Yi Cai

(878) 600-1933 *yicai@cs.umd.edu* *Homepage* *GitHub*

RESEARCH INTERESTS

I am broadly interested in the theory and practice of programming languages, especially type theory and type systems, constructive logics, formal methods, and their application in various computing systems.

EDUCATION

University of Maryland College Park, MD
Ph.D in Computer Science Aug. 2024 – Present

Carnegie Mellon University Pittsburgh, PA
M.S. in Electrical and Computer Engineering Aug. 2022 – Dec. 2023

University of Waterloo Waterloo, Canada
M.E. in Electrical and Computer Engineering Sept. 2020 – Aug. 2021

University of Electronic Science and Technology of China Chengdu, China
B.E. (First Class Honors) in Electronics and Electrical Engineering Aug. 2016 – June 2020

PUBLICATIONS

OwlC: Automatically Compiling Security Protocols to Formally Verified, Performant Implementations
Pratap Singh, Joshua Gancher, Yi Cai, Jay Bosamiya, and Bryan Parno.
In submission

RESEARCH EXPERIENCE

PLUM, University of Maryland
Advised by Prof. Milijana Surbatovich Aug. 2024 – Present

Secure Foundations Lab, Carnegie Mellon University
Advised by Prof. Bryan Parno May 2023 – Present

- Designed and implemented a verified, performant, and secure library for parser and serializer combinators in Rust that supports cryptographic constant-time parsing.
- Constructed a compiler that translates data format specifications to formally verified, performant parsers and serializers.

CyLab, Carnegie Mellon University
Advised by Prof. Limin Jia Sept. 2023 – Dec. 2023

- Implemented a type-driven, hybrid approach for secure information-flow control in WebAssembly, with a controlled declassification mechanism.

TEACHING EXPERIENCE

Teaching assistant – Language-based Security Fall 2024
Prof. Milijana Surbatovich, UMD CMSC838N

Teaching assistant – Introduction to Computer Security Fall 2023
Prof. Bryan Parno, CMU 15/18-330

- Revised assignments for software, cryptography, and web exploits, held weekly office hours, and upgraded course auto-grader infrastructure.

Teaching assistant – Introduction to Computer Systems Spring & Summer 2023
Prof. Swarun Kumar & Prof. Greg Kesden, CMU 18-213/613

- Held weekly recitations and office hours on topics including x86 assembly, caching, virtual memory, signals and exceptions, network and concurrent programming.

PROFESSIONAL EXPERIENCE

Oregon Programming Languages Summer School Eugene, OR
Participant Summer 2023

- Studied topics from proof theory, logical relations, dependent type theory to program synthesis, program analysis, and verified compilation.

Cyphercor Inc. Ottawa, Canada
Software Engineer Spet. 2021 – Spet. 2022

- Led the development of secure multi-factor authentication services for Windows Remote Desktop, Local Windows Logon, and iframe-based web integration.

HONORS

OPLSS Fellowship (Oregon Programming Languages Summer School) June 2023
James Watt Scholarship for Research Overseas Apr. 2019
Outstanding Undergraduate Students Award (UESTC, top 5%) Aug. 2018
Excellent Student Award (UESTC, top 10%) 2017-2019

SKILLS

Programming Languages
Multilingual, ranked with personal preference: Rust, Standard ML, OCaml, Haskell, λ-calculus, Typed Racket, Typescript, C0, Zig, C, C#, Go, python, Java, C++, JavaScript, MATLAB
Proof Assistants & Verification Languages
Dafny, Verus, Coq, Isabelle/HOL
Architectures
x86-64, WebAssembly, MSP430
Miscellaneous
Tree-sitter, Language Server Protocol (LSP), Yacc, Pest, Nvim, Bash, Git, LaTeX, Markdown, React, Node.js, MySQL, MongoDB, SQLite