Yanju **Chen**

CSE 3132, University of California, San Diego · 9500 Gilman Dr., La Jolla, CA 92093 USA
https://chyanju.github.io · yanju@ucsd.edu

RESEARCH INTERESTS

I develop program synthesis and verification methods in which logical reasoning and learned models complement each other, so that programs, and the AI agents that increasingly write and run them, are correct by construction, efficient at scale, and easy to use. My work falls into the following research thrusts.

Deduction-Powered Program Synthesis
Synthesis turns what a user intends into a program that provably does it. I study how deduction and learning reinforce each other, whether deduction guides learning [CAV'20] or learning guides deductive search [OOPSLA'22a], including how a synthesizer can learn from its own failed attempts [PLDI'23a], so that synthesis scales to real domains such as data science [VLDB'19, FSE'19, ASE'24], compilers [ASPLOS'22] and smart contracts [OOPSLA'22b]. The same methods apply to AI agents, whose architectures can be synthesized and improved automatically instead of being designed by hand [arXiv'26b].

Trustworthy Agentic Programming
Natural language is becoming how we ask for software and instruct agents, so whether a program does what was meant is a first-class correctness problem that formal reasoning can address. A model's output can be grounded in a program checked against the request [PLDI'22], and users, models and verifiers can supply examples [ASE'23], candidates or proofs [ASE'25]. Agent specifications are natural language; I give them a formal semantics so they can be audited [arXiv'26c, ICSE'27], tested [arXiv'26e], enforced at runtime [arXiv'26f] and used to grant authority safely [arXiv'26d], and study their supply chain [arXiv'26a].

Verified and Performant Cryptographic and Blockchain Systems
Cryptographic and blockchain systems must be fast and cannot afford mistakes, so I want them both efficient and provably correct. Synthesis-aided compilation [OOPSLA'25] and explicit circuit layout [SBC'25] optimize zero-knowledge circuits without changing their meaning, and analyses find under-constrained [PLDI'23b] or unsound [USENIX Sec'24] circuits and semantically divergent virtual machines [NDSS'27]. On chain, this gives verified protocols [CCS'26] and execution layers [ePrint'24a, ePrint'24b], contracts whose state [S&P'22], loops [ASE'20] and invariants [ASE'22] are checked before deployment, behavior-preserving optimization [OOPSLA'22b] and attack synthesis to contain live incidents [CCS'24].

EDUCATION

2023 **University of California, Santa Barbara, CA, USA**
Ph.D. in Computer Science
Committee: Yu Feng (advisor), Isil Dillig, Nadia Polikarpova, Xifeng Yan
Dissertation: Deduction-Powered Neural Program Synthesis: A Synergistic Perspective

2014 & 2017 **Sun Yat-sen University, Guangzhou, China**
B.S. & M.S. in Computer Science
Advisor: Rong Pan

APPOINTMENTS

2025 - Present **University of California, San Diego**
Postdoctoral Scholar | Host: Yufei Ding and Yu Feng

2024 - 2025 **University of California, Santa Barbara**
Postdoctoral Scholar | Host: Yu Feng and Tevfik Bultan

2022 - 2024 **Veridise Inc.**
Co-Founder & Chief Research Scientist

2019 **University of Washington**
Visiting Researcher | Mentor: Rastislav Bodik

2019 **The University of Texas at Austin**
Visiting Researcher | Mentor: Isil Dillig

2015 - 2017 **iPIN Inc.**
Research Scientist | Mentor: Rong Pan

PUBLICATIONS & MANUSCRIPTS

(+ means equal contribution)

Conference and Journal Publications

[ICSE'27] **Automated Safety Analysis for Agentic Workflows**
Yanju Chen, Ying Li, Bosi Zhang, Hanzhi Liu, Hongbo Wen, Yufei Ding, Yuan Tian, Yu Feng
Proceedings of the IEEE/ACM International Conference on Software Engineering (ICSE), 2027

