KEYAN ZHANG

zhangky03@gmail.com ◇ Linkedin: Keyan Zhang ◇ Github: zhangky11

EDUCATION

University of Texas at Austin (UT Austin) Aug. 2024(expected) - Jun. 2026 (expected)

Master of Science in Computer Science Austin, Texas, USA

- **Courses**: ADV Computer Vision, Automated Software Design, Parallel Systems, Database Systems.

Shanghai Jiao Tong University (SJTU) Sep. 2020 - Jun. 2024 (expected)

Bachelor of Engineering in Information Security Shanghai, China

- **Major GPA**: 90.05/100
- **Scholarship**: Shao Qiu Innovation Scholarship (Top 1%), Undergraduate Excellence Scholarship (Top 5%)
- **A+ Courses**: Methodology in Programming (C++), Principle of Databases, Artificial Intelligence and 13 others.

PROFESSIONAL EXPERIENCE

Trip.com Group | Recommendation Algorithm Engineer Intern | *Python*, *Java*, *SQL* May 2024 - Aug. 2024

- Enhanced feature extraction, preprocessing, and model training workflows by leveraging *Hive SQL* to extract raw features from databases, constructing preprocessing operators with *Java* and *Scala*, and utilizing *TensorFlow* for model training, ultimately consolidating the original five steps into three key steps.
- Developed a multi-entity recognition approach using an **MMoE** model trained on click-through and duration data, with a cutoff threshold set at half the importance score of the top-ranked item, successfully resolving the issue of search queries with ambiguous words failing to retrieve all common associated terms.
- Designed a feature importance assessment method using the **Integrated Gradient** algorithm that, after discarding the least significant 30 features, achieved a **1%** increase in Click Through Rate (CTR) during A/B testing on a base of tens of millions of daily clicks.

Intel | Machine Learning Engineer Intern | *Python*, *Pytorch*, *Vue.js*, *Django* Dec. 2023 - May 2024

- Added some demos showcasing common LLM invocation methods, facilitating user utilization, to *Ipex-LLM*, a library for running LLMs on Intel XPU with low-bit optimizations.
- Tested various open-source LLMs after optimizations such as KV Cache, assessing the degree of change in model output logits to ensure the accuracy of the model's predictions.
- Developed a WebUI with *Vue.js* and *Django*, incorporating the Llama3-6B model with the Ipex-LLM framework for multi-turn dialogue features, and utilizing LangChain-chatchat for text vectorization and similar texts retrieval to enhance **RAG**-based knowledge querying features.

Alibaba Ant Group | Machine Learning Engineer Intern | *Python*, *Pytorch*, *Tensorflow* Oct. 2022 - Oct. 2023

- Conducted a survey for submission, summarizing existing Split Learning attacks and defense techniques.
- Improved and Implemented Label Leakage Attacks for Split Learning, achieving an accuracy of over **90%**
- Contributed to *SecretFlow*, an open source framework for Privacy-Preserving Machine Learning (PPML), enhancing its framework to aid users in better utilization and ensure data security for various stakeholders.

ENTREPRENEURSHIP EXPERIENCE

Bright Eyes: AI Multimodal Diagnosis System for Orbital Disease Mar. 2022 - Feb. 2023

Advised by Prof. Huifang Zhou, School of Medicine, SJTU

- Developed solutions for early diagnosis of orbital diseases with Machine Learning, attaining an unmatched accuracy of **93%**, which exceeded human experts using only 2D images for diagnosis.
- Built a web application for orbital disease detection based on our algorithm using *Vue.js* and *Django*, which provided services to over **1.5k** people (36 patients diagnosed and treated on time).
- Won the **Golden Award** (Top 0.005% nation-wide) of the *China College Students "Internet+" Competition*, the highest award bestowed on the best university students in entrepreneurship and innovation competitions.

RESEARCH EXPERIENCE

Optimized Textual Inversion: Fast Generation and Watermark Protection Jul. 2023 - Dec. 2023

Advised by Prof. Qiang Liu, Statistical Learning & AI Group, UT Austin

- Introduced a special face model and applied *LoRA* Fine-tuning on *Stable Diffusion*, eliminating test-time tuning and drastically reducing textual inversion generation time **from 10 minutes to mere seconds**.
- Designed a semantic-level watermark method for textual inversion, guided by CLIP score function, achieving **90%** accuracy and robust *Intellectual Property* (IP) protection against adversarial inputs.

Explainable AI: Computing Shapley Value in a Single Forward Propagation Jan. 2022 - May 2023

Advised by Prof. Quanshi Zhang, John Hopcroft Center for Computer Science, SJTU

- Collaborated to propose an innovative neural network to calculate *Shapley* values *in a single forward propagation*, facilitating the attribution of inputs in order to explain the black box network.
- Reduced the error to just **10%** compared to the state-of-the-art *Shapely* value methods and improved time complexity from $\mathbf{O(2^n)}$ to $\mathbf{O(1)}$, while maintaining its equivalence to the exact *Shapley* value.
- Co-authored a research paper accepted by *ICML* 2023 as third author.

PUBLICATIONS

- Lu Chen, Siyu Lou, **Keyan Zhang**, et al. " *HarsanyiNet: Computing Accurate Shapley Values in a Single Forward Propagation*". The 40th International Conference on Machine Learning (ICML), 2023
- Haodong Zhao, **Keyan Zhang**, Wenjing Fang, et al. "*Safety of Split Learning: A Survey*". CHINESE JOURNAL OF COMPUTERS. (*Under Review*)

PROGRAMMING LANGUAGE & TOOLS

- Programming Language & Framework: Python, C++, Java, Scala, SQL, Javascript, Pytorch, Tensorflow, Django, Flask, Vue.js, React, MongoDB.
- Tools: Git, Matlab, Linux, Burp suite.