

Yunqi He

<http://actasclovn.github.io>

Email : [yunqi.he@u.northwestern.edu](mailto:yunqi.he@u.northwestern.edu)

Mobile : +1-773-290-0801

## Education

### Northwestern University

*Ph.D. in Computer Engineering, advised by Prof. Hai Zhou*

**Evanston, IL**

*Jan. 2022 – Jun. 2026(estimated)*

### Northwestern University

*M.S. in Computer Engineering*

**Evanston, IL**

*Sept. 2019 – Dec. 2021*

### Peking University

*B.S. in Computer Science*

**Beijing, China**

*Sept. 2013 – Jun. 2017*

## Research Interest

**Machine Learning Systems:** Designing and verifying reliable ML systems, with emphasis on robustness verification and security for various kinds of deep neural networks

**Multimodal Learning:** Developing robust architectures for integrating multiple data modalities (vision, text, metadata) with a particular focus on probabilistic frameworks and Bayesian methods

## Relevant Coursework

AI & ML Cores: Machine Learning, Artificial Intelligence, Probability Theory & Statistics, Random Processes

Computing: Massively Parallel Prog w/CUDA, Multicore Concurrent Programming, Design & Analysis of Algorithms

Applications: Information Retrieval, Biometrics, Human-Computer Interaction

Math Foundations: Linear Algebra, Set Theory & Graph Theory, Algebraic Structure & Combinatorial Mathematics

## Selected Projects

(<sup>M</sup> - Machine Learning | <sup>H</sup> - Hardware Design | <sup>F</sup> - Formal Verification)

<sup>M</sup> **Multimodal Automatic Skin Disease Diagnosis [1] [2] | Northwestern University** *May. 2021 - June. 2024*

- Developed an innovative multimodal Bayesian network architecture integrating deep learning with clinical metadata for skin disease diagnosis.
- Optimized network topology through semantic analysis, achieving efficient node distribution and connection reduction.
- Implemented a two-stage training pipeline for seamless integration of neural networks and Bayesian networks.
- Achieved 19.3% improvement in diagnostic accuracy compared to pure deep learning methods on PAD-UFES-20 and SkinCon benchmark datasets.

<sup>MF</sup> **Robustness Verification for Deep Neural Networks [3] [4] | Northwestern University** *Feb. 2023 - Present*

- Proposed a systematic I/O attack combining algebraic and learning-based approaches on DNNs protected by a logic locking scheme.
- Utilized probabilistic methods, abstract interpretation, and abstraction refinement to find adversarial examples or to certify the robustness of DNNs.
- Contribution: Designed the learning-based attack.
- Ongoing work: Conducting attack and defense research on logical encryption for more complex models including Transformer, Diffusion, etc., to provide a theoretical basis for applications such as protecting private LLM parameters.

<sup>F</sup> **Principles of Symbolic Model Checking [5] | Northwestern University** *Mar. 2022 - Nov. 2022*

- Model checking verifies whether a model satisfies the designated safety and liveness properties.
- Proposed an efficient algorithm to check whether two systems are modulo equivalent for arbitrary timing differences.
- Developed a tool to check the correctness of design transformations such as high-level synthesis and RTL optimization.
- Contribution: Designed and conducted experiments to compare our tool with existing commercial tools, including Cadence Jasper SEC, Mentor Catapult SLEC, and Synopsys HECTOR.

<sup>HF</sup> **Hardware IP Protection via Logic Encryption [6] [7] | Northwestern University** *May. 2021 - Present*

- Logic encryption embeds binary keys to integrated circuits to protect intellectual properties and thwart attacks.
- Employed logic synthesis and obfuscation to achieve indistinguishable encryption and to minimize the overheads.
- Utilized a behavioral model to launch oracle-guided I/O attacks on logic encryption.
- Contribution: Verified the obfuscation in aig level. Evaluated the overhead of our approach using Innovus and Genus.
- Ongoing work: Designing a new eFPGA redaction solution to make industrial applications of logics locking possible.

- <sup>H</sup> **GRT Sensing v1.0** | *Peking University* *June, 2017 - Jan, 2018*
- Modified the code of GRT 2.0(an FPGA-based software defined radio Platform) to derive an additional status output from the *rx\_channel\_estimation* module of the physical layer and export CSI.
  - Wrote a serial port receiving program for the exported output to visually display the changes in CSI near the antenna in real time, laying the foundation for wireless perception.

- <sup>MH</sup> **FPGA-based CNN Accelerator** | *Peking University* *April, 2016*
- Mapped the specific calculation process of neural network to FPGA hardware with Xilinx Vivado HLS tool.
  - Made use of compiler instructions to perform array partition and loop unrolling on the calculation process to significantly improve the calculation speed of the generated hardware.

## Work Experience

- Cadence Design Systems** | *Research & Design Intern* *Jun. 2024 - Sept. 2024*
- Participated in the next generation development of the company's star product Palladium emulator.
  - Researched GPU-accelerated circuit placement algorithms and improved them based on actual industrial benchmarks.
  - Tried to replace the classic algorithms of existing products and provide an order of magnitude of compile time boost.
- Beijing Yidian Science and Technology Co., Ltd** | *Project Manager* *Oct. 2017 - June. 2019*
- Participated in the preparation of a start-up company.
  - Participated in the design of a multi-sided platform to connect online diagnosis and treatment and offline resources
  - Completed functions of online inquiry, hospital searching, online registration, and after-treatment services

## Technical Skills

**Languages:** Python, C/C++, Java, CUDA, Verilog/VHDL, MySQL, Assembly, Rust

**Tools:** Linux, AWS, PyTorch, Tensorflow, Matlab

**Teaching Assistant:** Fundamentals of Blockchains and Decentralization (Fall 2021), Fundamentals of Computer System Software (Winter 2023), Advanced Digital Design (Spring 2023), Introduction to Computer Engineering (Winter 2024)

## Awards

- Northwestern University Ph.D. Fellowship (2022)
- 3rd Prize, ACM Programming Contest of Peking University (2015)
- "Excellent Graduation Design" (top 5%) of EECS Department, Peking University (2017)

## Publications

- [1] **Yunqi He**, Jiahe Liu, Linglong Cai, Taimei Cui, You Li, and Hai Zhou. Multimodal bayesian networks for automatic skin disease diagnosis. In *International Conference on Bioinformatics and Biomedicine (BIBM)*. IEEE, 2024.
- [2] **Yunqi He**, Linglong Cai, Taimei Cui, You Li, and Hai Zhou. A combination of dnn and bn for automatic skin disease diagnosis. In *International Symposium on Biomedical Imaging (ISBI)*. IEEE, 2023.
- [3] You Li, Guannan Zhao, **Yunqi He**, and Hai Zhou. Evaluating the security of logic locking on deep neural networks. In *Design Automation Conference (DAC)*. ACM/IEEE, 2024.
- [4] You Li, Guannan Zhao, **Yunqi He**, and Hai Zhou. Certifying global robustness for deep neural networks. *arXiv preprint arXiv:2405.20556*, 2024.
- [5] You Li, Guannan Zhao, **Yunqi He**, and Hai Zhou. Se3: Sequential equivalence checking for non-cycle-accurate design transformations. In *Design Automation Conference (DAC)*. ACM/IEEE, 2023.
- [6] You Li, Guannan Zhao, **Yunqi He**, and Hai Zhou. De2: Sat-based sequential logic decryption with a functional description. In *Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2025.
- [7] You Li, Guannan Zhao, **Yunqi He**, and Hai Zhou. Obfuslock: An efficient obfuscated locking framework for circuit ip protection. In *Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2023.