Zhifeng Jiang

Curriculum Vitae

Department of CSE, HKUST
Clear Water Bay, Kowloon, Hong Kong
zjiangaj@connect.ust.hk
samuelgong.github.io
SamuelGong
ZR-W8XsAAAAJ

Education

Sep 2019–Jul 2024 **Ph.D. in Computer Science and Engineering**,
The Hong Kong University of Science and Technology, Kowloon, Hong Kong
Dissertation: "Towards Private and Efficient Cross-Device Federated Learning"
Advisor: Prof. Wei Wang
Research Interests: Privacy Preserving Machine Learning

Sep 2015–Jun 2019 **B.Eng. in Computer Science**,
Zhejiang University, Hang Zhou, China
GPA: 3.97/4.0, Graduated with Outstanding Honor (Zhejiang Province)

Selected Projects

Large Language Models

2024–Now **Safeguarding System Prompts for LLMs**

- A defense mechanism for protecting system prompt privacy against extraction attacks, while preserving conversational capability and runtime efficiency during benign user interactions.
- 2.7 kloc codebase released and work preprinted.

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 in the Proc. of 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 in the Proc. of 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 released and work accepted in the Proc. of ACM SoCC 2022.

Intership

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 (acceptance rate: 17%)*

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: 15%)*

2024 Yongkang Zhang, Haoxuan Yu, Chenxia Han, Cheng Wang, Baotong Lu, **Zhifeng Jiang**, Yang Li, Xiaowen Chu, Huaicheng Li. "SGDRC: Software-Defined Dynamic Resource Control for Concurrent DNN Inference on NVIDIA GPUs" , *accepted to appear in ACM PPoPP 2025 (acceptance rate: 20%)*

2024 Peng Ye, **Zhifeng Jiang**, Wei Wang, Bo Li, Baochun Li. "Feature Reconstruction Attacks and Countermeasures of DNN Training in Vertical Federated Learning" , *accepted to appear in IEEE TDSC (IF: 7, top journal in Computer Security)*

2024 Na Lv, Zhi Shen, Chen Chen, **Zhifeng Jiang**, Jiayi Zhang, Quan Chen, Minyi Guo. "FedCA: Efficient Federated Learning with Client Autonomy" , *in the Proc. of ICPP 2024 (acceptance rate: 29%)*

2023 **Zhifeng Jiang**, Wei Wang, Bo Li, Qiang Yang. "Towards Efficient Synchronous Federated Training: A Survey on System Optimization Strategies" , *in IEEE TBD, Volume 9, Issue 2 (IF: 7.5. 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

2024 **Zhifeng Jiang**, Zhihua Jin, Guoliang He. "Safeguarding System Prompts for LLMs" , *in arXiv preprint*

2021 **Zhifeng Jiang**, Wei Wang, Yang Liu. "FLASHE: Additively Symmetric Homomorphic Encryption for Cross-Silo Federated Learning" , *in arXiv preprint (Citation: 66)*

Honors and Awards

2024, 2023 Redbird Academic Excellence Award, HKUST

2024 × 2, 2023 Research Travel Grant, UGC, Hong Kong

2024 Travel Grant, ACM EuroSys

2022 Student Travel Scholarship, ACM SoCC

2021 Best Paper Runner-Up Award (Top 3 out of 97 accepted papers), 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

Aug 2024 "Lotto: Secure Participant Selection against Adversarial Servers in Federated Learning". Philadelphia, PA, US.

Aug 2024 "Safeguarding Privacy in Machine Learning: Challenges and Innovations from Edge to Cloud". Seminar, Shanghai Jiao Tong University, Shanghai, China.

Jul 2024 "Lotto: Secure Participant Selection against Adversarial Servers in Federated Learning". Online Seminar, Huawei, Co. Ltd.

Jun 2024 "Towards Private and Secure Machine Learning on the Edge". Shenzhen Institute of Computing Sciences, Shenzhen, China.

Apr 2024 "Dordis: Efficient Federated Learning with Dropout-Resilient Differential Privacy". ACM EuroSys, Athens, Greece.

Feb 2023 "Taming Client Dropout and Improving Efficiency for Distributed Differential Privacy in Federated Learning". Online 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, IEEE Transactions on Big Data, IEEE Transactions on Neural Networks and Learning Systems

Program Committee Shadow ACM EuroSys 2023.

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

Journal Sub-Reviewer IEEE Transactions on Network Science and Engineering, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Big Data.

Conference 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.