Yuyang Zhao

Waterloo, ON

Email : yuyangzhao17@gmail.com
https://chaoyuyang.com | https://www.linkedin.com/in/chaoyuyang/

Education

University of Waterloo — Waterloo, ON
Doctor of Philosophy, Electrical and Computer Engineering — *2026 – Present*

- Supervised by Prof. Guang Gong (龔光); continuing my ECE 699 neural cryptanalysis project

University of Waterloo — Waterloo, ON
Master of Engineering, Electrical and Computer Engineering — *2025 – 2026*

- Conferred 2026-10-13. Project: ECE 699, Neural Cryptanalysis with LLM Agents
- **Coursework**: Safety Critical Embedded Systems, Computer Security, Network Security, Digital Integrated Circuits, Reconfigurable Computing, Software Quality Assurance, Database Systems

University of Illinois Urbana-Champaign — Urbana, IL
Bachelor of Science, Computer Engineering — *2017 – 2024*

- **Coursework**: Computer Systems Engineering, IC Device Theory & Fabrication, Computer Organization & Design, Semiconductor Electronics, Programming Languages & Compilers, Artificial Intelligence, Wireless Networks, Applied Linear Algebra, Numerical Methods, Algorithmic Market Microstructure, High Frequency Trading

Skills

Programming: Python, C++, C, Rust, SystemVerilog, x86 & RISC-V Assembly, OCaml, Dafny, JavaScript
ML/Crypto: PyTorch, TensorFlow/Keras, CUDA, NumPy, differential cryptanalysis, neural distinguishers
Hardware/EDA: FPGA, Quartus, Cadence Virtuoso, VLSI Design, IC Fabrication
Tools: Git, Linux, WSL2, MySQL, Kani, COFFE, LaTeX
Languages: Chinese, Japanese

Research

Neural Cryptanalysis with LLM Agents — University of Waterloo
ECE 699 M.Eng. Project, continued in Ph.D. — *2026 – Present*

- Reproduced Gohr's CRYPTO 2019 neural attacks on Speck32/64 (finding a defect in the reference key-ranking script) and studied how well LLM coding agents reproduce cryptanalysis research
- Trained staged neural distinguishers for 11-round Simeck32/64 (accuracy 0.513, near Speck's 0.514) and 10-round Simon32/64 (0.556), each extended one round with a free first round
- Built a three-stage neural key-ranking attack on 13-round Simeck32/64 that recovers the full 64-bit master key in all 43 trials (95% CI 0.92 to 1.00)
- Explained key-rank floors via the ciphertext bits the networks ignore, showed Simon's two-round effect is not caused by its Feistel swap, and benchmarked against Bao et al. (ASIACRYPT 2022) and DBitNet
- Ran multi-hour GPU job queues on three laptops (TensorFlow under WSL2) with interruption-safe result logging

Experience

Momokai — West Covina, CA
Firmware engineer — *2022-05 - 2024-08*

- Led firmware design for mechanical keyboard products, translating hardware features into firmware requirements, and completed firmware implementation for these specifications
- Planned and delivered firmware for 4 keyboard models, supporting product development schedules and manufacturing readiness, enabling product differentiation in responsiveness and feature support
- Implemented Hall-effect magnetic switch support, expanding the company's ability to develop premium magnetic-switch keyboard products

IDOBAO — Shenzhen, China
Firmware engineer (Contract) — *2022-02 - 2022-06*

- Supported commercialization of 6 keyboard models by implementing, optimizing, and maintaining production firmware to fully enable functionality of underlying hardware

- Acted as a technical bridge between manufacturers and the open-source firmware community to reduce integration risk and ensure licensing compliance

University of Illinois Urbana-Champaign Urbana, IL
Course Assistant *2023-02 - 2023-05*

- Audited assignments for organizational and improvement purposes, ensuring coherency and ease of access

Cravings Restaurant Champaign, IL
IT Coordinator *2020-06 - 2020-08*

- Created an online ordering system, allowing the business to increase order taking capacity
- Coordinated and implemented a network infrastructure update, identifying cost inefficiencies

Hao Sheng Wei Ye Computer Store (沈阳南湖昊晟伟业电脑) Shenyang, China
Computer repair technician *2018-06 - 2018-08*

- Performed computer servicing and repairs, and assembled computers to customer specifications

Projects

QMK Firmware Contributions | *atmega32u4, C*

- 130+ pull requests submitted and merged in an open-source keyboard firmware community (https://qmk.fm/)

gukhan: Hangul to Hanja Mixed-Script Converter | *Python, Kiwi, JavaScript, NLP*

- Converts Korean Hangul text to mixed Hangul–Hanja script using Kiwi morphological analysis and a 706,729-entry lexicon; handles HTML, Word, EPUB and subtitles, plus a Chrome/Firefox extension that runs on-device
- Flags ambiguous homographs instead of guessing: on the 1948 Constitution of Korea it got 4 of 1,897 words wrong

quochan: Vietnamese to Chinese-Character Mixed-Script Converter | *Python, NLP, Unihan*

- Vietnamese sibling of gukhan: writes Sino-Vietnamese words in Chinese characters via tone normalisation, dictionary segmentation and a Wiktionary/Unihan lexicon, with a CI regression set

Road Extraction from WWII Topographic Maps | *Python, PyTorch, U-Net, Computer Vision*

- Trained a 1.1M-parameter U-Net from scratch to extract roads from 1943–45 G.S.G.S. maps of north-west France: 0.842 quality and 0.940 completeness on a blind test set, against 0.467 for a rule-based reader; fully reproducible

TLS 1.2 Library in Rust | *Rust, TLS, TCP, RSA, DHE, AES-CBC, HMAC*

- Implemented the TLS 1.2 client/server handshake with RSA and DHE key exchange, certificate authentication, PRF and key expansion, record-layer HMAC and AES-CBC, and Finished-message verification
- Added Signature Algorithms and Secure Renegotiation extensions and validated interoperability with curl and nginx; analyzed tradeoffs such as forward secrecy, IV attacks and downgrade attacks

FPGA development | *SystemVerilog*

- Implemented and verified a pipelined RISC-V RV32I CPU on an FPGA, and built a game in hardware
- Implemented MXFP4 arithmetic and MXFP4 to/from bFP16 conversion on theoretical FPGAs, using COFFE to explore mapping onto different architectures
- Built high-frequency and 2048-bit adders and a parameterized floating-point add/multiply unit

Operating System Development | *C, x86 assembly*

- Built an x86 OS with context switching, segmented memory protection, a file system and I/O drivers

Hardware Design and Fabrication | *Cadence Virtuoso, Lab Work*

- Fabricated and characterized IC devices on a 100 mm silicon wafer at the UIUC fabrication facility
- VLSI design of an adder, transmission-gate flip-flop and 4-bit counter, from schematic to physical layout

Software Testing and Verification Toolkit | *Python, Rust, Kani, Dafny, Hypothesis*

- Built coverage-guided and grammar-based fuzzers, input reduction, property-based tests and formal proofs

Research Project | *Wi-Fi, Bluetooth, Power Analysis*

- Researched power-aware Wi-Fi + Bluetooth side-channel networking and analyzed power use across configurations

MySQL Median Aggregate Function | *C++, MySQL, SQL, UDFs*

- Added MEDIAN to MySQL as a loadable C++ aggregate UDF, handling coercion, NULLs and even-sized groups