Kaixin Yang

kaixinya@usc.edu · +1 (213) 284-6958

EDUCATION

Ph.D. student in Computer Engineering 2019 – Present

Viterbi School of Electrical and Computer Engineering, University of Southern California Los Angeles, CA, U.S.

M.S. in Electrical Engineering 2019 – 2021

Viterbi School of Electrical and Computer Engineering, University of Southern California Los Angeles, CA, U.S.

B.S. in Electronic and Information Science and Technology 2015 – 2019

School of Electronics Engineering and Computer Science, Peking University Beijing, China

EXPERIENCE

Research Assistant, University of Southern California Aug 2019 – Present

Advisor: Prof. Pierluigi Nuzzo

1. Trustworthy Hardware Design Exploration and Analysis
   - Developed models and metrics to evaluate security threats and information leakage in hardware design.
   - Helped build a design space exploration tool to provide optimized solutions in terms of information leakage.
   - Integrating the security metrics into the general synthesis flow.
2. Deep Learning-Based Circuit Reverse Engineering
   - Developed a GNN-based technique to distinguish between registers for control logic and data path.
   - Further rectified the prediction using graph algorithms.
   - Developing a defense method against illegal reverse engineering by reducing structural information leakage.

Graduate Technical Intern, Intel Corporation May 2024 – Present

- Worked on an Intel asynchronous Bitcoin mining design.
- Created detailed technical documents, including mining algorithms, design implementation, and optimizations.
- Helped convert the CAST design to a Verilog design.

TEACHING AND MENTORING

Teaching Assistant for EE577a: VLSI System Design, USC Spring 2022

Instructors: Prof. Akhilesh Jaiswal, Prof. Sandeep Gupta, and Dr. Sridhar Narayanan

Teaching Assistant for EE477L: MOS VLSI Circuit Design, USC Fall 2021

Instructor: Prof. Massoud Pedram

Teaching Assistant for Practice on Programming, PKU Spring 2019

Instructor: Prof. Na Yi

Mentor for EE581: Mathematical Foundations for System Design, USC Spring 2024, Fall 2022, Fall 2021

Instructor: Prof. Pierluigi Nuzzo

Mentor for Viterbi SHINE Program, USC Summer 2023, Summer 2022

2023: GNN-Enabled Attack Prediction on Locked Circuits (Mentees: Sean Ozalpasan, Steven Shi)

2022: State Register Identification for Circuit Reverse Engineering (Mentee: Aidan Wong)

Mentor for Viterbi Summer Institute, USC Summer 2023

Machine Learing-Enabled Attack on Logic Locking (Mentees: Olivia Quintana, Nyla Smith)

PUBLICATIONS

Book Chapter

1. Hu, Y., **Yang, K.**, Nazarian, S., Nuzzo, P., "SANSCrypt: Sporadic-Authentication-Based Sequential Logic Encryption". VLSI-SoC: Design Trends, Springer, 2021.

Journal Paper

1. Hu, Y., Zhang, Y., **Yang, K.**, Chen, D., Beerel, P., Nuzzo, P., "On the Security of Sequential Logic Locking Against Oracle-Guided Attacks". IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 2023.

Conference Papers

1. Hu, Y., **Yang, K.**, Chowdhury, S., Nuzzo, P., "DECOR: Enhancing Logic Locking Against Machine Learning-Based Attacks". International Symposium on Quality Electronic Design (ISQED), 2024.
2. Chowdhury, S., **Yang, K.**, Nuzzo, P., "Similarity-Based Logic Locking Against Machine Learning Attacks". Design Automation Conference (DAC), 2023.
3. Chen, D., Zhou, X., Hu, Y., **Zhang, Y.**, Yang, K., Beerel, P., Nuzzo, P., "Unraveling Latch Locking Using Machine Learning, Boolean Analysis, and ILP". International Symposium on Quality Electronic Design (ISQED), 2023.
4. Chowdhury, S., **Yang, K.**, Nuzzo, P., "ReIGNN: State Register Identification Using Graph Neural Networks for Circuit Reverse Engineering". International Conference on Computer-Aided Design (ICCAD), 2021.
5. Hu, Y., Zhang, Y., **Yang, K.**, Chen, D., Beerel, P., Nuzzo, P., "Fun-SAT: Functional Corruptibility-Guided SAT-Based Attack on Sequential Logic Encryption". IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2021.
6. Hu, Y., **Yang, K.**, Chowdhury, S. and Nuzzo, P., "Risk-Aware Cost-Effective Design Methodology for Integrated Circuit Locking". Design, Automation and Test in Europe Conference (DATE), 2021.
7. Hu, Y., **Yang, K.**, Nazarian, S. and Nuzzo, P., "SANSCrypt: A Sporadic-Authentication-Based Sequential Logic Encryption Scheme". Conference on Very Large Scale Integration (VLSI-SoC), 2020.

HONORS AND AWARDS

2022 59th Design Automation Conference Young Fellows
2019 Annenberg Fellowship
2018 Excellent Presentation in the sixth Peking University Young Scientists Symposium on Informatics
2018 Third prize in the 2018 Intel Undergraduate Electronic Design Contest

SKILLS

Programming Languages: Python, C++, C, Modula-3
Hardware Design Languages: Verilog, SystemVerilog, Caltech Asynchronous Synthesis Tools (CAST)
Scripting Languages: Python, TCL, Linux Shell
Softwares: Synopsys (Design Compiler, VCS), Cadence (Virtuoso, Innovus), MATLAB, LaTeX
Languages: Chinese(Native), English(Proficient)