Zhifeng Jiang

Curriculum Vitae

Department of CSE, HKUST
Clear Water Bay, Kowloon, Hong Kong
zjiangaj@connect.ust.hk
home.cse.ust.hk/~zjiangaj
SamuelGong

Education

2019–2024 **Ph.D. in Computer Science and Engineering**,
The Hong Kong University of Science and Technology, Kowloon, Hong Kong
Thesis Advisor: Prof. Wei Wang
Research Interests: Enhancing Privacy and Efficiency of Machine Learning Systems

2015-2019 **B.Eng. in Computer Science**,
Zhejiang University, Hang Zhou, China
GPA: 3.97/4.0, Graduated with Outstanding Honor (Top 1%)

Selected Projects

Large Language Models

2023–2024 **Vulnerabilities of LLMs to Membership Inference and Data Reconstruction**

- A uniformed pipeline for finetuning and testing LMs (e.g. GPT-2) with multiple tasks (e.g., text classification and autoregressive generation).
- Reproduced likelihood ratio attack for membership inference against finetuned LMs and five gradient leakage attacks for data reconstruction against pretrained LMs.

Federated Learning

2023–2024 **Secure Participant Selection against Adversarial Servers in Federated Learning**

- A VRF-based protocol for random client selection in FL that prevents the malicious server from forming a dishonest majority to protect honest clients' privacy.
- Extension to informed client selection for enhanced training efficiency.
- 1.2 kloc codebase released and work accepted to appear in USENIX Security 2024.

2022–2023 **Efficient Federated Learning with Dropout-Resilient Differential Privacy**

- An "add-then-remove" protocol for noise enforcement in FL with distributed DP that are resilient to missing noise contributions resulting from client dropout.
- A distributed execution framework for optimizing DPFL training efficiency via pipeline-parallelism and demonstrated a speedup of up to 2.4×.
- 10.3 kloc codebase released and work accepted to appear in ACM EuroSys 2024.

2021–2022 **Efficient Federated Learning via Guided Asynchronous Training**

- A client selection and model aggregation algorithm for optimizing FL training efficiency via asynchronous execution and demonstrated a speedup of up to 2×.
- 2.1 kloc codebase codebase released and work accepted in the Proc. of ACM SoCC 2022.

Intership

Feb-May 2019 **Distributed Parallel Computing Lab**, *Huawei*, Hangzhou, China

- Serverless infrastructure with Go, Docker, and Kubernetes.

Jul-Oct 2018 **Prof. Dean Tullsen's Research Group**, *UCSD*, San Diego, US

- Defense against Return-Oriented Programming with Context-Sensitive Decoding on x86-64.

Publications

Conference and Journal Publications

2024 **Zhifeng Jiang**, Peng Ye, Shiqi He, Wei Wang, Ruichuan Chen, Bo Li. "Lotto: Secure Participant Selection against Adversarial Servers in Federated Learning" , *in the Proc. of USENIX Security 2024*

2024 Peng Ye, **Zhifeng Jiang**, Wei Wang, Bo Li, Baochun Li. "Feature Reconstruction Attacks and Countermeasures of DNN Training in Vertical Federated Learning" , *accepted conditional on major revision at IEEE TDSC*

2024 **Zhifeng Jiang**, Wei Wang, Ruichuan Chen. "Dordis: Efficient Federated Learning with Dropout-Resilient Differential Privacy" , *in the Proc. of ACM EuroSys 2024 (acceptance ratio: 16%).*

2023 **Zhifeng Jiang**, Wei Wang, Bo Li, Qiang Yang. "Towards Efficient Synchronous Federated Training: A Survey on System Optimization Strategies" , *in IEEE TBD (IF: 7.2. top journal in Big Data).*

2022 **Zhifeng Jiang**, Wei Wang, Baochun Li, Bo Li. "Pisces: Efficient Federated Learning via Guided Asynchronous Training" , *in the Proc. of ACM SoCC 2022 (acceptance ratio: 25%).*

2021 Minchen Yu, **Zhifeng Jiang**, Hok Chun Ng, Wei Wang, Ruichuan Chen, Bo Li. "Gillis: Serving Large Neural Networks in Serverless Functions with Automatic Model Partitioning" , *in the Proc. of IEEE ICDCS 2021 (acceptance ratio: 20%;* ***Best Paper Runner-Up****, 3 out of 97 accepted submissions).*

Manuscripts

2021 **Zhifeng Jiang**, Wei Wang, Yang Liu. "FLASHE: Additively Symmetric Homomorphic Encryption for Cross-Silo Federated Learning" , *in arXiv preprint (Citation: 41).*

Honors and Awards

2024, 2023 Research Travel Grant, UGC, Hong Kong

2023 Redbird Academic Excellence Award, HKUST

2022 Student Travel Scholarship, ACM SoCC

2021 Best Paper Runner-Up Award (Top 3 out of 489 submissions), IEEE ICDCS

2019 Outstanding Graduate Award (Top 1%), Zhejiang Province

2017 He Zhijun Scholarship (Top 10 in Dept. of CS), ZJU

2017 National Scholarship (Top 0.1% nationwide), Ministry of Education, China

Talks and Presentations

Feb 2023 "Efficient Federated Learning with Dropout-Resilient Differential Privacy". Internal Seminar, Google LLC.

Nov 2022 "Pisces: Efficient Federated Learning via Guided Asynchronous Training". ACM SoCC, San Francisco, CA, US.

Professional Service

Invited Reviewer IEEE Transactions on Mobile Computing.

Program Committee Shadow ACM EuroSys 2023.

AEC Member USENIX OSDI 2022, USENIX ATC 2022, ACM SOSP 2021.

Sub-Reviewer IEEE INFOCOM 2020-2024, IEEE ICDCS 2024, 2023 and 2021, IEEE/ACM IWQoS 2020-2021, IEEE WoWMoM 2021, IEEE ICNP 2020.

Teaching

Teaching Assistant HKUST COMP3511 Operating System: Fall 2022, Fall 2020.
HKUST COMP4651 Cloud Computing: Fall 2021.
HKUST COMP4521 Mobile Application Development: Spring 2020.
ZJU Operating System (Educational Reform Class): Fall 2018.

Skills

Programming Python, PyTorch, Transformers, PEFT: proficient;
C/C++, Java, TensorFlow, Go, Docker, K8s: familiar with.

Language English: TOEFL iBT 105/120, GRE 153/170/3.5