Xiao Wang

wangxiao@cs.northwestern.edu http://cs.northwestern.edu/~wangxiao/

Education

- University of Maryland, College Park, 2018
  Ph.D. in Computer Science
  Dissertation: *A New Paradigm For Practical Maliciously Secure Multi-Party Computation*
  Adviser: Jonathan Katz
- The Hong Kong University of Science and Technology, 2013
  Bachelor of Engineering in Computer Science, First Class Honors
  Adviser: Ke Yi

Employment History

08/2019 - Now	Assistant Professor of Computer Science at Northwestern University, Evanston
09/2018 to 07/2019	Postdoctoral Researcher at MIT and Boston University, Boston with Vinod Vaikuntanathan and Ran Canetti
Summer, 2017	Internship at Bell Labs, Murray Hill with Vladimir Kolesnikov
Summer, 2015	Internship at SRI International, Menlo Park with Mariana Raykova
Summer, 2014	Internship at Technicolor Research, Los Altos with Nina Taft, Stratis Ioannidis, and Udi Weinsberg

Publications

[1] Chun Guo, Jonathan Katz, Xiao Wang, and Yu Yu. Efficient and Secure Multiparty Computation from Fixed-key Block Ciphers. In *IEEE Symposium on Security and Privacy (S&P)*, 2020

[2] Vladimir Kolesnikov, Mike Rosulek, Ni Trieu, and Xiao Wang. Scalable Private Set Union from Symmetric-Key Techniques. In *Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacypt)*, 2019

[3] Cheng Hong, Jonathan Katz, Vladimir Kolesnikov, Wen jie Lu, and Xiao Wang. Covert Security with Public Verifiability: Faster, Leaner, and Simpler. Advances in Cryptology – EUROCRYPT: Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2019

[4] Jonathan Katz, Vladimir Kolesnikov, and Xiao Wang. Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures. In *ACM Conference on Computer and Communications Security (CCS)*, 2018

[5] S. Dov Gordon, Jonathan Katz, and Xiao Wang. Simple and Efficient Two-Server ORAM. In *Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacypt)*, 2018

[6] S. Dov Gordon, Samuel Ranellucci, and Xiao Wang. Secure Computation with Low Communication from Cross-checking. In *Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacypt)*, 2018

[7] Jonathan Katz, Samuel Ranellucci, Mike Rosulek, and Xiao Wang. Optimizing Authenticated Garbling for Faster Secure Two-Party Computation. In *International Cryptology Conference (CRYPTO)*, 2018

[8] Xiao Wang, Samuel Ranellucci, and Jonathan Katz. Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation. In *ACM Conference on Computer and Communications Security (CCS)*, 2017, **Best Paper Award**

[9] Xiao Wang, Samuel Ranellucci, and Jonathan Katz. Global-Scale Secure Multiparty Computation. In *ACM Conference on Computer and Communications Security (CCS)*, 2017

[10] Xiao Wang, Alex J. Malozemoff, and Jonathan Katz. Faster Secure Two-Party Computation in the Single-Execution Setting. Advances in Cryptology – EUROCRYPT: Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2017

[11] Xiao Wang, S. Dov Gordon, Allen McIntosh, and Jonathan Katz. Secure Computation of MIPS Machine Code. In *European Symposium on Research in Computer Security (ESORICS)*, 2016

[12] Samee Zahur, Xiao Wang, Mariana Raykova, Adria Gascon, Jack Doerner, David Evans, and Jonathan Katz. Revisiting Square Root ORAM: Efficient Random Access in Multi-Party Computation. In *IEEE Symposium on Security and Privacy (S&P)*, 2016

[13] Justin Wagner, Joseph N Paulson, Xiao Wang, Bobby Bhattacharjee, and Hector Corrada Bravo. Privacy-Preserving Microbiome Analysis Using Secure Computation. In *Bioinformatics*, 2016

[14] Xiao Wang, T-H. Hubert Chan, and Elaine Shi. Circuit ORAM: On Tightness of the Goldreich-Ostrovsky Lower Bound. In *ACM Conference on Computer and Communications Security (CCS)*, 2015

[15] Xiao Wang, Yan Huang, Yongan Zhao, Haixu Tang, XiaoFeng Wang, and Diyue Bu. Efficient Genome-Wide, Privacy-Preserving Similar Patient Query based on Private Edit Distance. In *ACM Conference on Computer and Communications Security (CCS)*, 2015

[16] Kartik Nayak, Xiao Wang, Stratis Ioannidis, Udi Weinsberg, Nina Taft, and Elaine Shi. GraphSC: Parallel Secure Computation Made Easy. In *IEEE Symposium on Security and Privacy (S&P)*, 2015

