Leo Zhang

Curriculum Vitae

About Me

Position	Senior Lecturer (roughly Associate Professor in US) in Cyber Security
Affiliation	School of Information and Communication Technology Griffith University
Address	Room 1.50, Building G09, 1 Parklands Dr, Southport, QLD 4215
E-mail	leo.zhang@griffith.edu.au
Homepage	https://leozhangcs.github.io/

Research Interests

Trustworthy AI	Adversarial/poison attack and defense of ML/DL, IP protection of ML/DL model, privacy leakage and protection of AI systems, fairness, explainability.
Secure Computing	Privacy preserving computation, storage auditing, access control, blockchain-related applications, cloud/IoT-related secure multiparty computation task.
Multimedia Coding and Security	Watermarking/data hiding, design/cryptanalysis of multimedia cryptosystem, selective encryption, perceptual encryption, joint compression-encryption, secret entropy coding, signal processing in the encrypted domain.

Education

2019 - 2021	**Graduate Certificate of Higher Education**, *Deakin University*, Australia.
Sep. 2013 - Oct. 2016	**Doctor of Philosophy in Electronic Engineering**, *City University of Hong Kong*, Hong Kong SAR, *CGPA – 4.3 (out of 4.3).*
Sep. 2009 - Jun. 2012	**Master of Science in Mathematics**, *Xiangtan University*, Hunan Province, China, *CGPA – 3.77 (out of 4).*
Sep. 2005 - Jun. 2009	**Bachelor of Science in Mathematics**, *Xiangtan University*, Hunan Province, China, *CGPA – 3.5 (out of 4).*

Honors and Awards

2021	Australian Information Security Association (AISA) Researchers of the Year Award for the Development of Australian Cyber Criteria Assessment
2021	Teaching and Learning Award, School of Information Technology, Deakin University - for excellence in aligning courses with industry certifications
2021	International and Partnership Award, School of Information Technology, Deakin University - for excellence in enriching international student experience through online engagement activities
2020	Team Award for international student engagement, School of Information Technology, Deakin University

2019 Research Impact Award, School of Information Technology, Deakin University

2018 Early Career Research Performance Award, School of Information Technology, Deakin University

2013 - 2016 The Outstanding Academic Performance Award for Research Degree Students of City University of Hong Kong for three consecutive years

2014 Active Residence Award for 2013-2014 Semester B, City University of Hong Kong

2013 Excellent Master Degree Thesis of Hunan Province

2012 The Presidential Award for Excellence of research students of Xiangtan University (0.5%)

2012 Excellent master graduate of Hunan Province

Research and Working Experience

Mar. 2023 - Now Senior Lecturer in Security of School of Information and Communication Technology, Griffith University, QLD, Australia.

Nov. 2022 - Feb. 2023 Senior Lecturer in Security and Networking of School of Information Technology, Deakin University, VIC, Australia.

Jan. 2018 - Nov. 2022 Lecturer in Security and Networking of School of Information Technology, Deakin University, VIC, Australia.

Sep. 2016 - Sep. 2017 Postdoctoral researcher at the Department of Computer Science of City University of Hong Kong under the supervision of Prof. Cong Wang (IEEE Fellow, EiC for IEEE TDSC) and Prof. Kui Ren (IEEE Fellow, ACM Fellow).

Mar. 2016 - Sep. 2016 Research assistant at the Faculty of Science and Technology of University of Macau under the supervision of Prof. Jiantao Zhou.

Apr. 2015 - Jul. 2015 Visiting scholar to the Research Center on Electronic Systems of the University of Bologna and at the Department of Engineering of the University of Ferrara under the supervision of Prof. Gianluca Setti (IEEE Fellow, EiC for Proceedings of the IEEE) and Prof. Riccardo Rovatti (IEEE Fellow).

Jul. 2012 - Aug. 2013 Engineer at the State Grid Electric Power Research Institute of China.

Projects

2025 - 2028 Chief Investigator, Ensuring reliable deployment of deep neural network models, Linkage Projects (LP240100315), Australian Research Council, Australia. (Total: AUD $680,000).

2025 - 2027 Chief Investigator, Copyright protection of deep neural network models based on watermarking, Discovery Projects (DP250102634), Australian Research Council, Australia. (Total: AUD $478,000).

2025 - 2027 Chief Investigator, AI-Quantum Nexus: Revolutionizing Group Communication for Large Sport Events, Quantum 2032 Challenge Grant Program, Department of Environment, Science and Innovation, Australia. (Total: AUD $999,300).

2025 Sole Chief Investigator, Cyber Security Microcredentials Pilot in Higher Education Grant, Department of Education, Australia. (Total: AUD $250,000).

2024 Chief Investigator, High-end GPU server for AI research: Nvidia DGX A100, Research Infrastructure Program, Griffith University (Total: AUD $300,000).

2023 Sole Chief Investigator, Cryptographically Enhanced Watermarking for Copyright Protection of Deep Neural Network Models, New Researcher Grant, Griffith University (Total: AUD $20,000).

2022 Sole Chief Investigator, Cryptoanalysis of Prism: A full decentralized user authentication mechanism, CSRI Collaboration Grants Scheme, Deakin University (with Tide Foundation, Total: AUD $15,000).

2022 Sole Chief Investigator, Towards provable-secure proactive defence against neural model stealing attacks, CSRI Collaboration Grants Scheme, Deakin University (Total: AUD $11,722).

2020-2021 Chief Investigator, Development of Australian Cyber Criteria Assessment, Cyber Security Research Centre Limited (with QuintessenceLabs Pty Ltd., Total: AUD $187K).

