

Yupeng Zhang

CONTACT INFORMATION Coordinated Science Laboratory 468, Phone: 217-244-7595
1308 W Main St, Email: zhangyp@illinois.edu
Urbana, IL 61801 Web: <https://zhangyp.web.illinois.edu/>

RESEARCH INTERESTS Applied Cryptography and Security. Zero-knowledge Proofs (ZKP), Secure
Multiparty Computations (MPC), and their applications in Blockchain and
Machine learning privacy, scalability and fairness.

PROFESSIONAL APPOINTMENTS **University of Illinois Urbana-Champaign** Champaign, IL
Assistant Professor *Aug. 2023 – present*
Department of Electrical and Computer Engineering
Department of Computer Science (affiliate)

Texas A&M University College Station, TX
Assistant Professor *Aug. 2019 – Aug. 2023*
Department of Computer Science and Engineering

University of California, Berkeley Berkeley, CA
Postdoctoral Researcher *Sep. 2018 – Aug. 2019*
Mentor: Prof. Dawn Song

EDUCATION **University of Maryland** College Park, MD
Ph.D. in Electrical and Computer Engineering *Aug 2018*
Advisors: Prof. Charalampos Papamanthou and Prof. 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: Prof. Wing Shing Wong

B.S. in Information Engineering *July 2011*

PUBLICATIONS (*) denotes Zhang’s Ph.D. students and mentees. Summary: 10 in CCS, 5 in S&P, 3 in USENIX Security, 2 in Crypto.

PEER-REVIEWED
CONFERENCE

1. **Pianist: Scalable zkRollups via Fully Distributed Zero-Knowledge Proofs.** Tianyi Liu*, Tiancheng Xie*, Jiaheng Zhang*, Dawn Song and Yupeng Zhang. To appear at *IEEE Symposium on Security and Privacy (S&P)*, 2024.
2. **Private Polynomial Commitments and Applications to MPC.** Rishabh Bhaduria, Carmit Hazay, Muthuramakrishnan Venkitasubramaniam, Wenxuan Wu* and Yupeng Zhang. In *Proceedings of the IACR International Conference on Public-Key Cryptography (PKC)*, 2023.
3. **zkBridge: Trustless Cross-chain Bridges Made Practical.** Tiancheng Xie*, Jiaheng Zhang*, Zerui Cheng, Fan Zhang, Yupeng Zhang, Yongzheng Jia and Dawn Song. In *Proceedings of the 2022 ACM Conference on Computer and Communications Security (CCS)*, 2022.
4. **Orion: Zero Knowledge Proof with Linear Prover Time.** Tiancheng Xie*, Yupeng Zhang and Dawn Song. In *Proceedings of the Annual International Cryptology Conference (CRYPTO)*, 2022.
5. **Hyperproofs: Aggregating and Maintaining Proofs in Vector Commitments.** Shravan Srinivasan, Alex Chepurnoy, Charalampos Papamanthou, Alin Tomescu and Yupeng Zhang. In *Proceedings of the USENIX Security Symposium (USENIX Security)*, 2022.
6. **Polynomial Commitment with a One-to-Many Prover and Applications.** Jiaheng Zhang*, Tiancheng Xie*, Thang Hoang, Elaine Shi and Yupeng Zhang. In *Proceedings of the USENIX Security Symposium (USENIX Security)*, 2022.
7. **Zero Knowledge Static Program Analysis.** Zhiyong Fang*, David Darais, Joseph Near and Yupeng Zhang. In *Proceedings of the 2021 ACM Conference on Computer and Communications Security (CCS)*, 2021.
8. **zkCNN: Zero Knowledge Proofs for Convolutional Neural Network Predictions and Accuracy.** Tianyi Liu*, Xiang Xie and Yupeng Zhang. In *Proceedings of the 2021 ACM Conference on Computer and Communications Security (CCS)*, 2021.
9. **Doubly Efficient Interactive Proofs for General Arithmetic Circuits with Linear Prover Time.** Jiaheng Zhang*, Tianyi Liu*, Weijie Wang*, Yinuo Zhang*, Dawn Song, Xiang Xie and Yupeng Zhang. In *Proceedings of the 2021 ACM Conference on Computer and Communications Security (CCS)*, 2021.
10. **ZKPlus: Optimized Fair-exchange Protocol Supporting Practical and Flexible Data Exchange.** Yun Li, Cun Ye, Yuguang Hu, Ivring Morpheus, Yu Guo, Chao Zhang, Yupeng Zhang, Zhipeng Sun, Yiwen Lu and Haodi Wang. In *Proceedings of the 2021 ACM Conference on Computer and Communications Security (CCS)*, 2021.

