Nan Yan

Curriculum Vitae

Department of CSE, WHU
Wuchang District, Wuhan
✉ *lunan0320@gmail.com*
🌐 *lunan0320.github.io*
lunan0320
q-18YfAAAAAJ

Education

2023–Now **M.Eng. in Cyber Science and Engineering,**
Wuhan University, (WHU), Wuhan, China,
Advisor: Prof. Li Yuqing, Average Score: 90.07/100

2019–2023 **B.Eng. in Cyber Science and Engineering,**
Shandong University, (SDU), Qingdao, China
Average Score: 88.51/100, Graduated with Outstanding Honor

Research Interests

Trustworthy AI (LLMs and Agent security), Privacy (HE, DP) and Federated Learning

Selected Projects

Federated Learning

2023–2024 **Efficient and Straggler-Resistant Homomorphic Encryption for Heterogeneous Federated Learning**

- A contribution-aware encrypted weighted aggregation and sketching-based client selection algorithm for optimizing FL training efficiency with CKKS-based HE.
- Achieving a training speedup of 1.85–4.44×, cut the communication overhead by 1.24–22.62×, and reduce the straggler effect by up to 1.71–2.39×.
- 4.5 kloc in codebase, work earned 37 stars and accepted in the Proc. of IEEE INFOCOM 2024.

2022–2023 **Federated Learning with Knowledge Distillation**

- A fundamental and versatile federated learning framework, rigorously tested across diverse datasets and models, designed to facilitate efficient framework construction for federated learning tasks.
- Conducted a reproduction of federated learning incorporating knowledge distillation, alongside the implementation of five baseline methods for comprehensive comparison and earned 25 stars.

Open Source Software Release

2022–2024 **Pioneer: a low-cost Bluetooth-based virus tracking system**

- A cost-effective virus tracking system leveraging Bluetooth technology, secured with the national cryptographic algorithm SM3 for encryption and certification.
- Designed and implemented a comprehensive system encompassing backend database server development, Android application development, and iOS application development.
- 19.6 kloc, codebase released and work earned 153 stars, 86 forks.

Academic Experience

Conference and Journal Publications

2025 **Nan Yan**, Yuqing Li, Xiong Wang, Jing Chen, Kun He, Bo Li, "EmbedX: Embedding-Based Cross-Trigger Backdoor Attack Against Large Language Models," *in Proc. USENIX Security 2025 (acceptance rate: 17.1%).*

2025 Yuqing Li, **Nan Yan**, Jing Chen, Xiong Wang, Jianan Hong, Kun He, Wei Wang, Bo Li, "FedPHE: A Secure and Efficient Federated Learning via Packed Homomorphic Encryption," *in IEEE TDSC (The first author is the advisor).*

2024 **Nan Yan**, Yuqing Li, Jing Chen, Xiong Wang, Jianan Hong, Kun He, Wei Wang, "Efficient and straggler-resistant homomorphic encryption for heterogeneous federated learning," *in Proc. IEEE INFOCOM, 2024 (acceptance rate: 19.6%).*

Manuscripts

2025 **Nan Yan**, Yuqing Li, Jing Chen, Xiong Wang, Wei Wang, Shuhua Li, "Towards Improved Differentially Private Federated Fine-tuning of Language Models on Heterogeneous Clients," *Under Review.*

2025 Haoran Wang, Xiong Wang, Yuqing Li, Jing Chen, Junyi Zhang, **Nan Yan**, Kun He, "Federated LoRA via Error-Free Aggregation and Matrix-Wise Freezing," *Under Review.*

2025 Haoran Wang, Xiong Wang, Yuqing Li, Jing Chen, Yuntao Nie, **Nan Yan**, Meng Jin, Bo Li, Can Mao, "FedP2P: Towards Accelerated Federated Learning with Peer-to-Peer Communication," *Under Review.*

Scholarships and Honors

2025 BYD Scholarship (Top 3 in Dept.CSE), WHU

2025 USENIX Security'25 Student Grant

2023, 2025 Cyberspace Security Innovation Grant, TOPSEC'23 & Huawei'25

2024, 2025 National Scholarship (Top 0.2% nationwide), Ministry of Education, China

2024, 2025 Metrit Student (Ranking: Top 1%) WHU

2024, 2025 First Class Scholarship (Award Rate: 5% school-wide), WHU

2023 Outstanding Graduate Award, SDU

2023 Alumni Council Representative (Dept. CSE, 6/101), SDU

2023 The Power of Role Models Academy Person of the Year (Top 1 in Dept. CSE), SDU

2022 Excellent Student Cadre, SDU

2020, 2022 Second Class Scholarship (Award Rate: 10% school-wide), SDU

2020, 2022×3 Merit-Based Scholarship, SDU

Competition Awards

2025 Second Prize of the 1-st National Open Source Security Award Program, Cyber Security Association, China

2022 Second Prize of The 7-th National College Cryptography Mathematics Contest, Chinese Association for Cryptologic Research, China

2022 Second Prize of The 15-th National College Student Information Security Competition, Cyber Security Association, China

2022 First Prize of The 7-th National College Cryptography Mathematics Contest, Chinese Association for Cryptologic Research, North China Division

2021 First Prize of China Undergraduate Mathematical Contest in Modeling, Shandong Province

Patents and Software Copyrights

Sep 2025 "Differential privacy-based heterogeneous federal fine tuning language model construction method and system", China Patent Application ZL 2024 1 1379992.3, PatentGrant

Oct 2024 "Cross-silo heterogeneous federated learning system based on homomorphic encryption V1.0", Software Copyrights License 2024SR1516588

Technical Skills

Languages: Mandarin Chinese(native) and English (proficiency, IELTS: 7.0)

Programming Languages: Python, C++, Java, SQL, LaTeX