YAN JI

RESEARCH INTERESTS

Blockchain technology, Applied Cryptography, Security and Privacy, Distributed Systems, Decentralized Finance and Regulatory Compliance.

EDUCATION

2024 **Ph.D. in Computer Science**, *Cornell University*.
Advisor: Ari Juels, Department of Computer Science.

2022 **M.S. in Computer Science**, *Cornell University*.
Advisor: Ari Juels, Department of Computer Science.

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

EXPERIENCE

Jul 2024 - Present **Research Engineer**, Chainlink Labs.
Working on oracle solutions to securely connect blockchains and legacy systems with authentic and privacy-preserving data feeds.

Aug. 2018 - May 2024 **Graduate Research Assistant**, Cornell Tech.
Researched and designed on quasi-decentralized systems to bridge the gap between centralized reliability and decentralized transparency.

May 2023 - Dec. 2023 **Research Intern**, Mysten Labs.
Hosted by Dr. Kostas Chalkias. Worked on zkLogin and encrypted NFTs. zkLogin allows users to manage blockchain accounts with OAuth credentials in a privacy-preserving and user-friendly way. Encrypted NFTs allow fair exchange of fully or partially encrypted NFT contents in a secure and privacy-preserving manner.

Jun. 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

[CCS2024] Baldimtsi F, Chalkias KK, **Ji Y**, Lindstrøm J, Maram D, Riva B, Roy A, Sedaghat M, Wang J, "zkLogin: Privacy-Preserving Blockchain Authentication with Existing Credentials", To appear in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2024.

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

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

[CCS2023] Babel K, Javaheripi M, **Ji Y**, Kelkar M, Koushanfar F, Juels A, "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] Chalkias K, Chatzigiannis P, **Ji Y**, "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] **Ji Y**, Chalkias K, "Generalized Proofs of Liabilities", In *Proceedings of the 2020 ACM SIGSAC conference on Computer and Communications Security (CCS), pp. 3465-3486*, 2021.

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

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

[CCS19] Bentov I, **Ji Y**, Zhang F, Breidenbach L, Daian P, Juels A, "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.

[CCS17] Cecchetti E, Zhang F, **Ji Y**, Kosba A, Juels A, Shi E, "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

2024 **Ji Y**, Kelkar M, Maram D, Chalkias K, Hu Y, Juels A, "AVES: Approximately Verifiable Statistics on Append-Only Authenticated Dictionaries", Available upon request.

2024 Baldimtsi F, Chalkias K, **Ji Y**, Roy A, Wang J, "Encrypted NFTs with Partial Reveal", Available upon request.

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.

*: Equal contribution

- **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, FC 2025.
- **Reviewer**.
  AFT 2019, USENIX Security 2020, CCS 2020, FC 2021, S&P 2022, CCS 2023, LATINCRYPT 2023.

Programming Languages

Rust, C++, Go, Python, JavaScript.