Weixuan Ding

Weixuan.Ding@outlook.com

EDUCATION

Wuhan University, Wuhan, China — September 2022 — June 2026 (Expected)
School of Cyber Science and Engineering — GPA: 3.73/4.00
Bachelor Candidate in Cyberspace Security — 88.90/100

SKILLS

- **Programming:** Python, C, LaTEX
- **Libraries:** PyTorch, Sklearn, Pandas, Numpy, Git
- **Languages:** Chinese(Native), English(Proficent)

SELECTED COURSES

Bachelor's Courses

- Data Structure
- The Design and Analysis of Algorithms
- Machine Learning
- Artificial Intelligence
- Social Computing
- Computer Systems Fundamental
- Operating System

RESEARCH EXPERIENCE

Research on Privacy-Preserving Federated LLM with Heterogeneous Data Distributions

Team Member — March 2024 — Present

- **Explored Privacy Challenges:** Conducted an literature review to understand the privacy challenges associated with Federated Learning Large Language Models(LLMs), focusing on privacy-preserving techniques and their effectiveness.
- **Implemented Differential Privacy based Testing Framework:** Reproduced differential privacy(DP) methods and developed a basic local testing framework incorporating with DP techniques.
- **Experimental Replication and Testing:** Reproduced and evaluated several existing differential privacy approaches including FedProx, Bounded Local Update Regularization(BLUR) and Adaptive Noise Machanism.

PROJECTS

Binary Image Denoising Implementation

Online Course, University of Cambridge

Core Member — February 2023

- Developed and optimized energy functions for Markov Random Fields(MRF), incorporating pixel neighborhood interactions and noise characteristics to achive more accurate image restoration.
- Applied Iterated Conditional Modes and Simulated Annealing algorithms to iteratively minimize energy, resulting in a significant reduction of noise.

CAMPUS EXPERIENCE

Executive and Core Member of School Debate Team

September 2022 — Present

- Honed my ability to efficiently complete tasks under high-pressure conditions and enhanced my skills in information organization, significantly improved my endurance for sustained word and my critical thinking abilities.

INTERESTS

- **Research Interests:** Differentially Private Federated Learning, Trustworthy AI, LLM Safety, Human-computer Interactions,