Yinghua Hu

University of Southern California
EEB 337, 3740 McClintock Avenue, Los Angeles, CA 90089, United States
yinghuah@usc.edu · yinghuah.github.io

PRINCIPAL INTERESTS

Hardware security and trust, supply chain security, cryptography, computer-aided design, formal verification, and logic locking.

ACADEMIC BACKGROUND

University of Southern California — **Los Angeles, CA**
Ph.D. in Electrical Engineering — 2017 - Dec. 2022 (expected)

University of Southern California — **Los Angeles, CA**
M.S. in Electrical Engineering — 2017 - 2019

Nankai University — **Tianjin, China**
B.S. in Electrical Engineering — 2013 - 2017

PROFESSIONAL EXPERIENCE

Security Research Intern — May 2022 - present
Intel Corporation, Hillsboro, OR

- Working in the Client Computing Group (CCG) Security Assurance and Research team.
- Developing hardware root-of-trust solutions for next-generation Intel security processors.

Research Assistant — Aug. 2017 - present
University of Southern California, Los Angeles, CA

- Conducted research on hardware security solutions for intellectual property (IP) protection against threats coming from the integrated circuit (IC) supply chain, including the design and formal analysis of circuit obfuscation methods to prevent IC reverse engineering.
- Published 10+ research papers [link] in top-tier conferences and journals in the field of hardware security and electronic design automation.
- Received government research funding from the Air Force Research Laboratory (AFRL) and the Defense Advanced Research Projects Agency (DARPA).

Software Engineering Intern — May 2021 - Aug. 2021
Synopsys Inc., Mountain View, CA

- Worked on improving DSO.ai [link], a Synopsys AI application for chip design.
- Developed and debugged new features to incorporate previous design information and its optimal solution to the AI model, allowing DSO.ai to further reduce the time to results for new and similar designs.
- Built a user interface to visualize design similarities among a number of customers' designs, which helped the team efficiently analyze the performance of different similarity metrics and choose the optimal one.

Teaching Assistant — Jan. 2020 - May 2020
University of Southern California, Los Angeles, CA

- Course: EE577A (VLSI System Design), Spring 2020.

- Held weekly discussions and guided students on fully customized VLSI system design using Cadence tools.
- Received the highest student evaluation score for the year and Honorable Mention for Charles L. Weber Memorial Outstanding Teaching Assistant at USC ECE department.

Ph.D. Mentor Summer 2018, 2019, and 2020
University of Southern California, Los Angeles, CA

- Mentored three local high school students to complete a hardware security-related project during SHINE [link], a K-12 outreach program at USC.
- Helped mentees prepare for relevant skill sets for college entrance and develop interests in research in engineering.

AWARDS AND HONORS

- Young Fellow, Design Automation Conference, July 2022 & July 2020.
- Charles L. Weber Memorial Outstanding Teaching Assistant Award (Honorable Mention), USC, Apr. 2021.
- Outstanding Graduates Award, Nankai University, May 2017.
- Samsung Scholarship, Samsung Electronics, Dec. 2015.
- National Scholarship, Chinese Ministry of Education, Dec. 2014.

SELECTED PUBLICATIONS

Book Chapters

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

Conference Papers

9. Y. Zhang*, **Y. Hu***, P. Nuzzo, P. A. Beerel, **"TriLock: IC Protection with Tunable Corruptibility and Resilience to SAT and Removal Attacks"**, *IEEE Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Mar. 2022. [link]
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"**, *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Dec. 2021. [link] [code]
7. S. Dutta Chowdhury, G. Zhang, **Y. Hu**, P. Nuzzo, **"Enhancing SAT-Attack Resiliency and Cost-Effectiveness of Reconfigurable-Logic-Based Circuit Obfuscation"**, *IEEE International Symposium on Circuits and Systems (ISCAS)*, May. 2021. [link]
6. **Y. Hu**, K. Yang, S. Dutta Chowdhury, P. Nuzzo, **"Risk-Aware Cost-Effective Design Methodology for Integrated Circuit Locking"**, *IEEE Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Feb. 2021. [link]
5. **Y. Hu**, K. Yang, S. Nazarian, P. Nuzzo, **"SANSCrypt: A Sporadic-Authentication-Based Sequential Logic Encryption Scheme"**, *IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, Oct. 2020. [link]
4. V. Menon, G. Kolhe, J. Fifty, A. G. Schmidt, J. Monson, M. French, **Y. Hu**, P. A. Beerel, P. Nuzzo, **"Logic Obfuscation: Modeling Attack Resiliency"**, *GOMACTech*, Mar. 2020.

3. **Y. Hu**, V. Venugopalan, A. Schmidt, J. Monson, M. French, P. Nuzzo, **"Security-driven Metrics and Models for Efficient Evaluation of Logic Encryption Schemes"**, *ACM-IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE)*, Oct. 2019. [link]
2. V. Venugopalan, G. Kolhe, A. Schmidt, J. Monson, M. French, **Y. Hu**, P. A. Beerel, P. Nuzzo, **"System-Level Framework for Logic Obfuscation with Quantified Metrics for Evaluation"**, *IEEE Secure Development Conference (SecDev)*, Sept. 2019. [link]
1. V. Venugopalan, G. Kolhe, A. Schmidt, J. Monson, M. French, **Y. Hu**, P. A. Beerel, P. Nuzzo, **"Quantifying Security and Overheads for Obfuscation of Integrated Circuits"**, *GOMACTech*, Mar. 2019. [link]

Workshops, Posters, and Demos

2. **Y. Hu**, S. Dutta Chowdhury, K. Yang, M. Munir, J. Bollareddy, P. Nuzzo, **"Circumventing Machine Learning-Based Attacks to Logic Locking"**, *Design Automation Conference (DAC)*, July 2022. [link]
1. V. Venugopalan, G. Kolhe, A. Schmidt, J. Monson, M. French, **Y. Hu**, P. A. Beerel, P. Nuzzo, **"MIRAGE: A System-Level Framework for Inserting and Evaluating Logic Obfuscation"**, *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2019.