YAN JI

Cornell Tech
2 West Loop Road
New York, NY 10044
✉ *yj348 at cornell dot edu*

RESEARCH INTERESTS

Blockchains, Applied Cryptography, Security and Privacy, Distributed Systems, Decentralized Finance and Regulatory Compliance

EDUCATION

Aug. 2017 - May 2024 (expected) **Ph.D. student in Computer Science**, *Cornell University*
Advisor: Ari Juels, Department of Computer Science.

Sept. 2013 - Jul. 2017 **B.E. in Computer Science**, *Shanghai Jiao Tong University (SJTU)*, China
ACM Honored Class of Zhiyuan College.

RESEARCH EXPERIENCE

Aug. 2023 - Dec. 2023 **Research Intern**, Mysten Labs
Hosted by Dr. Kostas Chalkias. Worked on zkLogin, which allows users to manage blockchain accounts with OAuth credentials in a privacy-preserving and user-friendly way. Core developer of the zkLogin ceremony.

June. 2020 - Nov. 2020 **Research Intern**, *Novi*, Facebook
Hosted by Dr. Kostas Chalkias. Worked on proof of liabilities, a cryptographic primitive for auditing solvency at financial institutions and a wide range of application scenarios.

PUBLICATIONS

[PETS2024] N. Jean-Louis, Y. Li, **Y. Ji**, H. Malvai, T. Yurek, S. Bellemare, and A. Miller, SGXonerated: Finding (and Partially Fixing) Privacy Flaws in TEE-based Smart Contract Platforms Without Breaking the TEE, To appear in *Proceedings on Privacy Enhancing Technologies*, 2024

[CoDecFin24] **Y. Ji**, and J. Grimmelmann, Regulatory Implications of MEV Mitigations, To appear in *International Conference on Financial Cryptography and Data Security. FC 2024 International Workshops*, 2024

[CCS2023] K. Babel, M. Javaheripi, **Y. Ji**, M. Kelkar, F. Koushanfar, and A. Juels, Lanturn: Measuring economic security of smart contracts through adaptive learning, In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 1212-1226*, 2023

[CoDecFin22] K. Chalkias, P. Chatzigiannis, and **Y. Ji**, Broken Proofs of Solvency in Blockchain Custodial Wallets and Exchanges, In *International Conference on Financial Cryptography and Data Security. FC 2022 International Workshops, pp. 106-117*, 2022

[CCS21] **Y. Ji** and K. Chalkias, Generalized Proofs of Liabilities, In *Proceedings of the 2020 ACM SIGSAC conference on Computer and Communications Security (CCS), pp. 3465-3486*, 2021

[NDSS21] C. Hou, M. Zhou, **Y. Ji**, P. Daian, F. Tramer, G. Fanti, and A. Juels, SquirRL: Automating Attack Analysis on Blockchain Incentive Mechanisms with Deep Reinforcement Learning, In *Network and Distributed System Security Symposium (NDSS)*, 2021

[CCS20] M. Mirkin*, **Y. Ji***, J. Pang, A. Klages-Mundt, I. Eyal, and A. Juels, BDoS: Blockchain Denial of Service, In *Proceedings of the 2020 ACM SIGSAC conference on Computer and Communications Security (CCS), pp. 601-619*, 2020

[CCS19] I. Bentov, **Y. Ji**, F. Zhang, L. Breidenbach, P. Daian, and A. Juels, Tesseract: Real-time cryptocurrency exchange using trusted hardware, In *Proceedings of the 2019 ACM SIGSAC conference on Computer and Communications Security (CCS), pp. 1521-1538*, 2019

*: Equal contribution

[CCS17] E. Cecchetti, F. Zhang, **Y. Ji**, A. Kosba, A. Juels, and E. Shi, Solidus: Confidential distributed ledger transactions via PVORM, In *Proceedings of the 2017 ACM SIGSAC conference on Computer and Communications Security (CCS), pp. 701-717*, 2017

MANUSCRIPTS

2023 **Y. Ji**, M. Kelkar, D. Maram, K. Chalkias Y. Hu, and A. Juels, AVES: Approximately Verifiable Statistics on Append-Only Authenticated Dictionaries, Available upon request

2024 F. Baldimtsi, K.K. Chalkias, **Y. Ji**, J. Lindstrøm, D. Maram, B. Riva, A. Roy, M. Sedaghat, and J. Wang, zkLogin: Privacy-Preserving Blockchain Authentication with Existing Credentials, arXiv preprint arXiv:2401.11735

AWARDS & HONORS

2022 **Finalist for the Applied Research Competition**, *CSAW Cybersecurity Games & Conference*
For research on *Generalized proofs of Liabilities*.