[NDSS'27] **Revealing Semantic Gaps in Zero-Knowledge Virtual Machines via Obligation-Targeted Semantic Fuzzing**
Hongbo Wen, Jingyu Ke, Hanzhi Liu, Yanju Chen, Yu Feng
Proceedings of the Network and Distributed System Security (NDSS) Symposium, 2027

[CCS'26] **Thunderbolt: Fast Asynchronous Off-Chain Bitcoin Transfers**
Hongbo Wen, Hanzhi Liu, Yanju Chen, Jingyu Ke, Dahlia Malkhi, Yu Feng
Proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security (CCS), 2026

[ASE'25] **Automated Repair of OpenID Connect Programs**
Tamjid Al Rahat, Yanju Chen, Yu Feng, Yuan Tian
Proceedings of the IEEE/ACM International Conference on Automated Software Engineering (ASE), 2025

[OOPSLA'25] **Tabby: A Synthesis-Aided Compiler for High-Performance Zero-Knowledge Proof Circuits**
Junrui Liu, Jiaxin Song, Yanning Chen, Hanzhi Liu, Hongbo Wen, Luke Pearson, Yanju Chen, Yu Feng
Proceedings of the ACM on Programming Languages (OOPSLA), 2025

[ASE'24] **Refinement Types for Visualization**
Jingtao Xia + Junrui Liu, Nicholas Brown, Yanju Chen, Yu Feng
Proceedings of the IEEE/ACM International Conference on Automated Software Engineering (ASE), 2024

[CCS'24] **Foray: Towards Effective Attack Synthesis against Deep Logical Vulnerabilities in DeFi Protocols**
Hongbo Wen, Hanzhi Liu, Jiaxin Song, Yanju Chen, Wenbo Guo, Yu Feng
Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS), 2024

[USENIX Sec'24] **Practical Security Analysis of Zero-Knowledge Proof Circuits**
Hongbo Wen, Jon Stephens, Yanju Chen, Kostas Ferles, Shankara Pailoor, Kyle Charbonnet, Isil Dillig, Yu Feng
Proceedings of the 33rd USENIX Security Symposium (USENIX Security), 2024

[ASE'23] **Fast and Reliable Program Synthesis via User Interaction**
Yanju Chen, Chenglong Wang, Xinyu Wang, Osbert Bastani, Yu Feng
Proceedings of the IEEE/ACM International Conference on Automated Software Engineering (ASE), 2023

[PLDI'23b] **Automated Detection of Under-constrained Circuits in Zero-Knowledge Proofs**
Shankara Pailoor + Yanju Chen, Franklyn Wang, Clara Rodríguez, Jacob Van Geffen, Jason Morton, Michael Chu, Brian Gu, Yu Feng, Isil Dillig
Proceedings of the ACM on Programming Languages (PLDI), 2023

[PLDI'23a] **Conflict-Driven Synthesis for Layout Engines**
Junrui Liu, Yanju Chen, Eric Atkinson, Yu Feng, Rastislav Bodik
Proceedings of the ACM on Programming Languages (PLDI), 2023

[ASE'22] **Learning Contract Invariants Using Reinforcement Learning**
Junrui Liu + Yanju Chen, Bryan Tan, Isil Dillig, Yu Feng
Proceedings of the IEEE/ACM International Conference on Automated Software Engineering (ASE), 2022

[OOPSLA'22b] **Synthesis-Powered Optimization of Smart Contracts via Data Type Refactoring**
Yanju Chen + Yuepeng Wang, Maruth Goyal, James Dong, Yu Feng, Isil Dillig
Proceedings of the ACM on Programming Languages (OOPSLA), 2022

[OOPSLA'22a] **Automated Transpilation of Imperative to Functional Code Using Neural-Guided Program Synthesis**
Benjamin Mariano, Yanju Chen, Yu Feng, Greg Durrett, Isil Dillig
Proceedings of the ACM on Programming Languages (OOPSLA), 2022

