

# Fan Zhang

---

CONTACT INFORMATION      2 West Loop Road      <http://fanzhang.me>  
New York, NY 10044      [fanz@cs.cornell.edu](mailto: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 [1] 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] 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 *EuroS&P*, IEEE, 2019, pp. 185–200.  
[2] 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.  
[3] 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.  
[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.  
[5] 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.  
[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"> <li>• <b>Program Committee:</b> BITCOIN’18, collocated with Financial Crypto 2018.</li> <li>• <b>Reviewer:</b> ACM Computing Surveys (2018), Nature Sustainability (2018)</li> <li>• <b>Subreviewer:</b> USENIX Security (2016), TCC (2019)</li> </ul>	
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"> <li>• Town Crier: an Authenticated Data Feed For Smart Contracts <a href="https://town-crier.org">https://town-crier.org</a></li> <li>• CHURP: Dynamic-Committee Proactive Secret Sharing <a href="https://churp.io">https://churp.io</a></li> <li>• mbedtls-SGX: a SGX-friendly TLS stack (ported from mbedtls) <a href="https://github.com/bl4ck5un/mbedtls-SGX">https://github.com/bl4ck5un/mbedtls-SGX</a></li> </ul>	
WORKING EXPERIENCE	<p><b>Researcher</b> Oasis Labs</p> <p><b>Researcher</b> SPR (Security &amp; Privacy Research), Intel Labs</p> <p><b>System developer intern</b> 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"> <li>• TA for CS5435: Security and Privacy in the Wild</li> <li>• TA for CS5300: the Architecture of Large-scale Information Systems</li> <li>• TA for CS4410: Operating Systems</li> </ul>	<p>2015, Fall</p> <p>2015, Spring</p> <p>2014 Fall</p>
INVITED TALKS	<p><b>On Trusted Hardware and Blockchain Hybridization</b></p> <ul style="list-style-type: none"> <li>• Northeastern University, Cybersecurity Speaker Series.</li> <li>• MIT, CSAIL.</li> <li>• New York University, CS Colloquium.</li> </ul> <p><b>Paralysis Proof</b></p> <ul style="list-style-type: none"> <li>• IC3 Retreat, New York City.</li> <li>• 5th Bitcoin Workshop, Financial Crypto’18, Curacao.</li> </ul> <p><b>REM</b></p> <ul style="list-style-type: none"> <li>• USENIX Security’17, Vancouver BC, Canada.</li> </ul>	

**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 |