

VAUGHN VALLE

Brooklyn, NY · (929) 776-8543 · vaughnmv@pm.me · vaughnvalle.com
Google Scholar · ResearchGate · github.com/VaughnValle · linkedin.com/in/vaughnvalle

RESEARCH INTERESTS

Hardware security and trust: physical unclonable functions (PUFs) and hardware roots of trust for resource-constrained IoT and edge devices; information-theoretic leakage of secure sketches and fuzzy extractors; machine-learning attacks on PUFs; tool-grounded, LLM-assisted security verification of hardware designs.

EDUCATION

New York University, Tandon School of Engineering

Sep 2022 – May 2027

B.S. in Computer Engineering, Minor in Cybersecurity · Tandon Scholarship (full scholarship)

Brooklyn, NY

- *Selected coursework:* Computer Security; Network Security; Application Security; Offensive Security; Penetration Testing & Vulnerability Analysis; Digital Logic & State Machine Design; Computer Architecture; Operating Systems; Computer Networking; Quantum Science. *Fall 2026:* Embedded Systems Design; Computer Engineering Design Project I; Quantum Programming.

Philippine Science High School – Central Visayas Campus

Aug 2016 – Jun 2022

Secondary diploma (STEM), electronics engineering track · High Honors; Proficiency Award in Physics

Cebu, Philippines

RESEARCH EXPERIENCE

Undergraduate Researcher, OSIRIS Lab

Nov 2023 – Present

New York University · Advisor: Prof. Alon Hillel-Tuch

Brooklyn, NY

Hardware-based authentication for edge devices using SRAM PUFs [M1]

- Built a hardware root of trust for commodity ESP32 microcontrollers that have no TPM or secure element, using 512-bit SRAM power-up fingerprints captured across repeated cold boots.
- Characterized the PUF: ~6% per-boot noise and 19–21% of cells metastable over 10 boots. An ECC threshold of $t \approx 110$ gave 100% key reproducibility and 55.47% inter-device Hamming distance between derived keys; metastable-cell maps were nearly disjoint across devices (Jaccard distance 0.841).
- Threat-modeled the prototype and demonstrated two attacks: cloning the identity by dumping the stored golden baseline from flash, and replaying the static authentication hash. Hardened it with a code-offset secure sketch (no key at rest) and HMAC-SHA256 nonce challenge–response.
- Quantified helper-data leakage (≈ 990 bits at $t = 110$, $n = 512$): a 512-bit array keeps no secret after error correction, and at least 2 KB of SRAM is needed to support a 256-bit key.

Lead Researcher, LLM4Security

Sep 2026 – Present

New York University · Advisor: Prof. Ramesh Karri, Weihua Xiao

Brooklyn, NY

Does multi-agent orchestration with EDA-grounded feedback improve LLM hardware-security reasoning? [M2]

- Designed a controlled ablation that fixes the model, task, scorer, and 24-call budget across four configurations (tool-free, tool-augmented, supervisor–analyst–verifier, plus a blind critic), so that differences are attributable to orchestration and tool grounding, not to the model or compute.
- Built the local, reproducible stack: a 4-bit 27B-parameter model served with vLLM on ROCm across two AMD Radeon AI PRO R9700 GPUs (64K context, one replica per GPU, role routing), with Icarus Verilog, Verilator, and Yosys/ABC exposed as MCP servers in network-isolated Docker sandboxes and every tool call logged to a hashed, citable evidence ledger.
- Pilot (80 runs) on RTL whose visible testbench passes both safe and faulty designs: orchestration beat the same model as a single tool-using agent by +25 points (90% vs. 65%; 95% CI +10 to +40). Also reported the negative results: no significant gain over tool-free reading, and model-written checkers false-alarmed on 58% of safe-design verdicts.
- Built an 84-case, hash-frozen benchmark of oracle-labeled safe/faulty RTL, 64% from external sources (MITRE CWE, Trust-Hub AES/UART Trojans, Hack@DAC 2021 SoC bugs), and pre-registered a five-hypothesis study (2,268 runs per model, Holm-corrected tests) replicated on a second model family.

Pre-university research (Philippine Science High School; advisor: Benito A. Baje)

VISION: Wearable Edge-AI Navigation for the Visually Impaired · Founder & Project Lead

Jun 2019 – Jun 2022

- Granted a patent (WO202123); Designed a wearable system that processes all computer vision data locally via edge computing on a custom PCB (RPi CM 3+, Intel Neural Compute Stick v2, PiCam V2, GPS module, MPU6050, gTTs module for voice assistant); applied security-by-design principles to prevent data exfiltration and ensure user privacy
- Reached 157.5 ms worst-case latency in dynamic scenes, 13–14× faster than a stock Raspberry Pi 3B+. Registered as a utility model in the Philippines and Japan [P1]; presented at IDEX 2020 and the Singapore International Science

Challenge 2021; featured in *The Manila Times*, *New York University Tandon Page*, and *other news outlets* (2022).

