Jiahuai Mao (formerly Lulu Wang)

+86-19121701003 | jiahuai.mao@polyu.edu.hk
https://jiahuai-mao.github.io

EDUCATION

Singapore University of Technology and Design Jan 2024 - Jan 2025
Visiting Ph.D. Student, ISTD Pillar Supervisor: Prof. Zehui Xiong
Research Interest: Decentralized Federated Learning

University of Padua Oct 2022 - Oct 2023
Visiting Ph.D. Student, SPRITZ Security and Privacy Research Group Supervisor: Prof. Mauro Conti
Research Interest: Security and Privacy of Machine Learning

East China Normal University Sep 2019 - Jun 2025
Ph.D. Candidate, School of Software Engineering Supervisor: Prof. Lei Zhang
Research Interest: Privacy-Preserving Machine Learning（Federated Learning）

Jiangsu University of Science and Technology Sep 2015 - Jun 2019
Bachelor of Electrical and Information Engineering

WORK EXPERIENCE

The Hong Kong Polytechnic University Aug 2025 - Present
Postdoctoral Fellow, Department of Computing Supervisor: Prof. Man Ho Allen Au
Research Interest: Intersection of security, privacy, and machine learning

The Hong Kong Polytechnic University Feb 2025 - Aug 2025
Research Assistant, Department of Computing Supervisor: Prof. Man Ho Allen Au

RESEARCH EXPERIENCE

PreyLoop: Towards Long-Term Privacy Protection and Security Defense in Federated Learning

- While Federated Learning enables training without accessing private training data, it introduces vulnerabilities like inference attacks on senders and backdoor attacks on receivers.
- PreyLoop uses Differential Privacy (DP) to protect senders from inference attacks and applies DP with various backdoor defenses to safeguard receivers.
- Its modular design allows easy integration of additional attack profiles and defenses. Extensive experiments show that PreyLoop significantly reduces these risks with minimal impact on performance.

ADFed: Asynchronous Decentralized Federated Learning with Efficient Cluster-Based Aggregation

- As Federated Learning (FL) shifts to decentralized architectures, the increasing number of clients with varying computing capabilities and data distributions causes slow convergence, high communication overhead, and privacy risks.
- ADFed addresses these issues with a cluster-based asynchronous aggregation algorithm, grouping clients by similar computing power and data to minimize idle time and enhance aggregation efficiency.
- To ensure reliable results, ADFed incorporates a verification mechanism using homomorphic hashing and

signatures, while Local Differential Privacy (LDP) protects against privacy leakage.

PriVeriFL: Privacy-Preserving and Aggregation-Verifiable Federated Learning

- Federated learning faces critical challenges in data privacy and aggregation integrity, as model updates can expose sensitive information and malicious aggregators may manipulate results.
- This work first conducts a sensitivity analysis, revealing that only low bits of model parameters leak sensitive data. This finding allows for selective encryption to reduce overhead effectively.
- Building on this analysis, we propose a low-expansion homomorphic aggregation scheme that combines Paillier encryption with homomorphic hashing to enhance privacy and verify the integrity of results.
- The proposed scheme maintains model accuracy, resists collusion attacks, and reduces communication overhead by 98.35% and computation time by 99.12% compared to traditional Paillier encryption.

Dual-Server Privacy-Preserving Collaborative Deep Learning: A Round-Efficient, Dynamic and Lossless Approach

- Current Collaborative Deep Learning (CDL) faces challenges like high communication costs, limited support for dynamic clients, lack of model-weighted averaging, and accuracy loss.
- This work proposes a dual-server privacy-preserving CDL scheme using masking technology and homomorphic encryption, which reduces communication overhead, maintains the global model's accuracy, and allows clients to join or leave dynamically.
- The scheme is secure against inference attacks and resists collusion by up to *N-2* clients and one server.

PUBLICATIONS

- **Jiahuai Mao**, Jie Fu, Riccardo Spolaor, Qian Chen, Lei Zhang, Zehui Xiong, Mauro Conti, Shuo Wang, Man Ho Au. PreyLoop: Towards Long-Term Privacy Protection and Security Defense in Federated Learning. *Under Review (ESORICS 2026).*
- **Jiahuai Mao**, Zehui Xiong, Riccardo Spolaor, Baosheng Li, Yaxi Yang, Lei Zhang, Man Ho Au, Biplab Sikdar, Shuo Wang. ADFed: Asynchronous Decentralized Federated Learning with Efficient Cluster-Based Aggregation. *Under Review (TON).*
- **Lulu Wang**, Lei Zhang, Kim-Kwang Raymond Choo, Josep Domingo-Ferrer, Mauro Conti, Yuanyuan Gao. Dual-Server Privacy-Preserving Collaborative Deep Learning: A Round-Efficient, Dynamic and Lossless Approach. *TDSC 2025.*
- **Lulu Wang**, Mirko Polato, Alessandro Brighente, Mauro Conti, Lei Zhang, Lin Xu. PriVeriFL: Privacy-Preserving and Aggregation-Verifiable Federated Learning. *TSC 2024.*
- Changti Wu, **Lulu Wang✉**, Lei Zhang✉. Verifiable Private Federated Learning Achieving Low-Communication with CUR Decomposition. *TDSC 2026.*
- Jiasheng Chen, Zhenfu Cao, **Lulu Wang**, Jiachen Shen, Zehui Xiong, Xiaolei Dong. Subversion-Resistant Autonomous Path Proxy Re-Encryption with Secure Deduplication for IoMT. *TNSE 2025.*
- Liangyu Zhong, **Lulu Wang**, Lei Zhang, Josep Domingo-Ferrer, Lin Xu, Rui Zhang. Dual-Server Based Lightweight Privacy-Preserving Federated Learning. *TNSM 2024.*
- Jie Fu, Qingqing Ye, Haibo Hu, Zhili Chen, **Lulu Wang**, Kuncan Wang, Ran Xun. DPSUR: Accelerating differentially private stochastic gradient descent using selective update and release. *VLDB 2024.*
- Yuanyuan Gao, Lei Zhang✉, **Lulu Wang✉**, Kim-Kwang Raymond Choo, Rui Zhang. Privacy-Preserving and Reliable Decentralized Federated Learning. *TSC* 2023.
- Lei Zhang, Wendie Han, Rui Zhang, **Lulu Wang**, Xinyu Meng. Identity-Based Key Management Scheme for Secure Discussion Group Establishment in DOSNs. *TIFS* 2023.

PATENTS

- **Lulu Wang**, Yanfang Zheng, Xuebao Li. A Fire Detection Device Based on Near-Infrared Image Processing. Patent Number: 201721371005.0 (in Chinese).

HONORS & SCHOLARSHIPS

- National Third Prize of the 18th China Graduate Mathematical Modeling Contest in 2021
- University-level Outstanding Graduates in 2019
- Second Prize of Jiangsu Division of the 9th National Software and Information Technology Professional Talent Competition in 2018
- First prize of Jiangsu Division of the 11th iCAN International Innovation and Entrepreneurship Competition in 2018
- Second Prize of Jiangsu Division of the 4th China "Internet+" University Student Innovation and Entrepreneurship Competition in 2018
- National First Prize of the 11th China University Student Computer Design Competition in 2018
- Special Prize in the East China Division of the National University Student Internet of Things Design Competition in 2018
- "Merit Student" of the University in 2015-2016, 2016-2017, and 2017-2018
- National Inspirational Scholarship in 2015-2016, 2016-2017, and 2017-2018
- Second-class Scholarship for Outstanding Students in 2017-2018
- First-class Scholarship for Outstanding Students in 2015-2016 and 2016-2017