Kevin (Yu Ze) Zhang

Email: kevinzyz@pku.edu.cn | Phone: +86 1312011730

Address: Building 6, Zhongguang Global Village, Peking University, Haidian District, Beijing, 100871

EDUCATION

Peking University, School of Computer Science *Beijing, China*
Candidate for Bachelor of Science, Class of 2023, Major in Computer Science and Technology *2019.09-Present*
- Relevant Coursework: Data Science, Data Mining, Intro to AI, Probability & Statistics, Algorithms & Data Structures, OS

RESEARCH EXPERIENCES

Wangxuan Institute of Technology, Peking University. *Beijing, China*
Research Intern | Visual Data Interpreting and Generation Group *2021.05-Now*
- *CMUA-Watermark: A Cross-Model Universal Adversarial Attacks* **4th Author, Accepted to AAAI22**
  - Communicated with different collaborators and wrote the entire paper manuscript; created poster and author presentation.
  - Coded different adversarial perturbation generating algorithms including PGD, DAA, and Ensemble Attack. Ran tests to compare results with our proposed model, proving that our proposed method has higher efficiency and effectiveness.
  - Working on improving robustness to watermark attacks and presenting work to a journal publication.

School of EECS, Peking University. *Beijing, China*
Research Intern | Under supervision of Prof Tian Yu Jia *2021.05-Now*
- *SCP: Bit-level Sparsity Aware DeepLearning Accelerator with Runtime Pruning* **2nd Author, Working Conference Paper**
  - Coded and performed all software tests. Contributed to core precision algorithm and optimizations.
- *Weights Interleaving: Bit-level Sparsity Aware Pruning with Encoding* **1st Author, Working Conference Paper**
  - A runtime pruning algorithm utilizing encoding and balance tradeoff between two multiplicands to maintain precision.

WORK EXPERIENCES

Microsoft Research Asia, Microsoft Ltd. *Beijing, China*
Research Intern | Systems and Networking Research Group *2022.03-Now*
- Working on a system of decentralized trust with computer vision

Tencent Zhuque Security Labs, Tencent Ltd. *Beijing, China*
Project Assistant *2021.07-2021.12*
- *From Attack to Defense: Towards AI Model Security Protection* **3rd Author, Accepted to Power of Community 2021**
  - Summarized lab's research - model watermarking with adversarial attacks to defend against surrogate models - into a paper-like format; paper accepted to international security and hacking conference PoC21.
  - Spoke in PoC21 presentation; created corresponding presentation deck and speech manuscript.

PROJECT EXPERIENCES

Wanxiang Blockchain hackathon, Qtum Sponsor Special Award *Shanghai, China*
Frontend Leader, Core Member *2021.08-2021.10*
- Initially a summer study group for smart contract deployment; evolved as team of nine to participate in the Wanxiang Blockchain hackathon and won the **Qtum Sponsor Special Award.**
- Eagerly participated in meetings; constructed web main page using Vue.js and web3.js.

Data Mining: Chinese Riddle MCQ *Beijing, China*
Team Leader *2021.11-2021.12*
- Fine-tuned multiple ERNIE and BERT models on given Chinese riddle multiple choice dataset using Huggingface. After hyperparameter optimization with TPE and data augmentation, improved original paper's performance from 59.3% to 63.0%.
- Combined heuristic choice elimination methods and **surpassed all other 20 participating teams accuracy-wise (72.3%).**

"Challenge Cup" National Undergraduate Academic Works *Beijing, China*
Core member *2021.12-Now*
- Managed backend and indexation for a Korean corpus from textbooks. Conducted morphological analysis including POS-tagging, and tokenization using KoNLPy.
- Utilized boolean searching and inverted indexing to access records and k-means to cluster passages to topics.

Mini-app Full-Stack Development *Beijing, China*
Individual Full-Stack Development *2021.01-Now*
- Co-founded mini-app Coco.nuts to promote sustainable lifestyles. Developed using Tencent Serverless Cloud, Vue.js, Apache Echarts, and Mongodb. Currently at closed Beta stage.
- SMTea, a tea-ordering app built with Django REST framework and html css frontend.

SKILLS & INTERESTS

- **Skills**: C, C++, Python, Pytorch, Huggingface, Git, Linux, Latex, Vue.js, Django, SQL, Mongodb
- **Honors**: Beijing International Student Government Scholarship (4/257), PKU English Speaking Contest Second Prize (2021)
- **Student Organizations:** Hedge Fund Association Member, Geeklab Workshop Founder, SpeechCrafter Debate Club
- **Language**: English (Native), Mandarin (Native), Cantonese (Native), French (Fluent, 6 years)
- **Interests**: Drums (10+ performances on campus), Golf (varsity, 1st prize in Beijing Collegiate), Cryptocurrency Trading