[PLDI'22] **Visualization Question Answering Using Introspective Program Synthesis**
Yanju Chen, Xifeng Yan, Yu Feng
Proceedings of the ACM SIGPLAN International Conference on Programming Language Design and Implementation (PLDI), 2022
ACM SIGPLAN Distinguished Paper Award

[ASPLOS'22] **Tree Traversal Synthesis Using Domain-Specific Symbolic Compilation**
Yanju Chen, Junrui Liu, Yu Feng, Rastislav Bodik
Proceedings of the ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2022

[S&P'22] **SAILFISH: Vetting Smart Contract State-Inconsistency Bugs in Seconds**
Priyanka Bose, Dipanjan Das, Yanju Chen, Yu Feng, Christopher Kruegel, Giovanni Vigna
Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2022

[ASE'20] **Demystifying Loops in Smart Contracts**
Benjamin Mariano, Yanju Chen, Yu Feng, Shuvendu Lahiri, Isil Dillig
Proceedings of the IEEE/ACM International Conference on Automated Software Engineering (ASE), 2020

[CAV'20] **Program Synthesis Using Deduction-Guided Reinforcement Learning**
Yanju Chen, Chenglong Wang, Osbert Bastani, Isil Dillig, Yu Feng
Proceedings of the International Conference on Computer Aided Verification (CAV), 2020

[FSE'19] **Maximal Multi-Layer Specification Synthesis**
Yanju Chen, Ruben Martins, Yu Feng
Proceedings of the ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE), 2019

[VLDB'19] **TRINITY: An Extensible Synthesis Framework for Data Science**
Ruben Martins, Jia Chen, Yanju Chen, Yu Feng, Isil Dillig
Proceedings of the VLDB Endowment (VLDB), 2019

[AAAI'17] **Automatic Emphatic Information Extraction from Aligned Acoustic Data and Its Application on Sentence Compression**
Yanju Chen, Rong Pan
Proceedings of the AAAI Conference on Artificial Intelligence (AAAI), 2017

Preprints, Presentations and Others

[arXiv'26f] **VIGIL: Runtime Enforcement of Behavioral Specifications in AI Agent Skills**
Ying Li, Yanju Chen, Hongbo Wen, Bosi Zhang, Hanzhi Liu, Peiran Wang, Yu Feng, Yuan Tian
arXiv:2606.26524

[arXiv'26e] **No Attack Required: Semantic Fuzzing for Specification Violations in Agent Skills**
Ying Li, Hongbo Wen, Yanju Chen, Hanzhi Liu, Yuan Tian, Yu Feng
arXiv:2605.13044

[arXiv'26d] **Options, Not Clicks: Lattice Refinement for Consent-Driven MCP Authorization**
Ying Li, Yanju Chen, Peiran Wang, Issac Khabra, Faysal Hossain Shezan, Yu Feng, Yuan Tian
arXiv:2605.11360

[arXiv'26c] **Semia: Auditing Agent Skills via Constraint-Guided Representation Synthesis**
Hongbo Wen, Ying Li, Hanzhi Liu, Chaofan Shou, Yanju Chen, Yuan Tian, Yu Feng
arXiv:2605.00314

[arXiv'26b] **Synthesizing Multi-Agent Harnesses for Vulnerability Discovery**
Hanzhi Liu, Chaofan Shou, Xiaonan Liu, Hongbo Wen, Yanju Chen, Ryan Jingyang Fang, Yu Feng
arXiv:2604.20801

[arXiv'26a] **Your Agent Is Mine: Measuring Malicious Intermediary Attacks on the LLM Supply Chain**
Hanzhi Liu, Chaofan Shou, Hongbo Wen, Yanju Chen, Ryan Jingyang Fang, Yu Feng
arXiv:2604.08407

[SBC'25] **TESSEL: An Optimizing Compiler for Efficient Zero-Knowledge Circuits**
Junrui Liu, Jiaxin Song, Yanning Chen, Hanzhi Liu, Hongbo Wen, Yanju Chen, Yu Feng
The Science of Blockchain Conference (SBC), 2025