11. **Zero Knowledge Proofs for Decision Tree Predictions and Accuracy.** Jiaheng Zhang*, Zhiyong Fang*, Yupeng Zhang and Dawn Song. In *Proceedings of the 2020 ACM Conference on Computer and Communications Security (CCS)*, 2020.
12. **Ligero++: A New Optimized Sublinear IOP.** Rishabh Bhadauria, Zhiyong Fang*, Carmit Hazay, Muthuramakrishnan Venkitasubramaniam, Tiancheng Xie* and Yupeng Zhang (alphabetical order). In *Proceedings of the 2020 ACM Conference on Computer and Communications Security (CCS)*, 2020.
13. **Transparent Polynomial Delegation and Its Applications to Zero Knowledge Proof.** Jiaheng Zhang*, Tiancheng Xie*, Yupeng Zhang and Dawn Song. In *Proceedings of IEEE Symposium on Security and Privacy (S&P)*, 2020.
14. **CHURP: Dynamic-Committee Proactive Secret Sharing.** Sai Krishna Deepak Maram, Fan Zhang, Lun Wang, Andrew Low, Yupeng Zhang, Ari Juels and Dawn Song. In *Proceedings of the 2019 ACM Conference on Computer and Communications Security (CCS)*, 2019.
15. **Libra: Succinct Zero-Knowledge Proofs with Optimal Prover Computation.** Tiancheng Xie*, Jiaheng Zhang*, Yupeng Zhang, Charalampos Papamanthou and Dawn Song. In *Proceedings of the Annual International Cryptology Conference (CRYPTO)*, 2019.
16. **vRAM: Faster Verifiable RAM With Program-Independent Pre-processing.** Yupeng Zhang, Daniel Genkin, Jonathan Katz, Dimitris Papadopoulos and Charalampos Papamanthou. In *Proceedings of IEEE Symposium on Security and Privacy (S&P)*, 2018.
17. **vSQL: Verifying Arbitrary SQL Queries over Dynamic Outsourced Databases.** Yupeng Zhang, Daniel Genkin, Jonathan Katz, Dimitris Papadopoulos and Charalampos Papamanthou. In *Proceedings of IEEE Symposium on Security and Privacy (S&P)*, 2017.
18. **SecureML: A System for Scalable Privacy-Preserving Machine Learning.** Payman Mohassel and Yupeng Zhang. In *Proceedings of IEEE Symposium on Security and Privacy (S&P)*, 2017.
19. **An Expressive (Zero-Knowledge) Set Accumulator.** Yupeng Zhang, Jonathan Katz and Charalampos Papamanthou. In *Proceedings of IEEE European Symposium on Security and Privacy (Euro S&P)*, 2017.
20. **All Your Queries Are Belong to Us: The Power of File-Injection Attacks on Searchable Encryption.** Yupeng Zhang, Jonathan Katz and Charalampos Papamanthou. In *Proceedings of 25th USENIX Security Symposium (USENIX Security)*, 2016.
21. **Efficient Authenticated Multi-Pattern Matching.** Zhe Zhou, Tao Zhang, Sherman SM Chow, Yupeng Zhang, and Kehuan Zhang. in *Proceedings of the 2016 ACM Aisa Conference on Computer and Communications Security (AsiaCCS)*. 2016.

22. **IntegriDB: Verifiable SQL for Outsourced Databases.** Yupeng Zhang, Jonathan Katz and Charalampos Papamanthou. In *Proceedings of the 2015 ACM Conference on Computer and Communications Security (CCS)*, 2015.
23. **ALITHEIA: Towards Practical Verifiable Graph Processing.** Yupeng Zhang, Charalampos Papamanthou and Jonathan Katz. In *Proceedings of the 2014 ACM Conference on Computer and Communications Security (CCS)*, 2014.
24. **Streaming Authenticated Data Structures: Abstraction and Implementation.** Yi Qian, Yupeng Zhang, Xi Chen and Charalampos Papamanthou. In *Proceedings of the ACM Cloud Computing Security Workshop (CCSW)*, 2014.
25. **Distributed Load Balancing in a Multiple Server System by Shift-Invariant Protocol Sequences.** Yupeng Zhang and Wing Shing Wong. In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, 2013.
26. **Failure of TCP Congestion Control under Diversity Routing.** Yupeng Zhang, John Chapin and Vincent W.S. Chan. In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, 2011.