2021 **Facebook Fellowship in Blockchain and Cryptoeconomics**, *Facebook*
Top 1.2%: 26/2163; 1 fellow in Blockchain and Cryptoeconomics

2020 **DLI Doctoral Fellowship**, *Digital Life Initiative*, Cornell Tech

2020 **Finalist for the 2020 Facebook Fellowship Program**, *Facebook*

2018 **First Place**, *IC3-Ethereum Crypto Boot Camp*
Team co-leader of Project Chicago.

2017 **Cornell University Fellowship**, *Cornell University*

2017 **Excellent Graduate Award**, *Shanghai Jiao Tong University*

2017 **Outstanding Student Scholarship**, *Shanghai Jiao Tong University*

2014 **KoGuan Scholarship**, *Shanghai Jiao Tong University*

2014 - 2016 **Academic Excellence Scholarship**, *Shanghai Jiao Tong University*

2013 - 2018 **ACM-International Collegiate Programming Contest**

- ○ **Champion**, Greater New York Regional 2017.
  Proceeded to World Final 2018.
- ○ **Gold Medal & The Best Female Team**, Asia Regional Shanghai 2014.
  Team leader, *SJTU's first gold medal won by a female team*.
- ○ **Silver Medal & The Best Female Team**, Asia Regional Nanjing 2013.
- ○ **Silver Medal**, Asia Regional Phuket 2013.

OPEN-SOURCED PROJECTS

- **Groth16 Ceremony for Sui zkLogin**, `https://github.com/sui-foundation/zklogin-ceremony-contributions`
  The Groth16 Zero Knowledge Proof (ZKP) ceremony for Sui zkLogin with contribution client diversity, i.e., participants may contribute via either snarkjs in browser or Kobi's Rust implementation in docker.
- **EIP-5218: NFT Rights Management**, `https://eips.ethereum.org/EIPS/eip-5218`
  An interface for creating copyright licenses that transfer with an NFT.
- **CANDID NFT**, `https://dorahacks.io/buidl/2029`
  An NFT fairdrop toolkit allowing artists to sell NFTs directly to their collectors based on real-world off-chain identities in a trustworthy and privacy-preserving way.
  Won the *Grand Prize* of the Chainlink Labs' bug bounty and *Second Place* of the Most Creative Hack Incorporating Pocket Network at ETHDenver 2022.
- **DAPOL+**, `https://github.com/MystenLabs/dapol`
  An efficient and practical protocol for proof of liabilities with provable security and privacy.
- **SMTree**, `https://github.com/novifinancial/smtree`
  An implementation of paddable sparse Merkle tree, the data structure used by various cryptographic protocols including DAPOL+ and HashWires.

- **SquirRL**, https://github.com/wuwuz/SquirRL
  A framework for using deep reinforcement learning to identify attack strategies on blockchain incentive mechanisms.
- **Solidus**, https://github.com/ethancecchetti/Solidus-prototype
  A protocol for confidential yet verifiable transactions on public blockchains.
- **Town Crier**, https://www.town-crier.org
  An authenticated data feed for the blockchain.
- **Banyan**, https://github.com/iseriohn/Banyan
  An automated multi-track program committee meeting arrangement tool minimizing the number of sessions. Used in NDSS 2017 & 2018.

TEACHING

Spring 2022 **Teaching Assistant**, *CS5830: Cryptography*, Cornell
Instructed by Prof. Thomas Ristenpart.

Spring 2020 **Teaching Assistant**, *CS5433: Blockchains, Cryptocurrencies, and Smart Contracts*, Cornell
Instructed by Prof. Ari Juels.

Fall 2015 **Teaching Assistant**, *Automata Theory*, SJTU
Instructed by Prof. John Hopcroft.

Apr. 2015 - Jun. 2016 **Chief Student Coach**, *ACM-ICPC Team*, SJTU
SJTU won the second place in World Final 2016 and 4 championships in 2015-2016 Asia Regionals.
The first female in this position.

ACADEMIC SERVICE

- **Program Committee**
  FC 2024.
- **Reviewer**
  AFT 2019, USENIX Security 2020, CCS 2020, FC 2021, S&P 2022, CCS 2023, LATINCRYPT 2023.

Programming Languages

Rust, C++, Go, Python, JavaScript