Xiong (Leo) Fan

Contact Information

399 Boylston St
Boston, MA 02116.

Web: https://leofanxiong.github.io
Email: *leofanxiong@gmail.com*

Research interests

(Post-quantum) cryptography, formal methods and hardware acceleration.

Education

Ph.D. in Computer Science (with a minor in Applied Mathematics) 2019
Cornell University, Ithaca, NY
Thesis Advisor: Prof. Elaine Shi

Master of Science in Computer Science 2013
Chinese Academy of Science, China
Advisors: Prof. Yong Feng and Prof. Mingsheng Wang

Bachelor of Science in Mathematics 2010
Sichuan University, China

Employment History

Cryptography Researcher. June 2021 - present
Algorand, Inc. Boston, MA.

Postdoctoral Researcher. August 2019 - June 2021
University of Maryland. College Park, MD.
Host: Prof. Jonathan Katz and Prof. Xiaodi Wu.

Research Assistant. 2015 - 2019
Cornell University. Ithaca, NY.

Research Scientist Intern, Summer 2017
IBM T.J. Watson Research Center, Yorktown Heights, NY
Cryptographic Research Group.

Research Scientist Intern. Summer 2016
Bell Labs, Murray Hill, NJ
Mentor: Vladimir Kolesnikov

Research Scientist Intern. Summer 2015
Yahoo Labs, Sunnyvale, CA
Mentors: Juan Garay and Payman Mohassel

Teaching Experience

Volunteer Teaching Assistant for CS 6832 Applied Cryptography. Fall 2016
Instructor: Prof. Elaine Shi.
Cornell University

Teaching Assistant for CMSC 456 Introduction to Cryptography. Fall 2013, 2014
Instructor: Prof. Jonathan Katz.
University of Maryland, College Park

Guest Lecturer for Computational Number Theory. Fall 2011
Instructor: Prof. Kunpeng Wang.
Chinese Academy of Science, China.

Honors and Awards

NSF/RWC Travel Grant 2018
IACR Conference Travel Grants. 2016 - 2019
Travel Grants, Cornell University. 2016 - 2018
Travel Grant, Institute for Advanced Study. 2016
Dean's Fellowship Award, University of Maryland, College Park. 2013 - 2014
Meritorious Winner, Mathematical Contest in Modeling. 2009

Mentoring Experience

Unofficially: Zhedong Wang (Ph.D., Chinese Academy of Science, now assistant professor at Shanghai Jiaotong University.)

Academic Activities

Graduate Student Admission Committee

- Department of Computer Science, University of Maryland, College Park 2014
- Department of Computer Science, Cornell University 2019

Professional Activities

Program Committee Member: IEEE S&P'20 (Shadow), AsiaCCS-SBC'20, ProvSec'20 and '21.

Conference External Reviewer: Crypto, Eurocrypt, Asiacrypt, IEEE S&P, Usenix Security, ACM CCS, PKC, TCC, CSF, SCN, Inscrypt, ICICS, FC, ESORICS.

Journal External Reviewer: Journal of Cryptology, Transactions on Information Forensics and Security (IEEE), Transactions on Dependable and Secure Computing (IEEE), Information Sciences (Elsevier), Theoretical Computer Science (Elsevier), Security and Communication Networks (Wiley), Science China Information Sciences (Springer).

Workshop Co-Organizer.

Cryptography Frontier Workshop, Chongqing, China 12/2016
New Theory and Applications in Cryptography, Sanya, China 12/2017

Industrial Projects

[1] Movier: An iOS-based video sharing social network. 2012
[2] DSCore: A decentralized security services platform. 2019

Patents

[1] Method and System for Digital Signature-Based Adjustable One-Time Passwords. Payman Mohassel, Juan Garay, Xiong Fan. US Patent 20,170,264,436.

