Fan Zhang

https://fanzhang.me
fanz@cs.cornell.edu
2 West Loop, New York, NY 10044

Education

Ph.D. Candidate in Computer Science — Aug, 2014–present
Advisor: Prof. Ari Juels
Dept. of Computer Science
Cornell University, Ithaca, NY

B.S. in Electronic Engineering — Aug, 2010 – Jul, 2014
Tsinghua University, Beijing, China

Research Interests

My research interests center on the security and privacy of decentralized systems, especially those enabled by blockchain protocols and trusted execution environments.

Industry Adoption

My research has led to direct industry adoption. Town Crier [10] was licensed from Cornell by Chainlink and Ekiden [3] is used in Oasis Labs' products. CHURP [1] is on Oasis Labs product roadmap. DECO [2] is under licensing negotiation.

Awards

- IBM PhD Fellowship Award — 2018-2020
- Academic Excellence Scholarship, Tsinghua University, China — 2013
- National Scholarship, the Ministry of Education of China — 2012
- Freshman Scholarship, Tsinghua University, China — 2010

Selected Publications

[1] SKD Maram*, **Fan Zhang***, Lun Wang, Andrew Low, Yupeng Zhang, Ari Juels, and Dawn Song, "CHURP: dynamic-committee proactive secret sharing," in *ACM CCS*, ***first two authors made equal contribution**, 2019.

[2] **Fan Zhang**, Sai Krishna Deepak Maram, Harjasleen Malvai, Steven Goldfeder, and Ari Juels, "DECO: Liberating web data using decentralized oracles for TLS," *CoRR*, vol. abs/1909.00938, 2019, Talk accepted to Real World Crypto (RWC) '20.

[3] Raymond Cheng, **Fan Zhang**, Jernej Kos, Warren He, Nicholas Hynes, Noah M. Johnson, Ari Juels, Andrew Miller, and Dawn Song, "Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts," in *IEEE EuroS&P*, 2019.

[4] **Fan Zhang**, Philip Daian, Iddo Bentov, Ian Miers, and Ari Juels, "Paralysis proofs: Secure dynamic access structures for cryptocurrency custody and more," in *ACM Conference on Advances in Financial Technologies (AFT)*, 2019.

[5] Iddo Bentov, Yan Ji, **Fan Zhang**, Yunqi Li, Xueyuan Zhao, Lorenz Breidenbach, Philip Daian, and Ari Juels, "Tesseract: Real-time cryptocurrency exchange using trusted hardware," in *ACM CCS*, 2019.

[6] **Fan Zhang**, Ittay Eyal, Robert Escriva, Ari Juels, and Robbert van Renesse, "REM: resource-efficient mining for blockchains," in *USENIX Security*, 2017.

[7] Florian Tramèr, **Fan Zhang**, Huang Lin, Jean-Pierre Hubaux, Ari Juels, and Elaine Shi, "Sealed-glass proofs: Using transparent enclaves to prove and sell knowledge," in *IEEE EuroS&P*, 2017.

[8] Ethan Cecchetti, **Fan Zhang**, Yan Ji, Ahmed E. Kosba, Ari Juels, and Elaine Shi, "Solidus: Confidential distributed ledger transactions via PVORM," in *ACM CCS*, 2017.

[9] Florian Tramèr, **Fan Zhang**, Ari Juels, Michael K. Reiter, and Thomas Ristenpart, "Stealing machine learning models via prediction APIs," in *USENIX Security*, 2016.

[10] **Fan Zhang**, Ethan Cecchetti, Kyle Croman, Ari Juels, and Elaine Shi, "Town Crier: An authenticated data feed for smart contracts," in *ACM CCS*, 2016.

[11] Longqi Yang, Yin Cui, **Fan Zhang**, John P Pollak, Serge Belongie, and Deborah Estrin, "Plateclick: Bootstrapping food preferences through an adaptive visual interface," in *ACM CIKM*, 2015.

