Zihao Zhao

https://www.zihaozhao.site

Education

• Tsinghua University	Beijing, China
M.S. in Data Science and Information Technology; GPA: 4.00 / 4.00 (Rank: 1/134)	Sep. 2021 – Present
• University of Electronic Science and Technology of China (UESTC)	Chengdu, China
B.E. in Software Engineering (Internet Security); GPA: 3.93 / 4.00 (Rank: 2/127)	Sep. 2017 – Jul. 2021

Research Interests

My research interest centers on devising state-of-the-art solutions for important real-world problems, especially in (distributed) machine learning theory, mathematical optimization, and generalization analysis.

PUBLICATIONS

(* denotes equal contribution)

REFEREED JOURNAL ARTICLES

 AQUILA: Communication-efficient Federated Learning with Adaptive Quantization in Device Selection Strategy
 Zihao Zhao, Yuzhu Mao, Zhenpeng Shi, Yang Liu, Tian Lan, Wenbo Ding, Xiao-Ping Zhang

IEEE Transactions on Mobile Computing (TMC), 2023.

- [2] SAFARI: Sparsity-Enabled Federated Learning with Limited and Unreliable Communications Yuzhu Mao*, Zihao Zhao*, Meilin Yang, Le Liang, Yang Liu, Wenbo Ding, Tian Lan, Xiao-Ping Zhang *IEEE Transactions on Mobile Computing (TMC)*, 2023.
- [3] Towards Efficient Communications in Federated Learning: A Contemporary Survey Zihao Zhao, Yuzhu Mao, Yang Liu, Linqi Song, Ye Ouyang, Xinlei Chen, Wenbo Ding Journal of the Franklin Institute, 2023.
- [4] Communication-efficient Federated Learning with Adaptive Quantization Yuzhu Mao, Zihao Zhao, Guangfeng Yan, Yang Liu, Tian Lan, Linqi Song, Wenbo Ding ACM Transactions on Intelligent Systems and Technology (TIST), 2022.
- [5] MAGLeak: A Learning-based Side-channel Attack for Password Recognition with Multiple Sensors in IIoT Environment Dajiang Chen*, Zihao Zhao*, Xue Qin, Yaohua Luo, Mingsheng Cao, Hua Xu, Anfeng Liu *IEEE Transactions on Industrial Informatics (TII)*, 2020.

CONFERENCE PROCEEDINGS

- [6] Federated PAC-Bayesian Learning on Non-IID Data Zihao Zhao, Yang Liu, Wenbo Ding, Xiao-Ping Zhang IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2024.
- [7] Deep Leakage from Model in Federated Learning
 Zihao Zhao, Mengen Luo, Wenbo Ding.
 Conference on Parsimony and Learning (CPAL), Oral Presentation, 2024.
- [8] Inclusive Data Representation in Federated Learning: A Novel Approach Integrating Textual and Visual Prompt
 Zihao Zhao, Zhenpeng Shi, Yang Liu, Wenbo Ding
 ACM Conf. on Pervasive and Ubiquitous Computing (UbiComp-CPD), Oral Pre., Best Paper Runner-up, 2023.

IN SUBMISSION

[9] ChatGPT Can Be Conversational, Explainable and Universal Zero-shot Recommender Systems Jingwei Yi, Zihao Zhao, Jiawei Shao, Yueqi Xie, Guangzhong Sun, Fangzhao Wu In revision.

RESEARCH AND EXPERIENCE • Tsinghua-UC Berkeley Shenzhen Institution (TBSI)

Researcher, Advisor: Prof. Wenbo Ding

- Generalization analysis: Introduced a non-vacuous federated PAC-Bayesian generalization error bound tailored for non-IID local data, and presented an innovative Gibbs-based algorithm for its optimization. Tightness of the bound has been validated by real-world datasets.
- Privacy leakage: Introduced a model-based attack to recover privacy data of users using a novel matrix Frobenius norm loss functions, realizing 92% recovery accuracy and 32% higher than gradient-based attacks.
- Model sparsification: Developed a sparsity-enabled framework that employs a client similarity matrix to address unreliable communications (e.g., dropped clients), ensuring federated learning convergence even with 60% weight pruning and 80% dropped client update.

• Microsoft

Software Engineering Intern, Bing News & Feeds Group, Manager: Wei He

• GPT clustering and dimension reduction: Compressed the raw GPT-3.5 embedding of 1536-dim into 128-dim utilizing an encoder-decoder framework, along with a crafted reconstruction loss, and retained 92% of the permutation accuracy in our recommendation recall systems. This framework has been actively used in streaming services of Microsoft Bing System.

Research Intern, Social Computing Group, Mentor: Dr. Fangzhao Wu

- Unify prompt tuning: Introduced a twin prompt tuning algorithm for distributed learning integrating both visual and textual modalities, enhancing the data representation capacity of models and achieving superior performance over all baseline methods in 7 datasets.
- GPT for recommendation: Built an explainable recommendation system based on Large Language Models (LLM) like ChatGPT, enabling accurate user interest predictions and high-quality explanations across news and movie recommendation tasks without extra training.

• Institute for AI Industry Research (AIR), Tsinghua University

Research Assistant, Advisor: Prof. Yang Liu

- Adaptive quantization by brute force: Adjusted the quantization precision for each client by brute-force searching for the minimum precision that meets our quantization-error-based criteria, allowed a 25%-50% decrease in transmission compared to existing methods, and demonstrated resilience to up to 90% dropped client rates.
- Adaptive quantization by optimization: Crafted an optimization problem to minimize the impact of skipped client updates, then derived an optimal quantization precision strategy, demonstrating comparable model performance with a 60.4% communication costs reduction on both heterogeneous models and non-i.i.d. scenarios.

• Network and Data Security Key Laboratory, UESTC

Undergraduate Researcher, Advisor: Prof. Dajiang Chen

• Mobile phone password attack towards soft keyboard: Developed a side-channel-based password recognition system utilizing the 3 types of smartphone sensors for password detection, surpassing previous methods with up to 98% accuracy on limited training data.

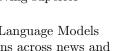
Awards And Honors

- Tsinghua University Graduate School Comprehensive Scholarship (2021-2022 and 2022-2023, First prize, **Top 3%**).
- Outstanding Graduates of Sichuan Province (2021, Top 5%).
- Outstanding Students Scholarship, Golden Award at UESTC (2021, Top 3%).
- First-class Scholarship at UESTC (2017-2018, 2018-2019, and 2019-2020, **Top 10%**).

PROGRAMMING SKILLS

• **Tools**: PyTorch, TensorFlow, Git, Linux

Languages: Python, C, C++, Java, MATLAB, Latex



Beijing, China Aug. 2021 - Dec. 2022

Chengdu, China

Jun. 2020 - Jul. 2021

Shenzhen, China Sep. 2021 - Present

Feb. - May 2023

Beijing, China Feb. - May 2023