Cheng-Yi Lee

Research Assistant, Taipei, Taiwan
chengyi.lee.1224@gmail.com — +886 933-070-982 — Google Scholar — Personal Page

RESEARCH INTERESTS

Trustworthy AI, Adversarial Robustness, Information Security

EDUCATION

Kanazawa University, Ishikawa, Japan — Apr 2021 — Mar 2024
M.S. in Electrical Engineering & Computer Science (Double-Degree Program) — Cumulative GPA: 4.00/4.0
Thesis Title: Hierarchical Encryption with Various Functionalities
Advisor: Dr. Masahiro Mambo

National Chengchi University, Taipei, Taiwan — Feb 2020 — Mar 2023
M.S. in Computer Science — Cumulative GPA: 3.90/4.0
Thesis Title: Privacy-preserving bidirectional keyword search over encrypted data for cloud-assisted IIoT
Advisor: Dr. Raylin Tso

Chang Gung University, Taoyuan, Taiwan — Sep 2016 — Jan 2020
B.S. in Information Management — Cumulative GPA: 3.97/4.0

WORK EXPERIENCE

Research Center for Information Technology Innovation, Academia Sinica — Taipei, Taiwan
Research Assistant — Jul 2025 – Present
Advisor: Dr. Jun-Cheng Chen (in collaboration with Dr. Chun-Shien Lu)

- Analyzed inversion-based watermark forgery attacks and designed robust verification frameworks to defend against forged AI-generated content.

Independent Research — Taipei, Taiwan
Researcher — Nov 2024 – Jun 2025

- Investigated robust watermarking methods to ensure authenticity and traceability in diffusion-based image and video generation, in collaboration with Dr. Jun-Cheng Chen.
- Designed proactive defenses against unauthorized model merging and conducted security analyses of typographic, backdoor, and jailbreak attacks in multi-modal models, under the guidance of Dr. Chia-Mu Yu.

Institute of Information Science, Academia Sinica — Taipei, Taiwan
Research Assistant — Apr 2023 – Jun 2024
Research Intern — Jun 2021 – Jan 2022
Advisor: Dr. Chun-Shien Lu (in collaboration with Dr. Chia-Mu Yu)

- Developed robust watermarking schemes integrated into deep learning models for reliable ownership verification and intellectual property protection.
- Conducted security-oriented research on adversarial robustness, focusing on backdoor and adversarial attacks as well as corresponding defense mechanisms in models.

PUBLICATIONS

Conference paper

- Cheng-Yi Lee*, Yu-Feng Chen*, Chun-Shien Lu, Jun-Cheng Chen, "On Forging Semantic Watermarks in Diffusion Models: A Theoretical Perspective," *NeurIPS GenProCC Workshop*, 2025. **[Oral]**
- Cheng-Yi Lee, Yu-Hsuan Chiang, Zhong-You Wu, Chia-Mu Yu, Chun-Shien Lu, "BadVim: Unveiling Backdoor Threats in Visual State Space Model," *28th European Conference on Artificial Intelligence (ECAI)*, 2025.
- Cheng-Yi Lee*, Ching-Chia Kao*, Cheng-Han Yeh, Chun-Shien Lu, Chia-Mu Yu, Chu-Song Chen, "Defending Against Repetitive Backdoor Attack on Semi-Supervised Learning through Lens of Rate-Distortion-Perception Trade-off," *IEEE Winter Conference on Applications of Computer Vision (WACV)*, 2025. (* Equal Contribution)
- Ching-Chia Kao, Cheng-Yi Lee, Chun-Shien Lu, Chia-Mu Yu, Chu-Song Chen, "On The Higher Moment Disparity of Backdoor Attacks," *IEEE Interational Conference on Multimedia Expo (ICME)*, 2024. **[Oral]**
- Cheng-Yi Lee, Cheng-Chang Tsai, Ching-Chia Kao, Chun-Shien Lu, Chia-Mu Yu, "Defending against Clean-Image Backdoor Attack in Multi-Label Classification," *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2024. **[Oral]**

Journal paper

- Cheng-Yi Lee, Zi-Yuan Liu, Masahiro Mambo, Raylin Tso, "Privacy-enhanced Data Sharing Systems from Hierarchical ID-based Puncturable Functional Encryption with Inner Product Predicates," IET Information Security, September, 2024.
- Cheng-Yi Lee*, Zi-Yuan Liu*, Raylin Tso, Yi-Fan Tseng, "Privacy-preserving bidirectional keyword search over encrypted data for cloud-assisted IIoT," Journal of Systems Architecture, Vol. 130, July, 2022. (* Equal Contribution)

Preprint

- Wei-Jia Chen, Min-Yan Tsai, Cheng-Yi Lee, Chia-Mu Yu, "Defending Unauthorized Model Merging via Dual-Stage Weight Protection," Under review, November, 2025.

AWARDS AND CERTIFICATES

Dean List, College of Management, Chang Gung University — Taoyuan, Taiwan
Class of 2020, for Outstanding Academic Performance — Jan 2020

Certified Ethical Hacker (CEH) — EC-Council
Certification Number: ECC25133919874 — Dec 2017 — Dec 2020

ACADEMIC ACTIVITIES AND SERVICES

Conference Reviewer

- IEEE International Conference on Multimedia and Expo (ICME), 2024–2026
- IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2026
- IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2026

OTHER EXPERIENCES

Teaching Assistant — National Chengchi University, Taiwan
Artificial Intelligence and Its Applications to Information Security — Spring 2022

LANGUAGE

TOEFL (Academic): 84 (overall score)
Listening: 24 — Reading: 21 — Speaking: 20 — Writing: 19 — Feb 2025

TECHINCAL SKILLS

- **Programming:** Python, Java, C++, R
- **Developer Tools:** LINUX, Git, Docker
- **Library:** PyTorch, OpenCV, Charm-crypto, PBC (Pairing-Based Crypto)

REFERENCES

Prof. Chun-Shien Lu
Research Fellow, Institute of Information Science, Academia Sinica, Taipei, Taiwan
E-mail: lcs@iis.sinica.edu.tw
Scholar Profiles: Personal Page — Google Scholar

Prof. Chia-Mu Yu
Associate Professor, Department of Electronics and Electrical Engineering, National Yang Ming Chiao Tung University (NYCU), Hsinchu, Taiwan
E-mail: chiamuyu@gmail.com
Scholar Profiles: Personal Page — Google Scholar

Prof. Raylin Tso
Distinguished Professor, Department of Computer Science, National Chengchi University (NCCU), Taipei, Taiwan
E-mail: tsoraylin@gmail.com
Scholar Profiles: Personal Page — Google Scholar