Zihao Zhao

https://www.zihaozhao.site

Email : zhao-zh21@mails.tsinghua.edu.cn
Mobile : +86-181-1662-1773

Education

- **Tsinghua University** Beijing, China
  *Master of Science in Computer Science; GPA: 4.00/4.00 (Rank: **1/134**)* *Sep. 2021 – Present*
- **University of Electronic Science and Technology of China (UESTC)** Chengdu, China
  *Bachelor of Engineering; GPA: 3.93 / 4.00 (Rank: **2/127**)* *Sep. 2017 – Jul. 2021*

Research Interests

Distribution learning, optimization, learning theory

Research and Experience

- **Tsinghua-UC Berkeley Shenzhen Institution (TBSI)** Shenzhen, China
  Researcher, Advisor: Prof. Wenbo Ding *Sep. 2021 - Present*
  - **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 recovery 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, ensuring federated learning convergence even with *60% weight pruning* and *80% client update loss*.
- **Microsoft** Beijing, China
  Software Engineering Intern, Bing News & Feeds Group, Manager: Wei He *Feb. 2023 - May 2023*
  - **GPT Clutering and Dimension Reduction**: Compressed an GPT embedding of *1536-dim* into *128-dim* utilizing a meticulously crafted Autoencoder in an end-to-end framework, retaining *92% of its permutation* in recommendation scenarios.

  Research Intern, Social Computing Group, Mentor: Fangzhao Wu *Feb. 2023 - May 2023*
  - **Unify Prompt tuning in FL**: Introduced a twin prompt tuning algorithm – integrating both *visual and textual* modalities, enhancing the data representation capacity of models and achieving superior performance over all baseline methods in 7 datasets.
  - **GPT4Rec**: Built an *explainable* recommendation system based on 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** Beijing, China
  Research Assistant, Advisor: Prof. Yang Liu *Aug. 2021 - Dec. 2022*
  - **Adaptive quantization by brute force**: Adjusted the quantization precision for optimal precision by brute-force searching, allowed a *25%-50% decrease* in transmission compared to existing methods, and demonstrated resilience to up to 90% client dropout 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 IID and non-IID scenarios.
- **Network and Data Security Key Laboratory, UESTC** Chengdu, China
  Undergraduate Researcher, Advisor: Prof. Dajiang Chen *Jun. 2020 - Jul. 2021*
  - **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.

Publications

(* denotes equal contribution)

Journal paper

[1] AQUILA: Communication Efficient Federated Learning with Adaptive Quantization of Lazily-Aggregated Gradients
Zihao Zhao, Yuzhu Mao, Zhenpeng Shi, Muhammad Zeeshan, Yang Liu, Tian Lan, Wenbo Ding, Xiao-Ping Zhang
Submitted to *IEEE Transactions on Mobile Computing*, major revision.

[2] SAFARI: Sparsity-Enabled Federated Learning with Limited and Unreliable Communications
Yuzhu Mao*, **Zihao Zhao***, Guangfeng Yan, Yang Liu, Tian Lan, Linqi Song, Wenbo Ding
IEEE Transactions on Mobile Computing, 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, 2020.

Conference paper

[6] Federated PAC-Bayesian Learning on Non-IID Data
Zihao Zhao, Yang Liu, Wenbo Ding, Xiao-Ping Zhang
Under review.

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

[8] Inclusive Data Representation in Federated Learning: A Novel Approach Integrating Textual and Visual Prompt
Zihao Zhao, Zhenpeng Shi, Yang Liu, Wenbo Ding
ACM Conference on Pervasive and Ubiquitous Computing (UbiComp), 2023.

[9] Deep leakage from model in federated learning
Zihao Zhao, Mengen Luo, Wenbo Ding.
IEEE East Asian School of Information Theory (IEEE EASIT), 2022.

Awards And Honors

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

Programming Skills

- **Tools**: PyTorch, TensorFlow **Languages**: Python, C, C++, Java, MATLAB, Linux, Git, Latex