

YUPENG ZHANG

CONTACT INFORMATION

Email: zhangyp@umd.edu
Phone: 240-565-8204

Web: <http://www.umiacs.umd.edu/~zhangyp>

RESEARCH INTERESTS

Applied Cryptography, Security and Privacy.

EDUCATION

University of Maryland – College Park

Ph.D. in Electrical and Computer Engineering

Sept 2013 – May 2018 (expected)

Advisors: Jonathan Katz and Charalampos (Babis) Papamanthou

Recipient of the 2017 **Google Ph.D. fellowship**

Chinese University of Hong Kong

M.Phil. in Information Engineering

July 2013

Advisor: Wing Shing Wong

B.S. in Information Engineering

July 2011

PUBLICATIONS

1. **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. (To appear)
2. **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. (Acceptance rate: 13.3%)
3. 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. (Acceptance rate: 13.3%) (author names in alphabetical order)
4. **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. (Acceptance rate: 19.5%)
5. **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)*, 2016. (Acceptance rate: 15.5%)
6. Zhe Zhou, Tao Zhang, Sherman SM Chow, **Yupeng Zhang**, and Kehuan Zhang, Efficient Authenticated Multi-Pattern Matching. In *Proceeding of the 2016 ACM on Asia Conference on Computer and Communications Security (AsiaCCS)*, 2016. (Acceptance rate: 23.1%)

7. **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. (Acceptance rate: 19.3%)
8. **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. (Acceptance rate: 19.5%)
9. 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.
10. **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.
11. **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.
12. **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

- Google PhD Fellowship (33 recipients, 3 in cybersecurity, 2017
from all universities in North America, Europe and the Middle East)
- 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
- Deans 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, World Wide Web Conference (**WWW**) 2017, security and privacy track.
- Reviewer for PoPETs 2017, 2018.
- Reviewer for Transactions on Information Forensics & Security.
- Student Program Committee, IEEE Symposium on Security and Privacy (S&P) 2016.
- External reviewer for: S&P 2018; CCS 2015, 2016; NDSS 2016, 2017, 2018; Crypto 2016, 2017; SCC 2016; TISSEC 2016; ACNS 2015; ISC 2014; WPES 2014.

INTERNSHIPS

Microsoft Research <i>Summer internship</i>	May 2017 to Aug 2017 <i>Redmond, WA</i>
Mentor: Dr. Ranjit Kumaresan <i>Secure de-duplication on distributed datasets</i>	
Visa Research <i>Summer internship</i>	May 2016 to Aug 2016 <i>Foster City, CA</i>
Mentor: Dr. Payman Mohassel <i>Privacy-preserving machine learning</i>	
RSA Laboratories <i>Summer internship</i>	May 2015 to Aug 2015 <i>Boston, MA</i>
Mentor: Dr. Nikolaos Triandopoulos <i>Password-based secret sharing</i>	
Massachusetts Institute of Technology <i>Charles Kao Research Exchange Student</i>	June 2010 - Sept 2010 <i>Cambridge, MA</i>
Mentor: Dr. Vincent W.S. Chan <i>TCP congestion control in satellite networks</i>	

INVITED TALKS

- *Privacy-preserving Machine Learning*
Princeton University, Nov 2017
US Census Bureau, Nov 2017
University of California, Berkeley, Aug 2017
- *Verifiable Databases and RAM Programs*
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

ELE 574 Guest Lecture on Privacy-preserving Machine Learning, Princeton University	<i>Nov 2017</i>
ENEE459P Parallel Algorithms (Teaching Assistant)	<i>Fall 2014</i>
IERG3010 Digital Communication (Teaching Assistant)	<i>Spring 2012</i>
ENGG2040 Introduction to Probability (Teaching Assistant)	<i>Spring 2011</i>
IERG1810 Digital Circuit Design Laboratory (Teaching Assistant)	<i>Fall 2011 & 2012</i>

REFERENCES

Jonathan Katz

Professor
Department of Computer Science and UMIACS
University of Maryland
jkatz@cs.umd.edu

Charalampos (Babis) Papamanthou

Assistant Professor
Department of Electrical and Computer Engineering and UMIACS
University of Maryland
cpap@umd.edu

Payman Mohassel

Principal Research Scientist
Visa Research
payman.mohassel@gmail.com

Bryan Parno

Associate Professor
Department of Computer Science and Electrical Computer Engineering
Carnegie Mellon University
parno@cmu.edu