Liangqin Ren

Homepage | liangqinren@gmail.com | GitHub | Google Scholar | Lawrence, KS

RESEARCH INTERESTS

My research interests lie in security and privacy of machine learning systems, particularly in model protection, deepfake defenses, and copyright protection.

EDUCATION

University of Kansas Aug 2021 – Jul 2026 (expected)
Ph.D. in Computer Science. Advisors: Prof. Fengjun Li and Prof. Bo Luo

University of Chinese Academy of Sciences Aug 2017 – Jul 2020
M.Eng. in Computer Technology

Shandong University of Science and Technology Aug 2013 – Jul 2017
B.Eng. in Network Engineering

PUBLICATIONS

1. Yuying Li, Zeyan Liu, Junyi Zhao, **Liangqin Ren**, Fengjun Li, Jiebo Luo, and Bo Luo. The Adversarial AI-Art: Understanding, Generation, Detection, and Benchmarking. In **European Symposium on Research in Computer Security (ESORICS)**, Bydgoszcz, Poland, 2024.
2. **Liangqin Ren**, Zeyan Liu, Fengjun Li, Kaitai Liang, Zhu Li, and Bo Luo. PrivDNN: A Secure Multi-Party Computation Framework for Deep Learning using Partial DNN Encryption. In **Proceedings on Privacy Enhancing Technologies (PETS)**, Bristol, UK, 2024.
3. Xin Xu, Quanwei Cai, Jingqiang Lin, Shiran Pan, and **Liangqin Ren**. Enforcing Access Control in Distributed Version Control Systems. In **IEEE International Conference on Multimedia and Expo (ICME)**, Shanghai, China, 2019.
4. **Liangqin Ren**, Wei Wang, Qiongxiao Wang, Linli Lu. A New Cloud Cryptographic Computing Platform Architecture and Implementation. **Netinfo Security**, vol. 19, no. 9, pp. 91-95, 2019.

PROFESSIONAL SERVICE

Conference Reviewer

- International Symposium on Circuits and Systems (ISCAS) 2025
- International Symposium on Circuits and Systems (ISCAS) 2024
- International Conference on Knowledge Science, Engineering and Management (KSEM) 2024

Journal Reviewer

- Transactions on Dependable and Secure Computing (TDSC) 2025

Community Service

- Session moderator, International Conference on Security and Privacy in Communication Networks (SecureComm) 2022

PRESENTATIONS AND TALKS

1. Enabling Mutually Confidential AI Inference: Selective Parameter Encryption for Deep Neural Networks, in **Central Area Networking and Security Workshop (CANSec)**, Kansas City, Missouri, Oct 15 2025.
2. Contextual Personalization via Interpretable Session-Aware Recommendations, in **I2S Student Organization Meeting**, Lawrence, Kansas, Sep 26 2025.
3. PrivDNN: A Secure Multi-Party Computation Framework for Deep Learning using Partial DNN Encryption, in **Proceedings on Privacy Enhancing Technologies (PETS)**, Bristol, UK, July 16 2024.

EMPLOYMENT

- **Applied Scientist Intern, Amazon, Seattle, WA** May 2025 – Aug 2025
  - Leveraged LLMs to infer user context patterns and long-term viewing preferences from watching records, synthesizing them into user portraits.
  - Enhanced retrieval candidate ranking by incorporating user portraits that encapsulate contextual watching patterns.
- **Applied Scientist Intern, Amazon, Seattle, WA** June 2024 – Sep 2024
  - Extracted potential user emotions from user reviews and movie metadata.
  - Improved personalized recommendations of Prime Video with the video's potential emotional impact.
- **Software Development Engineer Intern, Baidu, Beijing** Jan 2021 – May 2021
  - Developed Baidu translation software development kits for mobile devices.
  - Developed cross-compilation framework between X86 and embedding platforms.

TEACHING EXPERIENCE

Graduate Teaching Assistant, University of Kansas

- **EECS 348: Software Engineering I** Spring 2023 – Fall 2024, Spring 2026
  Instructor: Prof. Hossein Saiedian
- **EECS 348: Software Engineering I** Spring 2025 – Fall 2025
  Instructor: Prof. David Johnson
- **EECS 448: Software Engineering I** Fall 2022
  Instructor: Prof. Hossein Saiedian

HONORS AND AWARDS

- **CANSec Travel Grant Award** 2024
  CANSec Conference, $500
- **CANSec Travel Grant Award** 2022
  CANSec Conference, $500
- **Outstanding Student Leader** 2018
  University of Chinese Academy of Sciences

Last updated: November 25, 2025