钟有为 Youwei Zhong

youwei.zhong@yale.edu | https://ywzh.org/

PhD student at Yale University | New Haven, Connecticut, US

Education

PhD student in Computer Science — New Haven, Connecticut, US
Yale University — August 2025 – May 2030 (expected)

Member of the **Rigorous Software Engineering (ROSE)** group led by Prof. Ruzica Piskac

Bachelor of Engineering in Computer Science and Technology — Shanghai, China
Shanghai Jiao Tong University — September 2021 – June 2025
GPA: 3.91/4.3 (core courses)

Graduated as a member of the first **John Hopcroft Class**, an elite CS program at Zhiyuan College, Shanghai Jiao Tong University, for top 10% of students, with a focus on **Theoretical Computer Science**.

Research Interest

My research applies formal methods and cryptographic techniques to software security and trustworthy AI. I am interested in privacy-preserving verification of neural networks, and extending formal guarantees to AI agents, particularly through language-based security, sandboxing, and access-control policies for tools and data.

Publications

Certified but Private: Scalable Zero-Knowledge Proofs for Neural Network Guarantees — NeurIPS 2026
Youwei Zhong, Ben Merbaum, Timos Antonopoulos, Ning Luo, Charalampos Papamanthou, Katerina Sotiraki, Ruzica Piskac

- We present PANDA, a scalable system that uses zero-knowledge proofs (ZKPs) to prove the robustness and fairness properties of a model without revealing its private parameters, supporting neural networks 4 orders of magnitude larger than previous approaches with significantly reduced prover overhead.

A Parameterized Framework for the Formal Verification of Zero-Knowledge Virtual Machines — OOPSLA SRC 2024
Youwei Zhong (sole student author)

- Advised by Qinxiang Cao and Yuncong Hu
- **The Second Place Winner** in the undergraduate category of the Student Research Competition

Manuscripts

A Parameterized Verification Framework for the Constraint Generation Algorithms in Zero-Knowledge Virtual Machines — 2025
Youwei Zhong, Zihan Xu, Haixing He, Yuncong Hu, Xiang Xie, Qinxiang Cao

- This paper extends my OOPSLA 2024 SRC paper. We formalize the cryptographic security properties of zkVMs in the Rocq (Coq) proof assistant, including soundness, completeness, knowledge soundness, and zero-knowledge, by formalizing probabilistic programs using monads.

Research Experience

Visiting student / PhD student — New Haven, Connecticut, US
Rigorous Software Engineering (ROSE) group, Yale University — Nov 2024 – May 2025; Aug 2025 – Present
Advised by Ruzica Piskac

- Developed PANDA, a scalable system for privacy-preserving robustness certification of neural networks (paper accepted at NeurIPS 2026).
- Developed automated tools to synthesize optimized R1CS circuits.

Research internship — Remote
University of California, Santa Barbara / Riema Labs — March 2024 – October 2024
Advised by Yu Feng and Yanju Chen, in collaboration with Ranjit Jhala

- Developed prototype bug detectors by doing regular matching on the MIR of Rust programs used in Scroll zkEVM. Experimented on using LLMs to detect bugs in our benchmark.
- Developed bug finders for zero-knowledge virtual machines by synthesizing stub specifications with abstract interpretation to enable modular verification using the Flux refinement type checker.
- Developed an analyzer that translates Circom programs into C programs, which uses the KLEE symbolic execution engine to detect unconstrained zero-knowledge circuits.

Research internship — Shanghai, China
John Hopcroft Center, Shanghai Jiao Tong University — April 2023 – October 2024
Advised by Qinxiang Cao and Yuncong Hu

- Developed a parameterized framework for the formal verification of zero-knowledge virtual machines, using the Coq proof assistant. Verified the parameterized constraint generation algorithm used by zero-knowledge virtual machines. Instantiated our parameterized framework on two examples: Cairo VM and a simplified zkEVM. (paper accepted by OOPSLA 2024 SRC)
- Developed a DSL in Coq that provides a built-in field element type. Enabled symbolic execution and entailment generation in our DSL. Wrote an example of proving the correctness of a bit-decomposition program in our DSL.

Invited Talks

Certified but Private: Scalable Zero-Knowledge Proofs for Neural Network Guarantees
Fifteenth Summer School on Formal Techniques, Menlo College — May 2026

Certified but Private: Scalable Zero-Knowledge Proofs for Neural Network Guarantees
Yale Applied Cryptography Laboratory (YACL) seminar, Yale University — October 2026

Honors and Awards

2026 – Present	**Wu Tsai Institute Graduate Fellowship**, Yale University. Full stipend, tuition, and healthcare support for three years.
2024	**A-class Academic Excellence Scholarship**, Shanghai Jiao Tong University.
2024	**The 2nd Place Winner (300 USD)**, OOPSLA 2024 SRC.
2022	**Longfor Scholarship (10′000 yuan, 10 winners each year)**, Shanghai Jiao Tong University.
2024, 2023, 2022 and 2021	**Zhiyuan Honors Scholarship (5′000 yuan per year, Top 10%)**, Shanghai Jiao Tong University.
2024, 2023 and 2022	**Three Good Student of Shanghai Jiao Tong University**, Shanghai Jiao Tong University.

Academic Service

Workshop Reviewer
VeriCodeGen: AI for Verifiable Coding, NeurIPS 2026

Student Volunteer
OOPSLA/SPLASH 2024

Work Experience

Quantitative Developer — Shanghai, China
Minghong Investment — January 2024 – February 2024

- Worked in developing a high frequency trading system.
- Updated C++ system interfaces based on the RDB database format.
- Processed data from different cryptocurrency exchanges.

Teaching Experience

Graduate Teaching Fellow — New Haven, Connecticut, US
Yale University

CPSC 4540/5540: Software Analysis and Verification — Fall 2026

Teaching Assistant — Shanghai, China
Shanghai Jiao Tong University

CS 1207, Programming and Data Structure – III — Summer 2023

Miscellaneous

Community Fellow — New Haven, Connecticut, US
Yale Graduate Housing — May 2026 – Present

Graduate Affiliate — New Haven, Connecticut, US
Timothy Dwight College, Yale University — October 2025 – Present

Website Maintainer
John Class Online — December 2021 – Present

- Designed an internal class forum based on Discourse, a well-known open source discussion platform.
- Maintained the operation of the Aliyun server and the website.

Captain — Shanghai, China
Zhiyuan College Debate Team, Shanghai Jiao Tong University — July 2021 – July 2022

- Organized the recruitment of the debate team. Produced recruiting WeChat pushes.
- Lead the preparation for Freshman Cup and Union Cup. Organized team building activities.

Monitor — Shanghai, China
Monitor of Class F2103013, Shanghai Jiao Tong University — September 2022 – June 2025

- Organized team-building activities of Class F2103013
- Organized friendship-building activities across students in different years of John Hopcroft Class.

Technical Skills

Research Interests: Formal Methods | Zero-Knowledge Proofs | AI Safety
Programming Languages: Rocq (Coq) | C | C++ | Python | Rust | Dafny | Ocaml | Haskell
Machine Learning Libraries: PyTorch | scikit-learn
Coding Agents: Codex | Claude Code
Tools: Git | VSCode