[17] Chang Liu, Xiao Wang, Kartik Nayak, Yan Huang, and Elaine Shi. ObliVM: A Programming Framework for Secure Computation. In *IEEE Symposium on Security and Privacy (S&P)*, 2015

[18] Xiao Wang, Yan Huang, T.H. Hubert, abhi shelat, and Elaine Shi. SCORAM: Oblivious RAM for Secure Computation. In *ACM Conference on Computer and Communications Security (CCS)*, 2014

[19] Xiao Wang, Kartik Nayak, Chang Liu, T.H. Hubert, Elaine Shi, Emil Stefenov, and Yan Huang. Oblivious Data Structures. In *ACM Conference on Computer and Communications Security (CCS)*, 2014

Selected Talks

1. DIMACS/MACS Workshop on Usable, Efficient, and Formally Verified Secure Computation (Boston, MA): "Efficient and Secure Multiparty Computation from Fixed-Key Block Ciphers", 2019
2. Cryptography and Information Security Seminars at MIT (Boston, MA): "Covert Security with Public Verifiability: Simpler, Faster, and Leaner, 2018
3. IBM Research Cryptography Seminar Series (Yorktown Heights, NY): "Authenticated Garbling: Efficient Maliciously Secure Two-Party Computation and Global-Scale Secure Multiparty Computation", 2018
4. ACM Conference on Computer and Communications Security (Dallas, TX): "Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation", 2017.
5. ACM Conference on Computer and Communications Security (Dallas, TX): "Global-Scale Secure Multiparty Computation", 2017.
6. EUROCRYPT (Paris, France): "Faster Secure Two-Party Computation in the Single-Execution Setting", 2017.
7. Theory and Practice of Multi-Party Computation Workshop (Bristol, UK): "Authenticated Garbling and Efficient Maliciously Secure 2PC and MPC", 2017.
8. Seminar talk at Bell Labs (Murray Hill, NJ): "Efficient Genome-Wide, Privacy-Preserving Similar Patient Query based on Private Edit Distance", 2017.

9. Invited talk at iDASH Privacy & Security Workshop (Chicago, IL): "Privacy Preserving Top-k Search on Genome Data", 2016.
10. DC Area Anonymity/Privacy/Security Seminar (Washington, D.C.): "Faster Two-Party Computation Secure Against Malicious Adversaries in the Single-Execution Setting", 2016.
11. European Symposium on Research in Computer Security (Crete, Greece): "Secure Computation of MIPS Machine Code", 2016.
12. ACM Conference on Computer and Communications Security (Denver, CO): "Circuit ORAM: On Tightness of the Goldreich-Ostrovsky Lower Bound", 2015.
13. ACM Conference on Computer and Communications Security (Denver, CO): "Efficient Genome-Wide, Privacy-Preserving Similar Patient Query based on Private Edit Distance", 2015.
14. ACM Conference on Computer and Communications Security (Scottsdale, AZ): "SCORAM:Oblivious RAM for Secure Computation", 2014.

Selected Awards

1. Larry S. Davis Dissertation Award, Department of Computer Science, University of Maryland, 2018
2. Best Paper Award in ACM Symposium on Computer and Communications Security, 2017
3. Human Longevity, Inc. and Genecloud Award for iDASH Genome Privacy & Security Competition, 2016
4. Future Faculty Fellow, University of Maryland, 2016
5. First place in the NYU Polytechnic School of Engineering's CSAW Best Applied Security Paper, 2015
6. Human Longevity, Inc. Award for Secure Multiparty Computing, 2015
7. Finalist (Top 10) in the NYU Polytechnic School of Engineering's CSAW Best Applied Security Paper, 2014

Students and Vistors

Ph.D. student

1. Chenkai Weng, Ph.D. student (2019 -)

Visitors

1. Kaiyi Zhang, Undergraduate visitor from Shanghai JiaoTong University (08/2019 - 01/2020)
2. Xiao Lan, Visitor from Sichuan University (09/2019 - 08/2020)

Professional Activities

Program committees

- IEEE Symposium on Security and Privacy (S&P) 2020
- ACM Asia Conference on Computer and Communications Security (AsiaCCS) 2020
- International Cryptology Conference (CRYPTO) 2019
- ACM Symposium on Computer and Communications Security (CCS) 2019
- Information Security Conference (ISC) 2019
- ACM Workshop on Privacy Preserving Machine Learning (PPML) 2019
- ACM Cloud Computing Security Workshop (CCSW) 2019
- IEEE Military Communications Conference (MILCOM) 2016 – 2018