YUPENG ZHANG

CONTACT INFORMATION

414A, Harvey R. Bright Building (HRBB),
Texas A&M University,
College Station, TX, 77840

PHONE: 979-845-9980
WEB: http://people.tamu.edu/∼zhangyp
EMAIL: zhangyp@tamu.edu

RESEARCH INTERESTS

Applied Cryptography. Verifiable Computation and Zero-knowledge Proof. Privacy-preserving Machine Learning. Searchable Encryption.

PROFESSIONAL APPOINTMENTS

Texas A&M University Aug. 2019 – present
Assistant Professor *College Station, TX, USA*

Department of Computer Science and Engineering

University of California, Berkeley Sep. 2018 – Aug. 2019
Postdoctoral Researcher *Berkeley, CA*

Mentor: Prof. Dawn Song

EDUCATION

University of Maryland, College Park, MD
Ph.D., in Electrical and Computer Engineering, *Aug 2018*
Advisors: Charalampos Papamanthou and Jonathan Katz
Thesis: New (Zero-Knowledge) Arguments and Their Applications to Verifiable Computation

Chinese University of Hong Kong, Hong Kong
M.Phil., in Information Engineering, *July 2013*
Advisor: Wing Shing Wong

B.S., in Information Engineering, *July 2011*

INTERNSHIPS

Microsoft Research May 2017 to Aug. 2017
Summer internship *Redmond, WA*

Mentor: Dr. Ranjit Kumaresan

Visa Research May 2016 to Aug. 2016
Summer internship *Foster City, CA*

Mentor: Dr. Payman Mohassel

RSA Laboratories May 2015 to Aug. 2015
Summer internship *Boston, MA*

Mentor: Dr. Nikolaos Triandopoulos

Massachusetts Institute of Technology June 2010 - Sept 2010
Charles Kao Research Exchange Student *Cambridge, MA*
Mentor: Dr. Vincent W.S. Chan

PUBLICATIONS

1. Jiaheng Zhang, Tiancheng Xie, **Yupeng Zhang** and Dawn Song, Transparent Polynomial Delegation and Its Applications to Zero Knowledge Proof To appear at *IEEE Symposium on Security and Privacy* (S&P), 2020.
2. Sai Krishna Deepak Maram, Fan Zhang, Lun Wang, Andrew Low, **Yupeng Zhang**, Ari Juels and Dawn Song, CHURP: Dynamic-Committee Proactive Secret Sharing In *Proceeding of the 2019 ACM Conference on Computer and Communications Security (CCS)*, 2019.
3. Tiancheng Xie, Jiaheng Zhang, **Yupeng Zhang**, Charalampos Papamanthou and Dawn Song, Libra: Succinct Zero-Knowledge Proofs with Optimal Prover Computation. In *Proceeding of International Cryptology Conference (CRYPTO)*, 2019.
4. **Yupeng Zhang**, Daniel Genkin, Jonathan Katz, Dimitris Papadopoulos and Charalampos Papamanthou, vRAM: Faster Verifiable RAM With Program-Independent Preprocessing. In *Proceeding of IEEE Symposium on Security and Privacy* (S&P), 2018.
5. **Yupeng Zhang**, Charalampos Papamanthou and Jonathan Katz, Verifiable Graph Processing. In *ACM Transactions on Privacy and Security (TOPS)*, 2018.
6. **Yupeng Zhang**, Daniel Genkin, Jonathan Katz, Dimitris Papadopoulos and Charalampos Papamanthou, vSQL: Verifying Arbitrary SQL Queries over Dynamic Outsourced Databases. In *Proceeding of IEEE Symposium on Security and Privacy (S&P)*, 2017.
7. Payman Mohassel and **Yupeng Zhang**, SecureML: A System for Scalable Privacy-Preserving Machine Learning. In *Proceeding of IEEE Symposium on Security and Privacy (S&P)*, 2017.
8. **Yupeng Zhang**, Jonathan Katz and Charalampos Papamanthou, An Expressive (Zero-Knowledge) Set Accumulator. In *Proceeding of IEEE European Symposium on Security and Privacy (Euro S&P)*, 2017.
9. **Yupeng Zhang**, Jonathan Katz and Charalampos Papamanthou, All Your Queries Are Belong to Us: The Power of File-Injection Attacks on Searchable Encryption. In *Proceeding of 25th USENIX Security Symposium (USENIX Security 16)*, 2016.
10. Zhe Zhou, Tao Zhang, Sherman SM Chow, **Yupeng Zhang**, and Kehuan Zhang, Efficient Authenticated Multi-Pattern Matching in *Proceeding of the 2016 ACM on Aisa Conference on Computer and Communications Security (AsiaCCS)*. 2016.
11. **Yupeng Zhang**, Jonathan Katz and Charalampos Papamanthou, IntegriDB: Verifiable SQL for Outsourced Databases. In *Proceeding of the 2015 ACM Conference on Computer and Communications Security (CCS)*, 2015.
12. **Yupeng Zhang**, Charalampos Papamanthou and Jonathan Katz, ALITHEIA: Towards Practical Verifiable Graph Processing. In *Proceeding of the 2014 ACM Conference on Computer and Communications Security (CCS)*, 2014.
13. Yi Qian, **Yupeng Zhang**, Xi Chen and Charalampos Papamanthou, Streaming Authenticated Data Structures: Abstraction and Implementation. In *Proceeding of the ACM Cloud Computing Security Workshop (CCSW)*, 2014.

