Yunqi Li

+1 (607)279-7096 • lilioneviola@gmail.com; yunqil3@illinois.edu
lilione.github.io

Education

University of Illinois at Urbana-Champaign (UIUC) — **PhD in Electrical and Computer Engineering**
Advised by Prof. Andrew Miller — *Aug 2018 – Aug 2024 (Expected Completion)*

Shanghai Jiao Tong University (SJTU) — **Bachelor of Engineering in Computer Science**
***ACM Honors Class**, Zhiyuan College* — *Sep 2014 – Jun 2018*

Research Interests

Applied cryptography, cryptocurrency technologies, and design of secure distributed systems.

Internship Experiences

Meta — **Software Engineer Intern**
Applied Privacy Technology Team — *Summer 2022*
- Designed the workflow and database storage for a privacy-preserving measurement application, enabling surveys on sensitive data while ensuring user privacy via multi-party computation (MPC).
- Developed a 9k LoC end-to-end prototype in Rust and MySQL, achieving full-scale functionality in just a few weeks.

VMware Research — **Research Intern**
Advised by Avishay Yanai — *Spring 2022*
- Developed an MPC-based protocol for anonymous message broadcasting.
- Designed and implemented a front-running resistant decentralized exchange (in Python and Solidity).

Celer Network — **Software Engineer Intern**
Summer 2019
Designed and built the prototype (in Golang, JavaScript, and Solidity) of the State Guarding Network (SGN) to address off-chain availability challenges in state channels.

Cornell University, IC3 — **Research Intern**
Advised by Prof. Ari Juels — *Fall 2017*
Published the blog post The Cost of Decentralization in 0x and EtherDelta:
- Conducted the analysis of the advantages and drawbacks of centralized exchanges vs. decentralized exchanges.
- Developed and deployed an arbitrage bot to showcase arbitrage opportunities in decentralized exchanges.
- Featured in a Forbes interview and report: *Researchers Find Issues With 0x, An Ethereum-Based ICO Project*.

Publications

Nerla Jean-Louis, **Yunqi Li**, Yan Ji, Harjasleen Malvai, Thomas Yurek, Sylvain Bellemare, Andrew Miller. SGXonerated: Finding (and Partially Fixing) Privacy Flaws in TEE-based Smart Contract Platforms Without Breaking the TEE. *Proceedings on Privacy Enhancing Technologies (PoPETs) 2024, The Science of Blockchain Conference (SBC) 2023.*

Yunqi Li, Kyle Soska, Sylvain Bellemare, Mikerah Quintyne-Collins, Zhen Huang, Lun Wang, Amit Agarwal, Dawn Song, Andrew Miller. Ratel: MPC-Extensions for Smart Contracts. *Crypto Economics Security Conference (CESC) 2022.*

Philip Daian, Steven Goldfeder, Tyler Kell, **Yunqi Li**, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, Ari Juels. Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Transaction Reordering, and Consensus Instability. *IEEE Symposium on Security and Privacy (S&P) 2020.*

Sanket Kanjalkar, Joseph Kuo, **Yunqi Li**, Andrew Miller. I Can't Believe It's Not Stake! Resource Exhaustion Attacks on PoS. *Financial Cryptography and Data Security (FC) 2019.*

Awards & Honors

ACM-ICPC (International Collegiate Programming Contest)

- **2018 Mid-Central USA Regional Contest** (Team PinDuoDuo): Third Place
- **2014 Asia Regional Shanghai** (Team Pivot): Gold Medal & Best Women's Team (12th/270 teams). First women's team to win a gold medal in a Chinese ACM-ICPC regional.
- **2015 Asia Regional Beijing** (Team Lumos): Silver Medal & Best Women's Team
- **2015 China Shanghai Metropolitan Programming Contest** (Team SSM): Gold Medal (9th/195 teams)

Scholarships

- **2016 Eleme Scholarship**, SJTU (Top 5% in CS Department)
- **2015 XinDong Scholarship**, SJTU (Top 5% in CS Department)

Selected Projects

TEE Rollups: Fixing Access Patterns in TEE-based Smart Contracts with Off-chain Computing June 2023

- Developed an innovative off-chain obfuscation technique to reduce access pattern leakage in Trusted Execution Environment (TEE)-backed blockchains.
- Our proof-of-concept clinched First Place at the 2023 IC3 Blockchain Camp Hackathon.

Sting Framework March 2023 – June 2023

- Enhanced system security against information leakage by implementing an "informer" model, which provides publicly verifiable proofs to report corrupt services.
- Engineered a prototype for the Flashbots SGX builder.

Breaking Privacy of TEE-based Smart Contract Platforms Feb 2023

- Performed an in-depth privacy analysis of leading TEE-based smart contract platforms, focusing on state consistency, access pattern leakage, and software upgrade mechanisms.
- Developed a proof-of-concept tool that compromises privacy-preserving tokens by uncovering recipient details, transfer amounts, and token balances, and demonstrated successful front-running attacks on decentralized exchanges.

MPC Sidechain Framework Oct 2020 – April 2021

- Developed *MPC as a Sidechain* for general-purpose, fully confidential smart contracts.
- Designed a unified high-level language, enabling developers to code all components in a singular, common syntax.
- Engineered applications such as a confidential decentralized exchange that conceals trade data to prevent front-running.
- Won the top prize at the 2021 IC3 Blockchain Camp Hackathon with "BadgerSwapV3 using Ratel: Integrating Uniswap with MPC."

Resource Exhaustion Attack on PoS Aug 2018 - Oct 2018

- Investigated and disclosed resource exhaustion vulnerabilities which affected 26+ Proof-of-Stake cryptocurrencies.
- Medium Post of public disclosure is in *"Fake Stake" attacks on chain-based Proof-of-Stake cryptocurrencies*.

Teaching and Mentorship Experiences

ECE407/CS407 Cryptography **Teaching Assistant**
UIUC *Fall 2021*

ACM-ICPC Team **Assistant Coach**
SJTU *Apr 2016 – Jun 2017*