Xin Zhang

Personal website amanda4zx.github.io
LinkedIn linkedin.com/in/xin-zhang-amanda

Research Interests

My research interests are in the intersection of cybersecurity, formal verification and programming languages. I hope to formally verify the security properties of real-life programs, ideally executable code, so we can be confident that the critical code we depend on satisfies the security specifications. I believe in the power of security by design, and programming language theory, supported by rigorous mathematical foundations, is a promising way towards the goal. I hope to study how to represent programs and specifications at different levels of abstraction such that the representations can express meaningful properties and are still amenable to computer-aided formal verification.

Education

PhD student in Electrical Engineering and Computer Science Department 2023 - Present
Massachusetts Institute of Technology, United States
Area of research: Programming Languages and Formal Verification
Advisor: Adam Chlipala

Bachelor of Arts in Computer Science 2019 - 2022
University of Oxford, United Kingdom
First Class Honours
Cohort ranking: 1/43

Research Experience

Research Engineer in Cybersecurity 2022 - 2023
Agency for Science, Technology and Research, Singapore
Supervisors: Khin Mi Mi Aung, Chao Jin
I participated in a project that uses homomorphic encryption (HE) to securely perform the design of experiments (DOE) process in a collaborative setting and presented the work at the 5th HomomorphicEncryption.org Standards Workshop. Collaborating with a colleague, I developed a Python library for compressing artificial neural networks so that the model inference has a smaller multiplicative depth, which matters when the computation is in HE. Moreover, I worked on a project that applies HE to machine learning for privacy-preserving fake image detection.

Final-Year Project in Robustness Evaluation of Attention Neural Networks 2021 - 2022
University of Oxford, United Kingdom
Supervisor: Marta Kwiatkowska
I trained neural network models with attention mechanisms based on existing literature and evaluated their robustness. I found evidence suggesting that attention neural networks may not be more robust than models without attention mechanisms for image classification.

Summer Attachment in Lattice-Based Cryptography 2021
Agency for Science, Technology and Research, Singapore

Supervisors: Khin Mi Mi Aung, Benjamin Hong Meng Tan
I learnt about the mathematical problems underlying lattice-based cryptography, studied a paper on lattice-based signatures and gave a presentation on the topic.

Research Attachment in Computational Biology 2017 - 2018
Agency for Science, Technology and Research, Singapore
Supervisors: Zheng Yang Chin, Kai Keng Ang
I designed and conducted experiments to collect electroencephalogram (EEG) signals from subjects while the subjects performed mental arithmetic. Using the data, I trained a machine learning model to distinguish between different mental arithmetic difficulty levels based on the EEG signals.

Achievements and Awards

National Science Scholarship (BS-PhD) 2019 - Present
Awarded by Agency for Science, Technology and Research, Singapore

Hoare Prize 2022
For the best overall performance in Computer Science 2022
Awarded by Department of Computer Science, University of Oxford, United Kingdom

Book Prizes 2020, 2021
For two first-class vacation essays and performance in a few assessments
Awarded by St Catherine's College, University of Oxford, United Kingdom

College Scholarship 2020
For the performance in the end-of-year assessments in Computer Science
Awarded by St Catherine's College, University of Oxford, United Kingdom

Silver Award 2018
For the paper and the poster presentation at Singapore Science and Engineering Fair 2018

Publications

- Chao Jin, Khin Mi Mi Aung, Xin Zhang. *Secure Collaborative Design of Experiments with Homomorphic Encryption.* In Proceedings of the 5th HomomorphicEncryption.org Standards Workshop. September 2022.
- Zheng Yang Chin, Xin Zhang, Chuanchu Wang, Kai Keng Ang. *EEG-based discrimination of different cognitive workload levels from mental arithmetic.* In Proceedings of the 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). July 2018.
- Xin Zhang, Zheng Yang Chin, Kai Keng Ang. *Assessing user cognitive workload from changes in electroencephalogram elicited during mental arithmetic.* In Proceedings of the Singapore Science and Engineering Fair 2018. April 2018.