Research Publications

[1] Manuel Barbosa, Gilles Barthe, Xiong Fan, Benjamin Grégoire, Shih-Han Hung, Jonathan Katz, Pierre-Yves Strub, Xiaodi Wu and Li Zhou. "EasyPQC: Verifying Post-Quantum Cryptography." In *28th ACM Conference on Computer and Communications Security, Virtual, November 15 - 19, 2021.*

[2] Jing Xu, Xinyu Li, Xiong Fan, Yuchen Wang, Zhenfeng Zhang. "Puncturable Signatures and Applications in Proof-of-Stake Blockchain." In *IEEE Transactions on Information Forensics and Security), vol. 15, pp. 3872-3885, 2020.*

[3] Bo Pang, Long Chen, Xiong Fan and Qiang Tang. "Multi-Input Laconic Function Evaluation." In *25th Australasian Conference on Information Security and Privacy, Perth, Australia, November 25 - 27, 2020.*

[4] Prabhanjan Ananth, Xiong Fan and Elaine Shi. "Towards Attribute-Based Encryption for RAMs from LWE: Sub-linear Decryption, and More." In *25th IACR Annual International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8 - 12, 2019.*

[5] Xiong Fan and Feng-Hao Liu. "Proxy Re-Encryption and Re-Signatures from Lattices." In *17th International Conference on Applied Cryptography and Network Security, Bogotá, Colombia, June 5 - 7, 2019.*

[6] Zhedong Wang, Xiong Fan and Feng-Hao Liu. "FE for Inner Products and Its Application to Decentralized ABE." In *22nd IACR International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, April 14 - 17, 2019.*

[7] Gilles Barthe, Xiong Fan, Joshua Gancher, Benjamin Grégoire, Charlie Jacomme and Elaine Shi. "Symbolic Proofs for Lattice-Based Cryptography." In *25th ACM*

Conference on Computer and Communications Security, Toronto, Canada, October 15 - 19, 2018.

[8] Xiong Fan and Qiang Tang. "Making Public Key Functional Encryption Function Private, Distributedly." In *21st IACR International Conference on Practice and Theory in Public-Key Cryptography, Rio De Janeiro, Brazil, March 25 - 28, 2018.*

[9] Zhedong Wang, Xiong Fan and Mingsheng Wang. "Compact Inner Product Encryption from LWE." In *19th International Conference on Information and Communications Security, Beijing, China, December 6 - 8, 2017.*

[10] Xiong Fan, Chaya Ganesh and Vladimir Kolesnikov. "Hashing Garbled Circuits for Free." In *36th IACR Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017.*

[11] Daniel Apon, Xiong Fan and Feng-Hao Liu. "Deniable Attribute Based Encryption for Branching Program from LWE." In *14th IACR Theory of Cryptography Conference, Beijing, China, October 31 - November 3, 2016.*

Manuscripts in Submission

[1] IPDL: A Simple Framework for Formally Verifying Distributed Cryptographic Protocols.
Xiong Fan, Joshua Gancher, Greg Morrisett, Elaine Shi, Kristina Sojakova.

[2] Collusion-Resistant Functional Encryption for RAMs.
Prabhanjan Ananth, Kai-Min Chung, Xiong Fan, Luowen Qian.

[3] Quantum-Secure Identity-Based Encryption, Revisited.
Kai-Min Chung, Xiong Fan, Shih-Han Hung, Jonathan Katz.

[4] Accelerating Post Quantum Cryptography with Memristor Crossbar Arrays.
Sarabjeet Singh, Xiong Fan, Ananth Krishna Prasad, Anirban Nag, Rajeev Balasubramonian, Mahdi Nazm Bojnordi, Elaine Shi.

Invited and Conference Talks

[1] EasyPQC: Verifying Post-Quantum Cryptography.
- CCS 2021. 11/2021

[2] Deniable Attribute Based Encryption for Branching Program from LWE.
- Florida Atlantic University. 10/2016
- TCC 2016. 11/2016
- Institute of Software, Chinese Academy of Science. 11/2016

[3] Towards Attribute-Based Encryption for RAMs from LWE: Sub-linear Decryption, and More.
- University of Maryland, Baltimore County. 10/2019

[4] Making Public Key Functional Encryption Function Private, Distributedly.
- Crypto Seminar, Cornell University. 03/2018
- PKC 2018. 03/2018

[5] Proxy Re-Encryption and Re-Signatures from Lattices.
- ACNS 2019. 06/2019

[6] IPDL: A Probabilistic Dataflow Logic for Cryptography.
- University of Maryland, College Park. 11/2019