- Proved that localized, secure processing can outperform cloud-dependent models by optimizing on-device system latency to 157.5 ms, eliminating the need to transmit sensitive visual data over external networks

ResPi: A Wearable Real-Time Respiratory Disease Detection System with Convolutional Neural Networks Using Sound Data · *Author* 2021

- Developed a clip on wearable device that classified lung sounds with a transfer-learned Inception V3 CNN on spectrograms for early-onset detection of respiratory diseases, compiled with OpenVINO for an edge accelerator (57 ms inference). Designed the electret microphone amplifier and custom PCB. Research thesis [T1].
- Conducted developmental research using sound data to predict respiratory disease diagnosis in real-time. Built electret microphone hardware for a CNN model with an 89% model accuracy and a 0.05s time diagnosis across common respiratory disease classes, 15706 times faster diagnosis than identified baseline methods

HIKAway: An Arduino-based Monitoring System for Asthma Prevention · *Hardware Lead* 2020

- Built an asthma pre-detection device using particulate matter systems to prevent asthma attacks, yielded a 99% sensor accuracy across 6 trials, achieved 58.3% net promoter score for customer experience and marketability

ReefPatrol: Remote Coral-Reef Monitoring Buoy · *Team Lead* 2020

- Built a LoRa-linked buoy streaming pH, turbidity, temperature, and dissolved oxygen from an Arduino Nano on a custom PCB to an open-data Android app, for coral-reef preservation and health monitoring. Presented at the 8th Asian Youth Innovation Awards.

MANUSCRIPTS, INTELLECTUAL PROPERTY, AND THESES

[M1] **V. Valle** and A. Hillel-Tuch. "Hardware-Based Authentication for Edge Devices using SRAM Physical Unclonable Functions." In preparation, 2026.

[M2] **V. Valle**, W. Xiao, and R. Karri. "LLM4Security: A Controlled Evaluation of Multi-Agent LLM Orchestration with EDA-Grounded Evidence for Hardware-Security Verification." In preparation, 2026.

[P1] B. A. Baje and **V. M. Q. Valle**. "System for Assisting a Visually Impaired User." Registered utility model in the Philippines (No. 2-2020-050872, Jul. 30, 2021) and Japan (No. 3239665, Oct. 21, 2022); PCT International Application WO 2021/230759 A1, published Nov. 18, 2021.

[T1] S. S. D. Capadngan and **V. M. Q. Valle**. "Wearable Real-Time Respiratory Disease Detection System with Convolutional Neural Networks Using Sound Data." Research thesis, Philippine Science High School, 2022.

TEACHING EXPERIENCE

Graduate Teaching Assistant, Application Security, New York University Sep 2026 – Present

- Assisted graduate students in the MS Cyberfellows (online) program and in-person MS program about software development security in C, Web security (TLS, CSP, XSS, CSRF and OWASP Top 10), Database security (SQLi, key mgmt, HSMs), Cloud security (Docker, Microservices, Kubernetes), and Mobile security (Android intent systems, hardware security). Held weekly office hours and graded submissions, helped organize and evaluate GitHub repos, workflows, and submission pipelines for improving course logistics

Undergraduate Teaching Assistant, Department of General Engineering, New York University Sep 2023 – Present

- Taught first-year engineering labs: Arduino and Raspberry Pi programming (C, Python/OpenCV), digital logic with discrete ICs, and CAD (Fusion 360, Revit). Mentored 7 accessibility-focused design teams, e.g., a book-scanning reader for students with dyslexia and a pill dispenser for older adults.

SECURITY & SYSTEMS EXPERIENCE

Development Lead, OSIRIS Lab Jan 2025 – Jan 2026

New York University, Center for Cybersecurity

Brooklyn, NY

- Built the lab's 3-node Proxmox cluster (Ceph, ZFS) for highly available research and CTF infrastructure, and a self-hosted LLM service (vLLM, Ollama, Open WebUI) on two RTX 3090 GPUs that keeps inference on-premises.
- Secured lab services with zero-trust access (Twingate), UniFi IPS/IDS, Wazuh SIEM, and Authentik identity management; remediated XSS (CVE-2026-24778) and SQLi (CVE-2026-26980) exposure in the lab's Ghost CMS.