[VehicleSec'25] **Stateful Behavior Inference and Runtime Enforcement for Vehicle Network Security**
Achintya Desai, Ruochen Dai, Yanju Chen, Ky Ho, Austin Kee, Sophie Bulatovic, Md Shafiuzzaman, Ken (Yihang) Bai, Il Ung Jeong, David Siu, Tuba Yavuz, Tevfik Bultan
USENIX Symposium on Vehicle Security and Privacy (VehicleSec), 2025

[ePrint'24b] **Programmable Bitcoin Verification via Synthesis-Aided Lifting**
Hanzhi Liu, Jingyu Ke, Hongbo Wen, Luke Pearson, Robin Linus, Lukas George, Manish Bista, Hakan Karakuş, Domo, Junrui Liu, Yanju Chen, Yu Feng
Cryptology ePrint Archive, 2024/1768

[ePrint'24a] **Stateless and Verifiable Execution Layer for Meta-Protocols on Bitcoin**
Hongbo Wen, Hanzhi Liu, Shuyang Tang, Tianyue Li, Shuhan Cao, Domo, Yanju Chen, Yu Feng
Cryptology ePrint Archive, 2024/408

[Dissertation] **Deduction-Powered Neural Program Synthesis: A Synergistic Perspective**
Yanju Chen
University of California, Santa Barbara, 2024

ACADEMIC SERVICE

(**PC** - Program/Review Committee · **AEC** - Artifact Evaluation Committee · **ERC** - Extended Review Committee)

2027 **PC** | ACM International Conference on the Foundations of Software Engineering (FSE)
PC | International Workshop on Large Language Models for Code (LLM4Code@ICSE)
PC | USENIX Security Symposium (USENIX Security)
AEC | ACM SIGPLAN Symposium on Principles of Programming Languages (POPL)

2026 **PC** | ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)
PC | ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)
PC | USENIX Security Symposium (USENIX Security)
Shadow PC | IEEE/ACM International Conference on Software Engineering (ICSE)
Reviewer | ACM Transactions on Software Engineering and Methodology (TOSEM)
AEC | International Conference on Computer Aided Verification (CAV)
AEC | European Conference on Object-Oriented Programming (ECOOP)
AEC | ACM SIGPLAN International Conference on Functional Programming (ICFP)
AEC | ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)
AEC | IEEE Symposium on Security and Privacy (S&P)

2025 **PC** | ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA)
PC | USENIX Security Symposium (USENIX Security)
AEC | International Conference on Computer Aided Verification (CAV)
AEC | European Conference on Object-Oriented Programming (ECOOP)
AEC | ACM SIGPLAN International Conference on Functional Programming (ICFP)
AEC | ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)

2024 **PC** | International Workshop on No-Code Copilots (AutoMates@IJCAI)
Reviewer | ACM Transactions on Architecture and Code Optimization (TACO)
ERC | European Conference on Object-Oriented Programming (ECOOP)
AEC | ACM SIGSAC Conference on Computer and Communications Security (CCS)
AEC | European Conference on Object-Oriented Programming (ECOOP)
AEC | ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)
AEC | International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI)

2023 **PC** | International Workshop on the Future of No-Code Digital Apprentices (AutoMates@IJCAI)
PC | ACM SIGPLAN International Conference on Systems, Programming, Languages, and Applications: Software for Humanity (SPLASH) Student Research Competition
Reviewer | ACM Transactions on Architecture and Code Optimization (TACO)
Reviewer | ACM Transactions on Software Engineering and Methodology (TOSEM)
ERC | European Conference on Object-Oriented Programming (ECOOP)
AEC | European Conference on Object-Oriented Programming (ECOOP)
AEC | ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)
AEC | International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI)

2022 **AEC** | ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)

2021 **AEC** | ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)

2020 **AEC** | ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA)
Student Volunteer | ACM SIGPLAN Symposium on Principles of Programming Languages (POPL)

2017 **Student Volunteer** | AAAI Conference on Artificial Intelligence (AAAI)