14. **Yupeng Zhang** and Wing Shing Wong, Distributed Load Balancing in a Multiple Server System by Shift-Invariant Protocol Sequences. In *Proceeding of the IEEE Wireless Communications and Networking Conference (WCNC)*, 2013.

15. **Yupeng Zhang**, John Chapin and Vincent W.S. Chan, Failure of TCP Congestion Control under Diversity Routing. In *Proceeding of the IEEE Wireless Communications and Networking Conference (WCNC)*, 2011.

16. **Yupeng Zhang**, Daniel Genkin, Jonathan Katz, Dimitris Papadopoulos and Charalampos Papamanthou, A Zero-Knowledge Version of the Argument of vSQL. *Cryptology ePrint Archive*, Report 2017/1146.

AWARDS

- ACM SIGSAC Doctoral Dissertation Award Runner-up *2019*
- ECE Distinguished Dissertation Award, University of Maryland *2018*
- Google PhD Fellowship (33 recipients, 3 in cybersecurity, from all universities in North America, Europe and the Middle East) *2017*
- Facebook Fellowship Finalist (38 out of 800) *2017*
- 2nd place in iDASH Privacy & Security Competition *Nov 2017*
- Outstanding Graduate Assistant, University of Maryland (4 out of 255) *May 2017*
- Future Faculty Program, University of Maryland *Jan 2016*
- College Certificate of Academic Merit, Chinese University of Hong Kong *Sept 2011*
- Dean's list of Engineering, Chinese University of Hong Kong *2007 - 2011*
- Charles Kao Research Scholarship, Chinese University of Hong Kong *June 2011*
- Full scholarship for studying at CUHK, Chinese University of Hong Kong *Sept 2007*

SERVICE

- Program Committee: PoPETs 2020, AsiaCCS 2020, CCS 2019, ISC 2019, ACSAC 2019, WWW 2017
- Reviewer for PoPETs 2017, 2018, 2019.
- Reviewer for Transactions on Information Forensics & Security (TIFS), Transactions on Dependable and Secure Computing (TDSC), Transactions on Knowledge and Data Engineering (TKDE), Designs, Codes and Cryptography (DESI).
- Student Program Committee, IEEE Symposium on Security and Privacy (S&P) 2016.
- External reviewer for: S&P 2018, 2019; CCS 2015, 2016, 2018; NDSS 2016, 2017, 2018; Crypto 2016, 2017; SCC 2016; TISSEC 2016; ACNS 2015; ISC 2014; WPES 2014.

INVITED TALKS

- *Zero Knowledge Proofs*
  Facebook Inc. July 2019
  Visa Research, June 2019

- *Privacy-preserving Machine Learning*
  Princeton University, Nov 2017
  US Census Bureau, Nov 2017
  University of California, Berkeley, Aug 2017
- *Verifiable Databases and RAM Programs*
  Massachusetts Institute of Technology, Feb 2018
  Stanford University, Aug 2017
  DIMACS workshop on Outsourcing Computation Securely, July 2017
- *Secure De-duplication for Global Alliance for Genomics and Health (GA4GH) Data*
  iDASH Privacy & Security Workshop, 2017
- *Verifiable Databases*
  University of Pennsylvania, April 2017
- *Attacks on Searchable Encryption*
  Cornell University, April 2016
  DCAPS workshop, Feb 2016

TEACHING EXPERIENCE

CSCE465: Computer and Network Security, Texas A&M	*Spring 2020*
CSCE689: Techniques in Applied Cryptography, Texas A&M	*Fall 2019*
CS294-151: Blockchain and CryptoEconomics (Instructor), UC Berkeley	*Fall 2018*
ENEE459P Parallel Algorithms (Grader)	*Fall 2014*
IERG3010 Digital Communication (Teaching Assistant)	*Spring 2012*
ENGG2040 Introduction to Probability (Teaching Assistant)	*Spring 2011*
IERG1810 Digital Circuit Design Laboratory (Teaching Assistant)	*Fall 2011 & 2012*