ZIHAN WANG

zihan.wang@uq.edu.au +61 452-640-728 Brisbane, Australia

EDUCATION

The University of Queensland *Apr 2023 - Mar 2026 (expected)*
HDR representative *Brisbane, Australia*
Ph.D. Student at the School of Electrical Engineering and Computer Science

Research Area: *Machine Learning Security and Privacy.*
- Tackling real-world security & privacy issues of machine learning systems in a formally verifiable manner.
- Published papers in leading conferences (*IEEE S&P, ACM CCS, USENIX Security, NeurIPS, WACV*).

The University of Adelaide *Feb 2020 - Dec 2022*
Bachelor of Computer Science *(Advanced)* *Adelaide, SA*
GPA: 6.625 / 7.0

Awards:
- *IEEE S&P Travel Grant Award, 2024*
- *UQ RTP Scholarships, 2023-2026*
- *Adelaide Graduate Award, 2022*
- *Adelaide Research Scholarships, ECMS, 2021 Summer*
- *The University of Adelaide Global Citizens Scholarship, 2020-2022*

EXPERIENCE

CSIRO's Data61 *Oct 2022 - Apr 2023*
Visiting Scientist, Contract *Adelaide, Australia*
Research Area: *Machine Learning Security and Privacy.*

ECMS, University of Adelaide *July 2021 - Sep 2022*
Research Assistant *Adelaide, Australia*
Research Area: *Machine learning. Computer Vision.*
- Published my first paper as an undergraduate at *NeurIPS'22* (co-first authored).

PUBLICATIONS

Data Hiding With Deep Learning: *IEEE TCSS (JCR Q1)*
A Survey Unifying Digital Watermarking and Steganography
Zihan Wang, Olivia Byrnes, Hu Wang, Ruoxi Sun, Congbo Ma, Huaming Chen, Qi Wu, Minhui Xue.

CORELOCKER: Neuron-level Usage Control *IEEE S&P'24 (**Big Four**, A*)*
Zihan Wang, Zhongkui Ma, Xinguo Feng, Ruoxi Sun, Hu Wang, Minhui Xue, Guangdong Bai.

Being Transparent is Merely the Beginning: *USENIX Security'24 (**Big Four**, A*)*
Enforcing Purpose Limitation with Polynomial Approximation
Shuofeng Liu, Zihan Wang, Minhui Xue, Long Wang, Yuanchao Zhang, Guangdong Bai.

Uncovering Gradient Inversion Risks in Practical Language Model Training *ACM CCS'24 (**Big Four**, A*)*
Xinguo Feng, Zhongkui Ma, Zihan Wang, Chegne Eu Joe, Mengyao Ma, Alsharif Abuadbba, Guangdong Bai.

BPKD: Boundary Privileged Knowledge Distillation For Semantic Segmentation *WACV'24 (A)*
Liyang Liu, Zihan Wang, Minh Hieu Phan, Bowen Zhang, Jinchao Ge, Yifan Liu.

M^{4}I: Multi-modal Models Membership Inference *NeurIPS'22 (A*)*
Pingyi Hu, Zihan Wang*, Ruoxi Sun, Hu Wang, Minhui Xue.*

INVITED TALKS

Neuron-level Usage Control for AI Models *May 2024*
School of Computing, National University of Singapore (NUS)

PROJECTS

Urban-Sense Semantic Segmentation *May 2022- Jul 2022*
Developer, Coursework *University of Adelaide*
- **#1 Ranking** in Computer Vision course competition. Work highly endorsed by the course coordinator Dr. Yifan Liu.
- Provided a terrific solution that satisfies both efficiency and accuracy criteria to the given road segmentation task.

COVID-19 Contact Tracing Application *Mar 2021- Jul 2021*
Developer, Coursework *University of Adelaide*
- Lead developer in team effort. Reviewed, improved and integrated others' contributions.
- Front Page Design: Built frontend based on Vue.js and JavaScript.

Student Management System *Aug 2020- Nov 2020*
Developer, Coursework *University of Adelaide*
- Project Development: Implemented different system design techniques and object-oriented programming skills using C++; enabled data stores in the MySQL database and to interact with the application by ORM framework.

SKILLS

Languages: *C++, C, Java, Python, JavaScript, SQL*

Frameworks: *Torch, Django, Spring, Google Test, Vue.js*

Tools: *Git, Docker, Linux*

EXTRA-CURRICULAR ACTIVITIES

Academic Tutor
Tutoring at the University of Adelaide and other societies/clubs. Provided guidance, resources and lessons to students. Established excellent verbal and written communications. Specialized in first and second-year Computer Science.

Australian Red Cross COVID-19 Food Relief Program
Coordinator of AR International Group partnership with Australian Red Cross COVID-19 Food relief program.

Australia National Day Art Competition 2022
Photograph the submitted art pieces and prepare them for the showcase. Exhibition set up.

REFEREE

Guangdong Bai
Associate Professor School of ITEE
The University of Queensland Australia, Brisbane, Australia
E. g.bai@uq.edu.au
T. +61 4 6889 7516

Jason Xue
Senior Research Scientist at CSIRO's Data61
CSIRO's Data61, Sydney, Australia
E. minhuixue@gmail.com
T. +61 4 2037 8228

Sally-Ann Selway
Course Coordinator at the University of Adelaide
The University of Adelaide, SA 5000, Adelaide, Australia
E. sally.selway@adelaide.edu.au
T. +61 4 0880 8434

Keith Jin
Director of Australia Eye Media
Australia Eye Media PTY LTD, SA 5000, Adelaide, Australia
E. keith@australiaeyemedia.com.au
T. +61 4 1150 6680