Xinqiao Zhang

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

SUMMARY

I am a Computer Engineering Ph.D. student at UCSD, working on adversarial machine learning, computer vision, and privacy-preserving machine learning. I have numerous publications in top conferences and journals, such as ICCV, NeurIPS, CVPR, ICCAD, ACM TECS, and IEEE TIM. I am very interested in contributing to the future of spatial computing and generative AI.

EDUCATION

UC San Diego
PhD, Computer Engineering Expected Jun. 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. Thesis advisor: Ke Huang (GPA: 3.55)

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

PUBLICATION

- **X. Zhang*,** Z. Ghodsi*, M, Javaheripi*, N. Sheybani*, 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 Inferenc**e,** (ACM TECS) 2023
- **X. Zhang*,** Z. Ghodsi*, M, Javaheripi*, N. Sheybani*, 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 TEC**) 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**) 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

EXPERIENCE

Arm, Austin, TX **Jun. 2023 - Sep. 2023**
Research Intern
- Performed research on Large Language model-based security detector

Arm, Austin, TX **May 2022 - Aug. 2022**
Research Intern
- Developed a method based on Causality analysis and GNN for CPU security detection.

TrojAI Project funded by IARPA, UCSD **Expected Dec. 2024**
Graduate Student Researcher
- Built efficient methods to detect backdoored AI models.
- Main contributor. Got 2nd out of 16 teams in the competition.

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**
- Designed a specific recurrent neural network for prediction
- Identified an approach that outperforms existing methods in terms of aging prediction accuracy

---

SKILLS & ACTIVITIES
- 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)
- Playing badminton