

# Zeyan Liu

Department of EECS  
The University of Kansas  
1520 West 15th Street, Lawrence, KS 66046

Phone: xxx-xxx-xxxx  
Email: zyliu@ku.edu  
Web: <https://liuzey.com>

## RESEARCH INTERESTS

- **Security in AI/ML:** Adversarial Machine Learning, Generative AI Security, Privacy-preserving ML
- **Responsible AI:** AI Misinformation and Misusage, Usable Security of AI
- **AI for Cybersecurity:** Network Security

## WORK EXPERIENCE

**Boise State University**, Department of Computer Science, Boise, Idaho, USA  
Tenure-Track Assistant Professor, Starting July 2024

**Visa Inc.**, Cyber Analytics & AI Innovations, Ashburn, VA, USA  
Cybersecurity Research Scientist Intern, May 2023 - August 2023

## EDUCATION

**The University of Kansas**, Lawrence, KS, USA  
Ph.D. Candidate (ABD), Computer Science, 2024  
• Advisor: Prof. Bo Luo, Prof. Fengjun Li

**Wuhan University**, Wuhan, Hubei, China  
B.S., Mathematics and Applied Mathematics, 2019

## PUBLICATIONS

### Conference Papers

1. Aozhuo Sun, Jingqiang Lin, Wei Wang, **Zeyan Liu**, Bingyu Li, Shushang Wen, Qiongxiao Wang, Fengjun Li, "Certificate Transparency Revisited: The Public Inspections on Third-party Monitors", *31st ISOC Network and Distributed System Security Symposium (NDSS)*, 2024.
2. Liangqin Ren, **Zeyan Liu**, Fengjun Li, Kaitai Liang, Zhu Li, Bo Luo, "PrivDNN: A Secure Multi-Party Computation Framework for Deep Learning using Partial DNN Encryption", *Privacy Enhancing Technologies Symposium (PETS)*, 2024.
3. **Zeyan Liu**, Fengjun Li, Zhu Li, Bo Luo, "LoneNeuron: a Highly-effective Feature-domain Neural Trojan using Invisible and Polymorphic Watermarks", *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2022.
4. **Zeyan Liu**, Fengjun Li, Jingqiang Lin, Zhu Li, Bo Luo, "Hide and Seek: on the Stealthiness of Attacks against Deep Learning Systems", *European Symposium on Research in Computer Security (ESORICS)*, 2022.

## TEACHING EXPERIENCE

### The University of Kansas

- EECS 447 Introduction to Database Systems LEC, Spring 2023
- EECS 210 Discrete Structures LEC, Fall 2022
- EECS 647 Introduction to Database Systems LEC, Spring 2022
- EECS 210 Discrete Structures LEC, Fall 2021
- EECS 647 Introduction to Database Systems LEC, Spring 2021

## **MENTORING**

- Liangqin Ren, Ph.D. Student, The University of Kansas, 09/2021-present
- Yuying Li, MS Student, The University of Kansas, 08/2023-present
- Junyi Zhao, Undergraduate Student, The University of Kansas, 10/2021-present. Now MS student at KU.

## **GRANTS & AWARDS**

- EECS Robb Award, The University of Kansas, 2022
- ACM CCS Travel Grant Award, 2022
- Graduate Scholarly Presentation Travel Award, The University of Kansas, 2022
- CANSec Travel Grant Award, 2022
- Honors Graduate (Top 10%), Wuhan University, 2019

## **PROFESSIONAL SERVICES & TALKS**

### **Journal Reviewer**

- IEEE Transactions on Image Processing (TIP)

### **Organizing Committee**

- EAI International Conference on Applied Cryptography in Computer and Communications (EAI AC3), 2022 (Web Chair)

### **Conference Reviewer**

- ACM The Web Conference (WWW), 2024 (7 reviews)
- IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2024 (Artifact Evaluation PC)
- IEEE International Symposium on Software Reliability Engineering (ISSRE), 2023 (Artifact Evaluation PC)
- IEEE International Conference on Acoustics, Speech, & Signal Processing (ICASSP), 2024 (10 reviews), 2023 (10 reviews), 2022 (5 reviews)
- IEEE International Conference on Image Processing (ICIP), 2024 (10 reviews), 2023 (10 reviews), 2022 (4 reviews)
- International Workshop on Security and Trust Management (STM), 2022

### **Talks**

- I2S Student Research Symposium, The University of Kansas, 2023
- GEA Research Symposium, The University of Kansas, 2023.
- 15th Central Area Networking and Security Workshop (CANSec), Wichita State University, 2022.