YUKE ZHANG

EEB 236, 3740 McClintock Ave, Los Angeles, CA 90089
Email: yukezhan@usc.edu, Group: USC.E2S2C, Website: Google scholar

RESEARCH INTERESTS

Machine learning security and privacy, Hardware security

EDUCATION

University of Southern California Los Angeles, CA, USA
Ph.D., in Electrical and Computer Engineering. Advisor: Dr. Peter A. Beerel 2018-2024 (Expected)

Dalhousie University Halifax, NS, Canada
M.A.Sc. in Electrical and Computer Engineering. Advisor: Dr. Kamal El-Sankary 2014-2016

Beijing University of Posts and Telecommunications Beijing, China
B.E., in Electrical Engineering 2010-2014

HONORS

2023 USC MHI Scholar
2023 DAC Young Fellow
2023-2024 USC Annenberg Endowed Fellowship
2022 Qualcomm Innovation Fellowship Finalist
2021-2022 WiSE Qualcomm Top-Off Award
2020 SSCS WiC Rising Star
Student Travel Grant: DAC 2023, HOST 2022, ISSCC 2020, CICC 2020
2015 Faculty Scholarship (Dalhousie University)
2010 & 2011 Leadership Award (Twice @ BUPT)

PUBLICATIONS

[UR=Under review, *=Equal contribution, †= student I mentored]

[18 UR] D. Chen, Shiduo Li†, **Y. Zhang**, P. A. Beerel, DIA: Diffusion Based Inverse Network Attack on Collaborative Inference.

[17 UR] C. Li*†, D. Chen*, **Y. Zhang***, P. A. Beerel, Mitigate Replication and Copying in Diffusiong Models with Generalized Caption and Dual Fusion Enhancement, submitted to ICASSP 2024.

[16] **Y. Zhang***, D. Chen*, S. Kundu*, C. Cheng†, P. A. Beerel, SAL-ViT: Towards Latency Efficient Private Inference on ViT using Selective Attention Search with a Learnable Softmax Approximation, ICCV 2023.

[15] D. Chen*, **Y. Zhang*,** S. Kundu*, C. Cheng†, P. A. Beerel, RNA-ViT: Reduced-Dimension Approximate Normalized Attention Vision Transformers for Latency Efficient Private Inference, accepted at ICCAD 2023.

[14] **Y. Zhang**, D. Chen, S. Kundu, H. Liu†, R. Peng†, P. A. Beerel, C2PI: An Efficient Crypto-Clear Two-Party Neural Network Private Inference, accepted at DAC 2023.

[13] S. Kundu, **Y. Zhang**, D. Chen, P. A. Beerel, Making Models Shallow Again: Jointly Learning to Reduce Non-Linearity and Depth for Latency-Efficient Private Inference, accepted at CVPR workshop (ECV) 2023.

[12] Y. Hu, **Y. Zhang**, K. Yang, D. Chen, P. A. Beerel, P. Nuzzo, On the Security of Sequential Logic Locking Against Oracle-Guided Attacks, accepted at TCAD-I.

[11] S. Kundu, S. Lu, **Y. Zhang**, J. Liu, P. A. Beerel, SENet: Towards Secure and Efficient Private Inference via Automated Non-Linearity Trimmed Network, accepted at ICLR 2023.

[10] D. Chen, X. Zhou, Y. Hu, **Y. Zhang**, K. Yang, A. Rittenbach, P. Nuzzo, and P. A. Beerel, Unraveling Latch Locking Using Machine Learning, Boolean Analysis, and ILP, accepted at ISQED 2023.

[9] **Y. Zhang***, Y. Hu*, P. Nuzzo, P. A. Beerel, TriLock: IC Protection with Tunable Corruptibility and Resilience to SAT and Removal Attacks, DATE 2022.

[8] Y. Hu*, **Y. Zhang***, K. Yang, D. Chen, P. A. Beerel, P. Nuzzo, Fun-SAT: Functional Corruptibility-Guided SAT-Based Attack on Sequential Logic Encryption, Int. Symp. Hardware Oriented Security and Trust (HOST), 2021.

[7] D. El-Damak, P. Garcha, M. R. Abdelhamid, and **Y. Zhang**, Circuit Implementation Using Emerging Technologies, IEEE SSCS Magazine, Fall Issue, 2021.

[6] **Y. Zhang**, D. El-Damak, A Reconfigurable Passive Switched-Capacitor Multiply-and-Accumulate Unit for Approximate Computing, MWSCAS, Aug. 2020.

[5] C. Y. Ko, C. Chen, Z. He, **Y. Zhang**, K. Batselier, and N. Wong, Model Compression and Inference Speedup of Sum–Product Networks on Tensor Trains, IEEE TNNLS, Sep. 2019.

