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

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

Research

Security and Privacy, Blockchains, Applied Cryptography, Trusted Hardware

Industry Adoption

My research has led to direct industry adoption. Town Crier [9] was licensed from Cornell by Chainlink and Ekiden [2] is used in Oasis Labs' products. CHURP [5] is on Oasis Labs product roadmap. DECO [4] 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] I. Bentov, Y. Ji, **F. Zhang**, Y. Li, X. Zhao, L. Breidenbach, P. Daian, and A. Juels, "Tesseract: Real-time cryptocurrency exchange using trusted hardware," in *ACM CCS (to appear)*, 2019.

[2] R. Cheng, **F. Zhang**, J. Kos, W. He, N. Hynes, N. M. Johnson, A. Juels, A. Miller, and D. Song, "Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts," in *IEEE EuroS&P*, 2019.

[3] **F. Zhang**, P. Daian, I. Bentov, I. Miers, and A. Juels, "Paralysis proofs: Secure dynamic access structures for cryptocurrency custody and more," in *ACM Conference on Advances in Financial Technologies (AFT)*, 2019.

[4] **F. Zhang**, S. K. D. Maram, H. Malvai, S. Goldfeder, and A. Juels, "DECO: liberating web data using decentralized oracles for TLS," *CoRR*, vol. abs/1909.00938, 2019, Talk accepted to Real World Crypto (RWC) '20.

[5] S. K. D. Maram*, **F. Zhang***, L. Wang, A. Low, Y. Zhang, A. Juels, and D. Song, "CHURP: dynamic-committee proactive secret sharing," in *ACM CCS (to appear)*, ***indicates equal contribution**, 2019.

[6] E. Cecchetti, **F. Zhang**, Y. Ji, A. E. Kosba, A. Juels, and E. Shi, "Solidus: Confidential distributed ledger transactions via PVORM," in *ACM CCS*, 2017.

[7] **F. Zhang**, I. Eyal, R. Escriva, A. Juels, and R. van Renesse, "REM: resource-efficient mining for blockchains," in *USENIX Security*, 2017.

[8] F. Tramèr, **F. Zhang**, H. Lin, J. Hubaux, A. Juels, and E. Shi, "Sealed-glass proofs: Using transparent enclaves to prove and sell knowledge," in *IEEE EuroS&P*, 2017.

[9] **F. Zhang**, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *ACM CCS*, 2016.

[10] F. Tramèr, **F. Zhang**, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction apis," in *USENIX Security*, 2016.

Working Experience

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

Researcher Jul, 2017 – Aug, 2017
SPR (Security & Privacy Research), Intel Labs Hillsboro, OR

System developer intern Jun, 2013 – May, 2014
Intel Opensource Technology Center (01.org) 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

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)

Invited Talks

Connecting Blockchains to the Real World

- ETH Zürich, Switzerland. Oct, 2019
- IBM Watson Research Center (IBM PhD fellow). Sep, 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

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`