Fan Zhang *Curriculum vitae*

Basic Information

Fan Zhang
2 West Loop Road
New York, NY 10044

http://fanzhang.me
fanz@cs.cornell.edu

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 Area

Systems security, Applied Cryptography, Trusted Hardware, Blockchain

Honors and Awards

IBM PhD Fellowship Award 2018-2020

from IBM

Academic Excellence Scholarship 2013

from Tsinghua University, China

National Scholarship 2012

from the Ministry of Education of China

Freshman Scholarship 2010

from Tsinghua University, China

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)

Invited Talks

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

- 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

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 appointments held at Cornell

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

Software Artifacts

My research yields practical systems and production-ready software artifacts. Here is a selected list of them and please see my Github page for more.

- 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`

Publications

Last updated on August 19, 2019.

[1] S. K. D. Maram, F. Zhang, L. Wang, A. Low, Y. Zhang, A. Juels, and D. Song, "CHURP: dynamic-committee proactive secret sharing," *IACR Cryptology ePrint Archive*, vol. 2019, p. 17, 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 contract execution," *CoRR*, vol. abs/1804.05141, 2018. arXiv: `1804.05141`.

[3] F. Zhang, P. Daian, I. Bentov, and A. Juels, "Paralysis proofs: Safe access-structure updates for cryptocurrencies and more," *IACR Cryptology ePrint Archive*, vol. 2018, p. 96, 2018.

[4] E. Cecchetti, F. Zhang, Y. Ji, A. E. 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 2017, Dallas, TX, USA, October 30 - November 03, 2017*, B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu, Eds., ACM, 2017, pp. 701–717.

[5] 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 *2017 IEEE European Symposium on Security and Privacy, EuroS&P 2017, Paris, France, April 26-28, 2017*, IEEE, 2017, pp. 19–34.

[6] F. Zhang, I. Eyal, R. Escriva, A. Juels, and R. van Renesse, "REM: resource-efficient mining for blockchains," in *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017.*, E. Kirda and T. Ristenpart, Eds., USENIX Association, 2017, pp. 1427–1444.

[7] 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," *IACR Cryptology ePrint Archive*, vol. 2017, p. 1153, 2017.

[8] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi, Eds., ACM, 2016, pp. 270–282.

[9] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction apis," in *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, T. Holz and S. Savage, Eds., USENIX Association, 2016, pp. 601–618.

[10] L. Yang, Y. Cui, F. Zhang, J. P. Pollak, S. Belongie, and D. Estrin, "Plateclick: Bootstrapping food preferences through an adaptive visual interface," in *Proceedings of the 24th ACM International on Conference on Information and Knowledge Management*, ACM, 2015, pp. 183–192.