Employment

Cornell University — May, 2011 – present
Graduate Research Assistant — New York, NY

Oasis Labs — May, 2017 – Aug, 2017
Researcher — Berkeley, CA

Security & Privacy Research, Intel Labs — Jul, 2017 – Aug, 2017
Researcher — Hillsboro, OR

Intel Opensource Technology Center (01.org) — Jun, 2013 – May, 2014
Intern — Beijing, China

Teaching Experience

- TA for CS5435: Security and Privacy in the Wild — 2015, Fall
- TA for CS5300: the Architecture of Large-scale Information Systems — 2015, Spring
- TA for CS4410: Operating Systems — 2014 Fall

Invited Talks

Connecting Blockchains with the Real World
- CISPA-Helmholtz Center for Information Security, Germany. — Nov, 2019
- ETH Zürich, Switzerland. — Oct, 2019
- IBM Watson Research Center (IBM PhD fellow). — Sep, 2019

CHURP: Proactive Secret Sharing with Dynamic Committee
- ACM CCS'19, London, UK. — Nov, 2019

On Trusted Hardware and Blockchain Hybridization
- Northeastern University, Cybersecurity Speaker Series. — Jan, 2019
- MIT, CSAIL. — Nov, 2018
- New York University, CS Colloquium. — Oct, 2018

Paralysis Proof
- ACM AFT 2019, Zürich, Switzerland. — Oct, 2019
- IC3 Retreat, New York City. — May, 2018
- 5th Bitcoin Workshop, Financial Crypto'18, Curacao. — Mar, 2018

REM
- USENIX Security'17, Vancouver BC, Canada. — Aug, 2017

Town Crier
- Silicon Valley Ethereum Meetup, Santa Clara, CA. — Aug, 2017
- IC3 Retreat, San Francisco, CA. — Mar, 2017
- CCS'16, Vienna, Austria. — Oct, 2016
- IC3 Retreat, New York City. — May, 2016

Professional Activity

- **Program Committee**: BITCOIN'18, collocated with Financial Crypto 2018.
- **Reviewer**: ACM Computing Surveys (2018), Nature Sustainability (2018)
- **Subreviewer**: USENIX Security (2016), TCC (2019), FC (2019)

Software Artifacts

- Town Crier: an Authenticated Data Feed For Smart Contracts
  https://town-crier.org
- CHURP: Dynamic-Committee Proactive Secret Sharing
  https://churp.io
- mbedtls-SGX: a SGX-friendly TLS stack (ported from mbedtls)
  https://github.com/bl4ck5un/mbedtls-SGX

Selected Media Coverage

- *MIT Technology Review*, "Blockchain smart contracts are finally good for something in the real world", on Nov 19, 2018.
- *Forbes*, "Cornell's Town Crier Acquired By Chainlink To Expand Decentralized Oracle Network", on Nov 1, 2018.

- *BitcoinExchangeGuide*, "Chainlink Blockchain Company Acquires Cornell's Town Crier to Bolster Native Smart Contract Network" on Nov 2, 2018.
- *Unhashed*, "Chainlink Acquires Town Crier, a Hardware-Based Oracle", on Nov 3, 2018.
- *Forbes*, "Big Hitter Crypto Funds Pile Into Privacy-Enhanced Smart Contract Startup Oasis Labs", on Jul 9, 2018.
- *BitcoinMagazine*, "Cornell IC3 Researchers Propose Solution to Bitcoin's Multisig *Paralysis* Problem", on Jan 19, 2018.
- *IEEE Spectrum*, "The Ridiculous Amount of Energy It Takes to Run Bitcoin", on Sep 28, 2017.
- *CoinDesk*, "Trust Your Oracle? Cornell Launches Tool for Confidential Blockchain Queries", on May 17, 2017.
- *MIT Technology Review*, "How Encrypted Weather Data Could Help Corporate Blockchain Dreams Come True", on May 11, 2017.
- *ETHNews*, "Town Crier Service Delivers Solid Data To Coders", on May 11, 2017.

References *Contact information available upon request.*