JOURNAL

1. **Verifiable Graph Processing.** Yupeng Zhang, Charalampos Papamanthou and Jonathan Katz. In *ACM Transactions on Privacy and Security (TOPS)*, 2018.

IN SUBMISSION

1. **Confidential and Verifiable Machine Learning Delegations on the Cloud.** Wenxuan Wu*, Soamar Homsni and Yupeng Zhang. In submission to PoPETs 2024. *Cryptology ePrint Archive*, Report 2024/537.
2. **Field-Agnostic SNARKs from Expand-Accumulate Codes.** Alexander R. Block, Zhiyong Fang*, Jonathan Katz, Justin Thaler, Hendrik Waldner, Yupeng Zhang (alphabetical order). In submission to Crypto 2024.
3. **TensorPlonk: A Fast, General ZK Proving System for ML Inference.** Suppakit Waiwitlikhit, Yupeng Zhang, Daniel Kang. In submission to CCS 2024.

PREPRINTS

1. **Edrax: A Cryptocurrency with Stateless Transaction Validation.** Alexander Chepurnoy, Charalampos Papamanthou, Shravan Srinivasan and Yupeng Zhang. *Cryptology ePrint Archive*, Report 2018/968.
2. **A Zero-Knowledge Version of the Argument of vSQL.** Yupeng Zhang, Daniel Genkin, Jonathan Katz, Dimitris Papadopoulos and Charalampos Papamanthou. *Cryptology ePrint Archive*, Report 2017/1146.

RESEARCH
GRANTS

Summary: \$1.68 million in total. My share is \$1.42 million.

- Google Research Scholar Award
Proof of Training and its Applications in Machine Unlearning and Differential Privacy
PI, Period: Sep 2024 – Aug 2025, \$60,000.
- National Science Foundation (NSF) CAREER Award
Towards Efficient and Scalable Zero-Knowledge Proofs
PI, Period: Sep 2022 – Aug 2027, \$500,000.
- Air Force Research Lab (AFRL), Rome, NY
Machine Learning on RESCU Cloud via MPC and ZKP Techniques
PI, Period: Jan 2022 – Sep 2024, \$473,142. Co-PI: Juan Garay
- Defense Advanced Research Projects Agency (DARPA)
SIEVE: Wizkit: Wide-scale Zero-Knowledge Interpreter Toolkit
PI, Period: Jan 2021 – Apr 2024, \$400,000.
- Facebook Faculty Research Award
Privacy-Preserving Machine Learning via Alternating Direction Method of Multipliers
PI, Period: Sep 2021 – Sep 2022, \$100,000.
- Texas A&M Triads for Transformation program
Error-Correcting Code with Applications to Efficient Cryptographic Proof Systems
PI, Period: Jan 2021 – Dec 2022, \$30,000. Co-PI: Chao Tian, Wencai Liu
- Latticex Foundation Research Award
PI, Period: Sep 2020 – Sep 2021, \$120,000.

AWARDS

- Google Research Scholar Award 2024
 - NSF CAREER Award 2022
 - Facebook Faculty Research Award 2021
 - ACM SIGSAC Doctoral Dissertation Award Runner-up 2019
 - ECE Distinguished Dissertation Award, University of Maryland 2018
 - Google PhD Fellowship 2017
 - Facebook Fellowship Finalist (38 out of 800) 2017
 - 2nd place in iDASH Privacy & Security Competition 2017
 - Outstanding Graduate Assistant, University of Maryland 2017
 - Charles Kao Research Scholarship, Chinese University of Hong Kong 2011
-

