

Xinqiao Zhang

Joe.x.zhang10@gmail.com | (858) 625-1627 | [linkedin.com/in/xinqiaozhang](https://www.linkedin.com/in/xinqiaozhang)

SUMMARY

I am a Computer Engineering UCSD Ph.D. student working on Adversarial machine learning ([TrojAI Project](#)), Hardware Security, and Privacy-Preserving machine learning. I have many publications at conferences like NeurIPS, CVPR, ICCAD, TECS, and TECS.

EDUCATION

UC San Diego

PhD, Computer Engineering

Expected May 2024

- Supervisor: 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, (2022). zPROBE: Zero Peek Robustness Checks for Federated Learning. **NeurIPS 2022** (TSRML). (Accepted)
 - 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) (**ICCAD22**)
 - N. Sheybani, **X. Zhang**, S. U. Hussain, F. Koushanfar. SenseHash: Computing on Sensor Values Mystified at the Origin. IEEE (TETC-2021)
 - 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 (TECS) 2022. (**TILOS 2022 Retreat Poster**)
 - M. Samragh, S. Hussain, **X. Zhang**, K. Huang, & F. Koushanfar (**CVPR21**). On the Application of Binary Neural Networks in Oblivious Inference. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 4630-4639).
 - 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), vol. 68, no. 12, pp. 4756-4764, 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
-

EXPERIENCE

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 July 2023

Graduate Student Researcher

- Built efficient method 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

- 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