Xinqiao Zhang

Joe.x.zhang10@gmail.com | (858) 625-1627 | linkedin.com/in/xinqiaozhang | San Diego, CA

SUMMARY

An adept Computer Engineering Ph.D. candidate at UCSD, specializing in trustworthy secure machine learning, privacy-preserving machine learning, adversarial machine learning, and hardware security. Demonstrates a robust record of contributions with multiple publications in prestigious conferences and journals, including NeurIPS, ICCV, CVPR, ICCAD, ACM TECS, and IEEE TIM.

EDUCATION

UC San Diego
PhD, Computer Engineering Expected June 2024
- Supervisors: Prof. Farinaz Koushanfar and Prof. Ke Huang

San Diego State University
MSEE, Electrical Engineering Dec. 2019
- Thesis title: IC Aging Prediction based on Machine Learning.

Northeastern University (CN) May 2017
BSEE, Automation
- Outstanding Student Leaders

EXPERIENCE

Check-It Analytics, San Diego, CA Aug. 2023 - Current
Founder and Chief Technology Officer (CTO)
- Selected by UCSD StartR Inclusion+ Impact Accelerator program
- Established an Multi-Language AI-driven financial information platform that amalgamates GPT-like LLM model based financial news aggregator, Fact Check validator, Fundamental data Business Analytics tool for global U.S. Stock retail investors.

Arm, Austin, TX June 2023 - Sep. 2023
Research Intern
- Conducted in-depth research on security detection using Large Language Models
- Developed and implemented a data distillation framework, achieving a significant reduction in data size without compromising efficiency.

Arm, Austin, TX May 2022 - Aug. 2022
Research Intern
- Innovated a CPU security detection method using Causality Analysis and Graph Neural Networks (GNN), enhancing detection capabilities.
- Successfully identified strong causal relationships within pair-wise datasets, bolstering data analysis accuracy.

TrojAI Project funded by IARPA, UCSD Dec. 2024
Graduate Student Researcher
- Developed innovative techniques for identifying compromised artificial intelligence models and enhancing security.
- Played a leading role in a team that achieved 2nd place among 16 competitors in a notable AI security challenge.

（* indicates equal contribution）

Class Project: Optimization and Acceleration of Deep Learning on Various Hardware Platforms May 2020

- Parameter pruning and tensor decomposition with Python Keras framework
- Used various deep learning libraries and performed input pre-processing techniques

IC Aging Prediction Based on Machine Learning, Master's thesis. Jan. 2019

- Engineered a specialized recurrent neural network tailored for advanced prediction tasks.
- Developed a unique methodology that surpassed established benchmarks in predicting aging with superior accuracy.

PUBLICATION

- S. Hussain*, P. Neekhara*, **X. Zhang**, K. Huang, J. Duarte, F. Koushanfar. FaceSigns: Semi-Fragile Watermarks for Media Authentication (ACM-TOMM) 2024
- Z. Ghodsi*, M, Javaheripi*, N. Sheybani*, **X. Zhang*,** K, Huang, & F. Koushanfar, (2023). zPROBE: Zero Peek Robustness Checks for Federated Learning**, (ICCV)** 2023
- **X. Zhang,** M. Samragh, S. Hussain, K. Huang, & F. Koushanfar. Scalable Binary Neural Network applications in Oblivious Inference**,** (ACM TECS) 2023
- Z. Ghodsi*****, M, Javaheripi*****, N. Sheybani*****, **X. Zhang*,** K, Huang, & F. Koushanfar, zPROBE: Zero Peek Robustness Checks for Federated Learning. (**NeurIPS** TSRML**)** 2022 ***[Outstanding Paper Award]***
- S. Hussain, N, Sheybani, P. Neekhara, **X. Zhang**, J. Duarte, F. Koushanfar, (2022) FastStamp: Accelerating Neural Steganography and Digital Watermarking of Images on FPGAs. In Proceedings of 2022 International Conference on Computer-Aided Design) (**ICCAD**) 2022
- N. Sheybani, **X. Zhang**, S. U. Hussain, F. Koushanfar. SenseHash: Computing on Sensor Values Mystified at the Origin. IEEE (TETC) 2022
- H. Chen, **X. Zhang**, K. Huang, F. Koushanfar. "AdaTest: Reinforcement Learning and Adaptive Sampling for On-chip Hardware Trojan Detection," ACM Transactions on Embedded Computing Systems (ACM TECS) 2022. (**TILOS 2022 Retreat Poster**)
- M. Samragh, S. Hussain, **X. Zhang**, K. Huang, & F. Koushanfar. On the Application of Binary Neural Networks in Oblivious Inference. (**CVPR** BNN) 2021
- D. Ma, **X. Zhang**, et al. "DEVoT: Dynamic Delay Modeling of Functional Units under Voltage and Temperature Variations." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (2021).
- K. Huang, **X. Zhang**, and N. Karimi, "Real-time prediction for IC aging based on machine learning. " IEEE Transactions on Instrumentation and Measurement (TIM), 2019
- K. Huang, M.T.H. Anik, **X. Zhang**, and N. Karimi, "Real-Time IC Aging Prediction via On-Chip Sensors." 2021 IEEE Computer *Society Annual Symposium on VLSI (ISVLSI). IEEE, 2021*

PATENTS

- **Xinqiao Zhang,** Farinaz Koushanfar, Shehzeen Samarah Hussain, Paarth Neekhara, and Julian McAuley "Facesigns: Semi-Fragile Neural Watermarks For Media Authentication And Countering Deepfakes" Application Serial No.63/323,470.
- **Xinqiao Zhang,** Zahra Ghodsi, Mojan Javaheripi, Nojan Sheybani, and Farinaz Koushanfar, "Zero Peek Robustness Checks for Federated Learning" Application Serial No.63/496,157.
- **Xinqiao Zhang,** Danfeng Xiang, Chao Wang, "Peasants Joy precisely pushes guiding device" CN205754440U, 2016
- **Xinqiao Zhang,** Qiang Li, Yuan Gao, "Bicycle lock based on Bluetooth," CN205621091U, 2016
- **Xinqiao Zhang,** Qiang Li, Zhenzhong Xu, "Portablely lead blind waistband" CN204766395U, 2015

（* indicates equal contribution）

SKILLS & AWARDS

- Outstanding Paper Award, NeurIPS TSRML, 2022
- Reviewer for IEEE Transactions on Dependable and Secure Computing, 2022
- DAC Young Fellow (58th Design Automation Conference), Nov. 2021
- Honorable Mention of Mathematical Contest in Modeling, Oct. 2016
- Major award of 11th Siemens Industrial Automation Design Competition, Aug. 2016
- Program language: Python, C, Verilog/System Verilog, MATLAB
- Bilingual- English (fluent) / Mandarin (native)

（* indicates equal contribution）