

# Yibo Wang

☎ 315-898-5037

✉ ywang349@syr.edu

🌐 <https://yibo-wang.com>

---

## Education

### Syracuse University

*Ph.D., Electrical & Computer Engineering*

*M.S., Computer Engineering*

Syracuse, NY

08/2020 – Present

05/2019

### Huazhong University of Science and Technology (HUST)

*B.E., Electrical Engineering*

Wuhan, China

06/2016

---

## Publications

- Asymmetric Mempool DoS Security: Formal Definitions and Provable Secure Designs  
*Wanning Ding, Yuzhe Tang, Yibo Wang, IEEE S&P 2025*
- Understanding Ethereum Mempool Security under Asymmetric DoS by Symbolized Stateful Fuzzing  
*Yibo Wang, Yuzhe Tang, Kai Li, Wanning Ding, Zhihua Yang, USENIX Security 2024*
- Towards Understanding Crypto-Asset Risks on Ethereum Caused by Key Leakage on the Internet  
*Yuxuan Zhou, Jiaqi Chen, Yibo Wang, Yuzhe Tang and G. Gu, ACM Web Conference 2024, short*
- Understanding the Security Risks of Decentralized Exchanges by Uncovering Unfair Trades in the Wild  
*Jiaqi Chen, Yibo Wang, Yuxuan Zhou, Wanning Ding, Yuzhe Tang, XiaoFeng Wang, Kai Li, Euro S&P 2023*
- Ethical Challenges in Blockchain Measurement Research  
*Yuzhe Tang, Kai Li, Yibo Wang, Jiaqi Chen, EthiCS 2023*
- Towards Saving Blockchain Fees via Secure and Cost-Effective Batching of Smart-Contract Invocations  
*Yibo Wang, Kai Li, Yuzhe Tang, Jiaqi Chen, Qi Zhang, Xiapu Luo, Ting Chen, IEEE TSE 2023*
- Enabling Cost-Effective Blockchain Applications via Workload-Adaptive Transaction Execution  
*Yibo Wang, Yuzhe Tang, Poster ACM CCS 2022*
- iBatch: Saving Ethereum Fees via Secure and Cost-Effective Batching of Smart-Contract Invocations  
*Yibo Wang, Qi Zhang, Kai Li, Yuzhe Tang, Jiaqi Chen, Xiapu Luo, Ting Chen, ESEC/FSE 2021*
- DETER: Denial of Ethereum Txpool sERvices  
*Kai Li, Yibo Wang, Yuzhe Tang, ACM CCS 2021*
- TopoShot: Uncovering Ethereum's Network Topology Leveraging Replacement Transactions  
*Kai Li, Yuzhe Tang, Jiaqi Chen, Yibo Wang, Xianghong Liu, ACM IMC 2021*
- Scalable Log Auditing on Private Blockchains via Lightweight Log-Fork Prevention  
*Yuzhe Tang, Kai Li, Yibo Wang, Sencer Burak Somuncuoglu, SERIAL@Middleware 2020*
- Denial of Block-Building Services on Ethereum: New Attacks by Transaction Mutual Exclusion and Exhaustion then Exclusion  
*Zhihua Yang, Yibo Wang, Wanning Ding, Yuzhe Tang, Taesoo Kim, Under Submission*
- Towards Automated Discovery of Asymmetric Mempool DoS in Blockchains  
*Yibo Wang, Yuzhe Tang, Kai Li, Wanning Ding, Zhihua Yang, Under Submission*

---

## Research Projects

### Blockchain mempool security

*Syracuse University*

Syracuse, New York

01/2021 – Present

- Discover the vulnerability of transaction pool in Ethereum clients by reading source code, testing cases and fuzzing.
- Report 12 unique attacks that can deny the service of transaction pool with 0 or low cost. Receive Bug bounty from Ethereum Foundation \$4,000 (2023), \$12,000 (2021), \$2,000 (2022) and OpenEthereum/Parity \$8,000 (2021).