2019-2021 Chief Investigator, Cyber-Safe Connected Vehicles: Ensuring Secure, Trusted, and Robust Cooperative Automotive Systems, Automotive Engineering Graduate Program of the Department of Industry, Innovation and Science, Australia (with Bosch Australia Pty Ltd., Total: AUD $494K)

2019 Sole Chief Investigator, Storing Media in Public Cloud: Overcome Privacy and Copyright Challenges, Research Grants Scheme of Faculty of SEBE, Deakin University (Total: AUD $5K) .

2018 Sole Chief Investigator, Minor Equipment Scheme, Faculty of Science Engineering and Built Environment, Deakin University (Total: AUD $22,844.80)

2017 - 2019 Sole Chief Investigator, Research on the Secrecy of Compressed Sampling and its Application to IoT, Natural Science Foundation of China (Total: RMB 260K = AUD $50K).

Professional Memberships and Activities

Professional Memberships: Member of IEEE, IEEE Cloud Computing Society, IEEE Signal Processing Society and IEEE Circuits and Systems Society; Member of ACM; Member of Australian Computer Society (ACS); Member of Australian Information Security Association (AISA); EC-Council Certified Ethical Hacker (CEH); EC-Council Certified Security Analyst (ECSA);

Associate Editor: Editorial member for: IEEE Transactions on Dependable and Secure Computing (since 2023, CCF A/Scimago Q1), IEEE Transactions on Multimedia (since 2024, CCF B/Scimago Q1), International Journal of Bifurcation and Chaos (2019-2022, IF 2.145, Scimago Q1), Security and Communication Networks (since 2020, IF 1.288, Scimago Q2)

Guest Editor: IEEE Journal of Biomedical and Health Informatics (2022, Scimago Q1), Complexity (2021, Scimago Q1), Signal Processing-Image Communication (2020, Scimago Q2), International Journal of Distributed Sensor Networks (2019, Scimago Q2), Security and Communication Networks (2018, Scimago Q2);

Organising Committee: Ithings-2018 (Workshop Chair), ATIS-2019 (Program Chair), CIMSS-2023 (Workshop Chair), ProvSec-2024 (General Chair), PAKDD-2025 (Survey Track Chair), RAID-2025 (Local Organisation Chair), IWQoS-2025 (Local Co-Chair).

Program Committee: NSS 18-22 (core b); ML4CS 19; DSC 19; GPC 20 (core c); EAI Qshine 20 (core c); ISSRE 20 (core a); PRDC 20-24 (core b); MSN 21; BlockApp 20-21; CPSCom 21; NeurIPS 22, 24 (core a*); ACM MM 21-24 (core a*); ICME 23 (core a); CVPR 23-25 (core a*); IJCAI 22-25 (core a*); ICCV 23 (core a*); ECCV 24 (core a*); ICML 24 (core a*); AAAI 22-25 (core a*); CIKM 24 (core a); PETS 25 (core a); AsiaCCS 25 (core a); ICLR 25 (core a*).

Teaching Experiences

2024 3015IC/7017ICT Turstworthy AI; 1811ICT/2807ICT/7001ICT Programming Principles; 2007ICT/7019ICT Cyber Security Risk Management & Standards

2023 1811ICT/2807ICT/7001ICT Programming Principles

2022 SIT728 Blockchain Technologies and Real-World Applications; SIT182 Real-World Practices for Cyber Security; SIT379 Ethical Hacking; SIT704 Advanced Topics in Digital Security

2021 SIT379 Ethical Hacking; SIT704 Advanced Topics in Digital Security; SIT281 Cryptography; SIT102 Introduction to Programming

2020 SIT379 Ethical Hacking; SIT704 Advanced Topics in Digital Security; SIT281 Cryptography; SIT202 Networks and Communications

2019 SIT379 Ethical Hacking; SIT281 Cryptography; SIT102 Introduction to Programming

2018 SIT379 Ethical Hacking; SIT281 Cryptography; SIT703 Advanced Digital Forensics

Recent Publications

Citations: 4000+, h-index: 34 (Please refer to my Google Scholar profile for the complete list)

Z. Zhang, X. Zhang, Y. Zhang, **L. Y. Zhang***, C. Chen, S. Hu, A. Gill, S. Pan, *Stealing Watermarks of Large Language Models via Mixed Integer Programming*, to appear in ACSAC, 2024. (core a)

Z. Zhou, M. Li, W. Liu, S. Hu, Y. Zhang, W. Wan, L. Xue, **L. Y. Zhang**, D. Yang, H. Jin, 2024. *Securely Fine-tuning Pre-trained Encoders Against Adversarial Examples*, in Oakland, 2024. (core a*)

X. Mo, Y. Zhang, **L. Y. Zhang***, W. Luo, N. Sun, S. Hu, S. Gao, Y. Xiang, *Robust Backdoor Detection for Deep Learning via Topological Evolution Dynamics*, in Oakland, 2024. (core a*)

Y. Zhang, S. Hu, **L. Y. Zhang**, J. Shi, M. Li, X. Li, W. Wan, H. Jin, *Why Does Little Robustness Help? A Further Step Towards Understanding Adversarial Transferability*, in Oakland, 2024. (core a*)

H. Zhang, Z. Yao, **L. Y. Zhang***, S. Hu, C. Chen, A. W.-C. Liew, Z. Li, *Denial-of-Service or Fine-Grained Control: Towards Flexible Model Poisoning Attacks on Federated Learning*, in IJCAI 2023. (core a*)