

Fan Zhang

CONTACT INFORMATION 2 West Loop Road <http://fanzhang.me>
New York, NY 10044 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 AREAS Applied Cryptography, Trusted Hardware, Blockchain

INDUSTRY ADOPTION My research has led to direct industry adoption. Town Crier [10] was licensed from Cornell by [Chainlink](#) and Ekiden [2] is used in [Oasis Labs](#)’ products.

HONORS/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] 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.
[4] F. Zhang, P. Daian, I. Bentov, and A. Juels, “Paralysis proofs: Safe access-structure updates for cryptocurrencies and more,” in *ACM AFT (to appear)*, 2019.
[5] 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.
[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*, B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu, Eds., ACM, 2017, pp. 701–717.
[7] 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*, IEEE, 2017, pp. 19–34.

- [8] F. Zhang, I. Eyal, R. Escriva, A. Juels, and R. van Renesse, “REM: resource-efficient mining for blockchains,” in *USENIX Security*, E. Kirda and T. Ristenpart, Eds., USENIX Association, 2017, pp. 1427–1444.
- [9] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, “Stealing machine learning models via prediction apis,” in *USENIX Security*, T. Holz and S. Savage, Eds., USENIX Association, 2016, pp. 601–618.
- [10] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, “Town crier: An authenticated data feed for smart contracts,” in *ACM CCS*, E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi, Eds., ACM, 2016, pp. 270–282.
- [11] L. Yang, Y. Cui, F. Zhang, J. P. Pollak, S. Belongie, and D. Estrin, “Plateclick: Bootstrapping food preferences through an adaptive visual interface,” in *ACM CIKM*, ACM, 2015, pp. 183–192.

PROFESSIONAL ACTIVITY	<ul style="list-style-type: none"> • Program Committee: BITCOIN’18, collocated with Financial Crypto 2018. • Reviewer: ACM Computing Surveys (2018), Nature Sustainability (2018) • Subreviewer: USENIX Security (2016), TCC (2019) 	
SOFTWARE ARTIFACTS	<p>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.</p> <ul style="list-style-type: none"> • 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 	
WORKING EXPERIENCE	<p>Researcher Oasis Labs</p> <p>Researcher SPR (Security & Privacy Research), Intel Labs</p> <p>System developer intern Intel Opensource Technology Center (01.org)</p>	<p>May, 2017 – Aug, 2017 Berkeley, CA</p> <p>Jul, 2017 – Aug, 2017 Hillsboro, OR</p> <p>Jun, 2013 – May, 2014 Beijing, China</p>
TEACHING EXPERIENCE	<ul style="list-style-type: none"> • TA for CS5435: Security and Privacy in the Wild • TA for CS5300: the Architecture of Large-scale Information Systems • TA for CS4410: Operating Systems 	<p>2015, Fall</p> <p>2015, Spring</p> <p>2014 Fall</p>
INVITED TALKS	<p>On Trusted Hardware and Blockchain Hybridization</p> <ul style="list-style-type: none"> • Northeastern University, Cybersecurity Speaker Series. • MIT, CSAIL. • New York University, CS Colloquium. <p>Paralysis Proof</p> <ul style="list-style-type: none"> • IC3 Retreat, New York City. • 5th Bitcoin Workshop, Financial Crypto’18, Curacao. <p>REM</p> <ul style="list-style-type: none"> • USENIX Security’17, Vancouver BC, Canada. 	
		<p>Jan, 2019</p> <p>Nov, 2018</p> <p>Oct, 2018</p> <p>May, 2018</p> <p>Mar, 2018</p> <p>Aug, 2017</p>

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 |