Cybersecurity Awareness Week (CSAW) Lead

Sep 2024 – Present

New York University, Center for Cybersecurity

Brooklyn, NY

- Wrote reverse-engineering and forensics challenges for the CSAW '24 CTF Qualifiers, built to resist LLM-assisted solving; playtested CSAW '23 and '24 challenges; support CI/CD, outreach, and sponsorships.

Systems Administration Head, EG1004: Introduction to Engineering and Design

Sep 2024 – Present

New York University, Department of General Engineering

Brooklyn, NY

- Primary incident-response contact for 35 departmental endpoints (BigFix, ESXi, Cortex XDR, InsightVM, BeyondTrust); remediated critical incidents and coordinated Windows 11 patching with NYU IT.

OPEN-SOURCE CONTRIBUTIONS & WORK

Founder, Mirth OS and NixLabs

2018 – Present

- Free, lightweight Linux distributions for low-end hardware that let about 5,000 students attend online classes on decades-old computers during COVID-19; Linux tutorials on YouTube (@sudo_rice) with 349K+ views.

AUR Contributor and Maintainer

2024 – 2025

- Former co-maintainer for the Linux AUR package python-dlib, a modern C++ toolkit containing machine learning algorithms and tools for creating complex software in C++ to solve real world problems

LEADERSHIP & OUTREACH

President, NYU Cybersecurity Club

Jun 2024 – Sep 2025

New York University

Brooklyn, NY

- Ran weekly CTF workshops and Hack Nights; demonstrated Android privilege escalation and Active Directory/Kerberos attacks; hosted a bug-bounty and vulnerability-disclosure program with Bugcrowd.

Controls Team Member, NYU RoboMaster Team Ultraviolet (Vertically Integrated Projects)

Spring 2024

- Helped develop a CAN module for the controls team to interface with the PIC32CM MCU using Altium Designer

Peer Mentor, CAUSE Philippines

2022 – 2023

- Mentored Filipino mentees for U.S. and U.K. college applications (got into New York University and Amherst College; held weekly check-ins, reviewed essays, offered guidance on timeline, recommendations, and selection process)

Vice President & Lead Hardware Engineer, EINSTEIN Club, Philippine Science High School

2019 – 2022

- Led and pioneered 6 humanitarian inventions and 4 innovation groups with international recognition and awards
- Spearheaded streamlined schematics and PCB fabrication in Autodesk EAGLE for rapid prototype development

HONORS & AWARDS

- Tandon Scholarship (full scholarship), New York University 2022 – 2027
- Undergraduate Summer Research Program, General Engineering, New York University 2025
- Finalist, National Olympiad in Informatics Philippines (three consecutive years) 2019, 2020, 2021
- Best Presentation, 8th APEC Conference for Teen Scientists 2021
- Gold Award and Silver Award, 8th Asian Youth Innovation Awards, Malaysia 2021
- Universal Award (People's Choice, Design & Build), Singapore International Science Challenge 2021
- Award of Merit, Malaysia–Croatia Technology Exchange 2021
- Gold Award, ASEAN+3 Center for the Gifted in Science, Korea 2020
- 1st Place, UP Cebu Inter-High School Programming Contest 2019
- 1st Place, Samahang Pisika ng Visayas at Mindanao Research Conference 2019
- Most Promising Invention, Haquathon, Save Philippine Seas 2019
- Finalist, Young Inventors Challenge, Malaysia 2019
- Grand Champion, QBO Startup Basics 2019
- Finalist, NASA Space Apps Challenge 2019
- Finalist, Cognizant Einstein Hunt 2019

SKILLS

- **Hardware security:** SRAM PUFs, secure sketches and fuzzy extractors, min-entropy and leakage analysis, challenge-response protocols, threat modeling, firmware extraction.
- **Hardware & EDA:** Verilog/SystemVerilog, Icarus Verilog, Verilator, Yosys/ABC; ESP32, Arduino, Raspberry Pi, Intel NCS2/OpenVINO; PCB design (EAGLE, KiCad); Fusion 360.
- **Systems & ML:** Linux, Docker, LXC, Proxmox, Kubernetes; vLLM, ROCm, Model Context Protocol, TensorFlow/Keras, OpenCV; Binary Ninja, Metasploit, Wireshark, Wazuh, Splunk.
- **Programming:** Python, C/C++, Verilog/SystemVerilog, Bash, SQL, Lua, MATLAB/Simulink.
- **Languages:** English, Filipino (Tagalog), Cebuano (all native or bilingual).