- Design defense against transaction pool DoS attacks by tightening the TxPool validation rules. Co-develop the patch code of the defense against transaction pool DoS attack and the code is merged in Geth client V1.11.4.
- Work as a contributor of Go-Ethereum (Geth) V1.11.4, <https://github.com/ethereum/go-ethereum/releases/tag/v1.11.4>.

### **Blockchain cost-effectiveness**

**Syracuse, New York**

*Syracuse University*

*08/2020 – Present*

- Design a middleware system running on top of a blockchain network to optimize the cost of blockchain-based DApps.
- Achieve saving 14.6% – 59.1% Gas cost per invocation without losing security or causing extra delay.
- Implement smart-contract rewriting techniques on source/bytecode for the integration of the middleware with contract.

### **Decentralized bug reporting system for smart contracts**

**Atlanta, Georgia**

*Georgia Institute of Technology*

*05/2024 – 09/2024*

- Develop a decentralized bug-reporting system for smart contracts, allowing anyone to submit bug reports to the blockchain, with validation by a decentralized group of verifiers, addressing manipulation and transparency issues in centralized systems like CVE.
- Achieve secure and transparent bug verification using encrypted Proof of Evidence (PoE) and Trusted Execution Environment (TEE).

---

## **Teaching**

### **Lab instruction, Syracuse University**

**09/2024**

- Instruct the Buffer Overflow Attack Lab in SEED Lab for Computer Security (CSE 364) under Dr. Yuzhe Tang.
- Present in-depth knowledge of buffer overflow attacks, covering memory and stack layout, buffer overflow vulnerabilities, and the practical execution of buffer overflow attacks.
- Lead hands-on lab sessions where students exploit buffer overflow vulnerabilities to obtain root privileges on both ARM64 and AMD64 architectures, providing practical insights into vulnerability exploitation and attack techniques.

### **Guest lecture, The State University of New York at Oswego (SUNY Oswego)**

**04/2024**

- Deliver a lecture on “Introduction to Blockchain and Web 3.0” for FIN 426 – Multi-National Financial Management at SUNY Oswego. This lecture is part of the curriculum taught by Dr. Hong Wan.
- Deliver an introduction to the development of blockchain and key concepts while guiding students through the step-by-step process of using a wallet to send a transaction.

---

## **Employment**

### **Certified Kernel Tech LLC (CertiK)**

**New York, New York**

*Security Research Intern*

*09/2024 – Present*

- Conduct research on security issues in Move-based blockchains, i.e., Sui, under the guidance of Dr. Zhaofeng Chen, focusing on identifying and analyzing vulnerabilities and developing mitigation strategies.
- Investigate the security aspects of Account Abstraction (ERC-4337) bundlers to identify and examine vulnerabilities in the bundling process.

### **Fulton**

**Pulaski, New York**

*Global Supply Chain Engineer*

*08/2019 – 12/2019*

- Provide IT support for supply chain groups. Communicate with suppliers about quotations and get credit issues.

---

## **Professional Services**

### **Program committee member**

- The Web Conference 2025

### **Reviewer**

- Computer Communications 2024
  - The Web Conference 2024
  - TDSC 2022
-

# Achievements & Certifications

## Academic awards

- USENIX Security '24 Grant, *USENIX Security* 08/2024
- CCS'22 workshop registration fellowship, *Protocol Lab* 10/2022
- USENIX Security '21 Grant, *USENIX Security* 07/2021
- Student Registration Grant, *IEEE Symposium on Security and Privacy* 05/2021
- Graduate Award (50% tuition scholarship), *Syracuse University* 05/2017

## Bug bounties

- Bug report for Flashbot, awarded \$200 2023
- Bug report for Erigon and Nethermind, awarded \$4,000 2023
- Bug report for Go-Ethereum, awarded \$2,000 2022
- Bug report for Go-Ethereum, awarded \$12,000 2021
- Bug report for Open-Ethereum, awarded \$8,000 2021

## Certifications

- NSF I-Corps Regional Course 2024

## Grants & Research Funding

- **Co-Principal Investigator (Co-PI)** **Ethereum Ecosystem Support Program**  
*DoS-Secure Transaction Propagation on Ethereum: Exploit Generation and Attack Detection.* 2022