversarial Attack on Traffic Sign Classification". arXiv preprint, 2024.
- **Anthony Etim** and Jakub Szefer. "Time Traveling to Defend Against Adversarial Example Attacks in Image Classification". arXiv preprint, 2024.
- Ferhat Erata, TingHung Chiu, **Anthony Etim**, Srilalith Nampally, Tejas Raju, Rajashree Ramu, Ruzica Piskac, Timos Antonopoulos, Wenjie Xiong, and Jakub Szefer. "Systematic Use of Random Self-Reducibility in Cryptographic Code against Physical Attacks". Accepted by the IEEE International Conference on Computer-Aided Design **(ICCAD)**, 2024.
- **Anthony Etim**, Shanquan Tian, and Jakub Szefer. "Extending FPGA Information Leaks with Trojan Phantom Circuits". Accepted by the IEEE International Symposium on Secure and Private Execution Environment Design (**SEED**), 2024.
- Theodoros Trochatos, **Anthony Etim,** and Jakub Szefer. "Covert-channels in FPGA-enabled SmartSSDs". Accepted by the 22nd International Conference on Field-Programmable Technology (**FPT**), Journal Track at ACM Transactions on Reconfigurable Technology and System **(TRETS)**, 2023.

TEACHING EXPERIENCE

- **Teaching Fellow,** Yale University, New Haven, CT — Spring 2023
  Introduction to Computer Engineering (EENG 201)
- **Teaching Fellow,** Yale University, New Haven, CT — Fall 2022
  Introduction to Electronics (EENG 200)

SERVICE

- **ACM Transactions on Architecture and Code Optimization (TACO),** Reviewer — August 2025
- **Yale Cloud Computing and FPGA Security Symposium (CCFS) 2022,** Co-organizer — November 2022
- **Yale Grad Society of Women Engineers,** Undergrad Liaison Co-chair — Fall 2022 - Present

LEADERSHIP EXPERIENCE

Tau Beta Pi, National Engineering Honor Society, Villanova Chapter, Vice-President — March 2020-May 2021

- Planned and conducted various professional events for the chapter's members such as the initiation information session for new members.
- Helped in the advancement of the technical and professional education of the active members by connecting them with various alumni.

Villanova Engineering Student Council, Co-Chair — September 2019- May 2021

- Planned events for the College of Engineering and acted as a bridge between the students and faculty.

National Society of Black Engineers, Senator — August 2017-September 2018

- Represented Villanova chapter at the 2017 Fall Regional Conference in Greensboro, NC.

SELECTED HONORS AND AWARDS

- AsianHOST PhD Forum — December 2024
- Yale New Student Fellowship — September 2021
- Dean's Award for Academic Excellence — May 2021
- Dean's Award for Meritorious Service — May 2021
- Dean's List — December 2017 - May 2021
- Tau Beta Pi, the National Engineering Honor Society, — Spring 2020
  Selected based on academic ranking 1/8th of the junior class.
- Klingler Unitas Prize, — April 2020
  Villanova Student Entrepreneurship Competition
- Klingler Unitas Prize, — April 2019
  Villanova Student Entrepreneurship Competition