CHENGHAO QIU

qiuchenghao2003@gmail.com github (979)574-7878 website google-scholar

EDUCATION

Texas A&M University College Station, TX
PhD @ Computer Science | GPA: 4.0 / 4.0 Aug 2025 - Jun 2030 (Expected)

Tianjin University Tianjin, China
Bachelor @ Computer Science | GPA: 3.75 / 4.0 Sep 2021 - Jun 2025

SKILLS AND INTERESTS

Program Language	Python	SQL	C++
ML Framework	PyTorch	Huggingface
Tools & Liberties	Git	Transformers	Scikit-learn	Pandas	Numpy

RESEARCH EXPERIENCE

ZHOU LAB, Texas A&M University
Graduate Research Assistant, with Prof. Yi Zhou Aug 2025 - present

- Investigating the interpretability of **In-Context Learning (ICL)** by proposing a novel adversarial attack framework that perturbs context demonstrations to induce targeted misjudgments, facilitating a deeper understanding of how Large Language Models utilize contextual information for inference.
- Developing an **analog-circuit-friendly CNN architecture** capable of directly processing noisy RAW RGGB data, and introducing a specialized robustness-aware training scheme that effectively mitigates hardware non-idealities, specifically mismatch drift and noise, for efficient edge computing.

MAGICS LAB, Northwestern University
Undergraduate Research Assistant, with Prof. Han Liu Apr 2024 - July 2025

- Proposed **GERM**, a fast and low-cost genomic foundation model for resource-constrained settings, by replacing standard attention with an outlier-free mechanism, improving fine-tuning performance by **37.98%** and quantization robustness by **64.34%** over the baseline.
- Developed the **GenoArmory** framework, the first unified benchmark for systematically evaluating the adversarial robustness of Genomic Foundation Models (GFMs), and introduced the **GenoAdv** dataset, achieving a **34.71%** increase in Defense Success Rate when used in training.

SELECTED PAPER

[1] Haozheng Luo*, **Chenghao Qiu***, Maojiang Su, Zhihan Zhou, Zoe Mehta, Guo Ye, Jerry Yao-Chieh Hu, Han Liu. Fast and Low-Cost Genomic Foundation Models via Outlier Removal. Forty-Second International Conference on Machine Learning (**ICML 2025**). link

MANUSCRIPT IN PREPARATION

[1] Haozheng Luo*, **Chenghao Qiu***, Yimin Wang, Shang Wu, Jiahao Yu, Han Liu, Binghui Wang, Yan Chen. GenoArmory: A Unified Evaluation Framework for Adversarial Attacks on Genomic Foundation Models. Manuscript in preparation for submission to ICML 2026.

*denotes equal contribution