TEACHING

(F. - Fall · W. - Winter · S. - Spring · M. - Summer)

Teaching Assistant | University of California, Santa Barbara

F.2025, S.2024 CS 190J: Blockchain Technologies and Security
W.2022, W.2021 CS 595N: Research Seminar
S.2021 CS 190I: Program Synthesis
W.2020 CS 162: Programming Languages

S.2019 CS 130A: Data Structures and Algorithms - I
W.2019 CS 4: Computer Science Bootcamp
F.2018 CS 165A: Artificial Intelligence
M.2018 CS 8: Introduction to Computer Science
S.2018 CS 16: Problem Solving with Computers - I
F.2017 CS 40: Foundations of Computer Science

(Guest) Lecturer | University of California, Santa Barbara

F.2025, S.2024 CS 190J: Blockchain Technologies and Security
S.2022 CS 292C: Computer-Aided Reasoning for Software
S.2021 CS 190I: Program Synthesis
S.2018 CS 291K: Deep Learning

HONORS & AWARDS

2025 University of California, Riverside: FAME Award
2023 Ethereum Foundation Academic Award
UCSB Computer Science Outstanding PhD Student of the Year
2022 ACM SIGPLAN PLDI Distinguished Paper Award
ACM SIGPLAN PAC Award - OOPSLA
ACM SIGPLAN PAC Award - PLDI
2017 AAAI Student Scholarship

RECENT TALKS

2026 **A Synthesis-Aided Compiler for High-Performance Zero-Knowledge Proof Circuits**
SoCal PLS — *University of Southern California, CA, USA*

2025 **An Optimizing Compiler for Efficient Zero-Knowledge Circuits**
The Science of Blockchain Conference (SBC) 2025 — *University of California, Berkeley, CA, USA*

2025 **Towards Intelligent Agents for Trustworthy Zero-Knowledge Circuit Programming**
University of California, Riverside: FAME Workshop — *University of California, Riverside, CA, USA*

2025 **Compiler-Assisted Optimization of Finite Field Arithmetic via Refinement Types**
SoCal PLS — *University of California, San Diego, CA, USA*

2024 **DeFi Security**
Guest Lecture, CS 190J (Blockchain) — *University of California, Santa Barbara, CA, USA*

2023 **ZKSwift: A Programming Language for High-Performance ZK Circuits**
ProgCrypto: Programmable Cryptography Conference @ Devconnect — *Istanbul, Turkey*

2023 **Program Synthesis for All: A Synergistic Perspective**
Purdue CS Research Seminar — *Purdue University, IN, USA*
Berkeley Programming Systems Seminar — *University of California, Berkeley, CA, USA*
Stanford Software Research Seminar — *Stanford University, CA, USA*
UCSB Graduate Research Seminar — *University of California, Santa Barbara, CA, USA*

2022 **Formal Verification for Zero-Knowledge Circuits**
0xPARC Summer Residency — *New York City, NY, USA*

2022 **Program Synthesis for Complex Software Systems**
PhD Proposal Talk — *University of California, Santa Barbara, CA, USA*

2022 **Attack Synthesis for Blockchain Security**
Guest Lecture, CS 292C (Computer-Aided Reasoning) — *University of California, Santa Barbara, CA, USA*

2022 **A Symbolic Virtual Machine for Automated R1CS Verification**
0xPARC ZK Learning Group #2 — *New York City, NY, USA*

2021 **Multi-Modal Program Synthesis**
Guest Lecture, CS 190I (Program Synthesis) — *University of California, Santa Barbara, CA, USA*

2021 **Program Synthesis for Data Science**
Tutorial, ISEC'21 Synthesis4SE Workshop — *Bhubaneswar, India*

2020 **Bridging Logical Reasoning and Machine Learning in Program Synthesis**
PhD Major Area Examination Talk — *University of California, Santa Barbara, CA, USA*

2018 **Deep Learning in Open-Domain Dialogue Systems**
Guest Lecture, CS 291K (Deep Learning) *University of California, Santa Barbara, CA, USA*