# YU ZHANG

⌂ https://zymatrix.top/ · showlibia · ✉ frunnever@gmail.com

## Education

**Wuhan University, Wuhan, China** September 2022 — June 2026 (Expected)
School of Cyber Science and Engineering GPA : 3.6/4.0, Average: 87/100

## Experience

**Data Security Lab** Student Assistant
Undergraduate Research Intern 2023.10 -- 2024.06

- **Description**: Research on the Security of Adversarial Attacks on Speech Translation Systems
- **Contribution**:
    - Exploring manipulation attacks (volume modulation, echo injection, fade effects) against Seamless speech translation systems
    - Devised multi-metric evaluation protocol: BLEU score for translation quality degradation, edit distance for transcription distortion, and MiniLM embedding cosine similarity for semantic drift
    - Conducting a comparison of traditional untargeted attacks, conventional direct targeted attacks, and our untranslation attack in speech translation systems.

## Publications

- **When Translators Refuse to Translate: A Novel Attack to Speech Translation Systems**. Wu, H., Liu, C., Chen, J., Du, R., He, K., **Zhang, Y.**, Wu, C., Zhang, T., Guo, Q., & Zhang, J. (2025). To appear in Proceedings of the Usenix Security Symposium 2025.

## Selected Projects

**LLM-based Chinese-Text-Correction** Natural Language Processing
Core Developer, Algorithm Design 2024.09 -- 2025.06(Expected)

- **Project Description**: An undergraduate training program for innovation and entrepreneurship, focusing on the development of an intelligent Chinese text proofreading system aimed at addressing grammatical, semantic, and spelling errors in user-generated content.
- **Technical Contribution**: LLM-based paradigm for text correction: Proposed the implementation adapting DeepSeek-R1-Distill-Qwen-7B model to Chinese CTC task. designed LoRA + task-specific instruction tuning strategy.

**Build a Rust OS on RISC-V From Scratch** Operating System · Tsinghua University OS Camp
Core Developer 2024.9 -- 2024.12

- **Description**: Using system-level development languages (Rust/C) to implement a Unix-like operating system based on RISC-V
- **Contribution**: Developed a OS kernel supporting RISC-V64GC architecture from scratch. Implemented POSIX system calls. Designed memory management with 3-level page tables

## Skills and Interests

- **Programming Languages**: Proficient in C/C++; familiar with Rust, Python
- **Development Tools**: Proficient in Git, Docker
- **Interests**: Machine Learning, Natural language processing, Speech Process, Operating System, etc.