STUDENTS

- *PhD Students*
 - Ruofan Xu (2023 –)
 - Tianyi Liu (2021 –)
 - Zhiyong Fang (2019 –) expected graduation: summer 2024
 - Wenxuan Wu (2019 –) expected graduation: summer 2024
 - *Mentees*
 - Jiaheng Zhang (2018 – 2023). Now Assistant Professor at National University of Singapore
 - Tiancheng Xie (2018 – 2023). Now CTO at Polyhedra.
 - *Master's Students*
 - Fatima Elsheimy (2021 – 2022), co-advised with Prof. Juan Garay. Now Ph.D. at Yale University
 - *Undergraduate Students*
 - Yupeng Ouyang, (Spring 2024).
 - Daniel Vilardell, (Fall 2023). Incoming Ph.D. at Cornell
 - Hanson Yu (Spring 2022). Now master's student at Texas A&M
 - Yinuo Zhang (Summer 2020). Now Ph.D. at UC Berkeley
 - Weijie Wang (Summer 2020). Now Ph.D. at Yale University
 - Yunuo Min (Fall 2020) Now master's student at Texas A&M
 - Skyler Zheng (Fall 2019). Now Software Engineer at Pinterest
-

TEACHING EXPERIENCE

Massive open online course (MOOC) on zero-knowledge proofs *Spring 2023*
<https://zk-learning.org/>, Enrollment: 4000+

University of Illinois Urbana-Champaign, IL

- ECE/CS407: Cryptography *Spring 2024*
Enrollment: 60
- ECE598: Advanced Topics in Applied Cryptography *Fall 2023*
Enrollment: 14

Texas A&M University, College Station, TX

- CSCE465: Computer and Network Security *Fall 2022*
Enrollment: 93
- CSCE749: Introduction to Applied Cryptography *Spring 2022*
Enrollment: 29
- CSCE465: Computer and Network Security *Fall 2021*
Enrollment: 59

- CSCE489/689: Techniques in Applied Cryptography *Spring 2021*
Enrollment: 27
- CSCE465: Computer and Network Security *Spring 2020*
Enrollment: 55
- CSCE689: Techniques in Applied Cryptography *Fall 2019*
Enrollment: 13

University of California, Berkeley, CA

- CS294-151: Blockchain and CryptoEconomics (Instructor) *Fall 2018*

University of Maryland, College Park, MD

- ENEE459P Parallel Algorithms (Teaching Assistant) *Fall 2014*

Chinese University of Hong Kong, Hong Kong

- IERG3010 Digital Communication (Teaching Assistant) *Spring 2012*
- ENGG2040 Introduction to Probability (Teaching Assistant) *Spring 2011*
- IERG1810 Digital Circuit Design (Teaching Assistant) *Fall 2011 & 2012*

PROFESSIONAL
ACTIVITIES

- Program Co-Chair:
 - USENIX Security 2024, Program Vice Co-Chair
 - WEB3SEC Workshop, affiliated with ACSAC 2022
 - Zero-Knowledge Proof Workshop, affiliated with CESC 2022
- Program Committee:
 - Crypto 2024
 - SBC 2024
 - ACM Conference on Computer and Communications Security (CCS) 2019, 2021-2023
 - USENIX Security 2023
 - Asiacrypt 2023
 - Privacy Enhancing Technologies Symposium (PoPETs) 2020, 2021, 2022
 - Financial Cryptography and Data Security (FC) 2022, 2023
 - Crypto Economics Security Conference (CESC) 2022
 - ACM Aisa Conference on Computer and Communications Security (AsiaCCS) 2020,2021
 - Annual Computer Security Applications Conference (ACSAC) 2019, 2020
 - Information Security Conference (ISC) 2019
 - World Wide Web Conference (WWW) 2017
- Journal Referee:

- 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).

INTERNSHIP
EXPERIENCE

- Microsoft Research** Redmond, WA
Summer internship *May 2017 to Aug. 2017*
 Mentor: Dr. Ranjit Kumaresan
- Visa Research** Foster City, CA
Summer internship *May 2016 to Aug. 2016*
 Mentor: Dr. Payman Mohassel
- RSA Laboratories** Boston, MA
Summer internship *May 2015 to Aug. 2015*
 Mentor: Dr. Nikolaos Triandopoulos
-

INVITED
TALKS

- **Zero Knowledge Proofs for Machine Learning**
 Coinbase Machine Learning & Blockchain Research Summit, May 2024
 Carnegie Mellon University, October 2022
 Facebook, December 2021
 Visa Research, August 2021
 Monash University, July 2021
 Keynote at PPML Workshop, CCS 2020
- **Efficient Zero Knowledge Proofs Schemes**
 Google, October 2022
 Facebook, 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
-