[4] **Y. Zhang**, C. Y. Ko, C. Chen, K. Bastelier, N. Wong, Sparse Tensor Network System Identification for Nonlinear Circuit Macromodeling. 2018 IEEE 14th International Conference on Solid-State and Integrated Circuit Technology. (Invited)

[3] **Y. Zhang**, K. El-Sankary, J. Zhou, A Blind Digital Background Calibration for VCO-based ADC, Analog Integrated Circuits and Signal Processing, vol 97, no.2, pp.387-394, Nov. 2018.

[2] **Y. Zhang**, K. El-Sankary, Offset-Injection Digital Background Calibration for VCO-based ADC, Analog Integrated Circuits and Signal Processing, vol. 92, no.3, pp.501-506, Jul. 2017.

[1] **Y. Zhang**, K. El-Sankary, Orthogonal Polynomials Nonlinearity Compensation for a digital VCO-based ADC, Electronics Letters, vol 52, no.11, pp 915-917, May 2016.

RESEARCH EXPERIENCE

Research Assistant, USC. (Advisor: Dr. Peter A. Beerel) Aug. 2020-Present

Private inference

- C2PI: a private inference framework yields less computational and communicational costs.
- SAL-ViT: a private-inference-friendly framework for vision transformers.

Hardware security

- TriLock: a sequential logic locking method achieving high resilience to SAT-based attack and removal attack, and tunable functional corruptibility.
- Fun-SAT: a functional corruptibility guided SAT attack for sequential logic locking.

Mixed-signal computing (Advisor: Dr. Dina El-Damak) Aug. 2018- Jul. 2020

- MACU**:** a reconfigurable passive switched-capacitor multiplication-and-accumulation unit.

Research Assistant, University of Hong Kong (Advisor: Dr. Ngai Wong) Mar. 2018 - Jul. 2018

System identification and tensor computation

- Sparse tensor network system identification for circuit macro-modeling.

MASc., Dalhousie University (Advisor: Dr. Kamal El-Sankary) Sep. 2014 - Dec. 2016

Analog to Digital Converter

- Digital calibration for voltage-controlled-oscillator (VCO)-based ADC.

Research Assistant, Tsinghua University (Advisor: Dr. Fei Qiao) Jun. 2013 - Jan. 2014

Energy harvesting

WORKING EXPERIENCE

Software engineer, CIeNET, Beijing, China Jul. 2017- Feb. 2018

TEACHING ASSISTANTSHIP

EE 552 Asynchronous VLSI Design, USC, Spring 2023
EE 326 Essentials of electrical engineering, USC Spring 2018
ECED 2200 Digital Circuit, Dalhousie University Winter 2016
ECED 4260 IC design and fabrication, Dalhousie University Fall 2015
ECED 3202 Analog Electronics, Dalhousie University Summer 2015
Part-time Tutor, Dalhousie University Fall 2014

Tutored 4 courses including **ECED 2000** (electric circuits), **PHYC 1190** (physics), **ENGM 1081**(computer programming) and **ENGM 2032** (Applied probability and statistics).

MENTORSHIP

Ruiheng Peng (2022 Summer – 2022 Fall, USC master student, @Sumsung)
Haomei Liu (2022 Summer – 2022 Fall, USC master student, @TSMC)
Chenghao Li (2023 Spring – 2023 Fall, USC master student)
Shiduo Li (2023 Summer, Tsinghua undergraduate student)
Divya Reddy (2023 Summer – 2023 Fall, USC master student)

COMMUNITY SERVICES

Conference Reviewer: ICLR 2024, NeurIPS 2023, IJCNN 2023, ASYNC 2021, CICC 2021,
Journal Review: TCAS-I, Analog Integrated Circuits and Signal Processing

OUTREACH

WEE (Women in Electrical and computer Engineering), USC, Organizer Nov. 2023-present

- Propose and organize events for women Ph.D. students to connect with each other and share research
- Propose and organize panels with faculty and mentorship events with upperclassmen

PROPOSAL DEVELOPMENT EXPERIENCE

- Proposals I initiated, shaped the research vision, and played the lead role in writing.
  Amazon Research Award 2024 (Under review): Efficient Private Inference for Protecting and Preserving Data Privacy in the Cloud

- Proposals I wrote. Despite not being accepted, I like them.
  Amazon-USC Research Award 2023: Accelerating Privacy-Preserving Machine Learning Inference
  Qualcomm Innovation Fellowship (Finalist): Algorithm-Hardware Co-Design for Securing the Chip and the Data on the Chip
  DARPA Seedling 2022: Algorithm-Hardware Co-Design for Efficient Private Inference
  SRC 2022: An Efficient, Secure, and Privacy-Preserving ML Inference Accelerator

REFEREE

Dr. Peter A. Beerel
Email: pabeerel@usc.edu

Dr. Pierluigi Nuzzo
Email: nuzzo@usc.edu

Dr. Stephen P. Crago
Email: crago@isi.edu