Xiao Wang

wangxiao@northwestern.edu https://wangxiao1254.github.io

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 Northwestern University, Evanston, IL
09/2018 to 07/2019	Postdoctoral Researcher MIT and Boston University, Boston, MA with Vinod Vaikuntanathan and Ran Canetti
Summer, 2017	Internship Bell Labs, Murray Hill, NJ with Vladimir Kolesnikov
Summer, 2015	Internship SRI International, Menlo Park, CA with Mariana Raykova
Summer, 2014	Internship Technicolor Research, Los Altos, CA with Nina Taft, Stratis Ioannidis, and Udi Weinsberg

Selected Awards

1. JPMorgan Chase Faculty Research Award, 2023
2. Google Research Scholar, 2023
3. NSF CAREER award, 2023
4. Notable reviewer award, IEEE SaTML, 2023
5. Distinguished Paper Award in ACM Symposium on Computer and Communications Security (CCS), 2022
6. Research Mentor Award, Department of Computer Science, Northwestern University, 2022
7. Best Paper Award Runner-up in ACM Symposium on Computer and Communications Security (CCS), 2021
8. Larry S. Davis Dissertation Award, Department of Computer Science, University of Maryland, 2018
9. Best Paper Award in ACM Symposium on Computer and Communications Security (CCS), 2017
10. Human Longevity, Inc. and Genecloud Award for iDASH Genome Privacy & Security Competition, 2016
11. Future Faculty Fellow, University of Maryland, 2016
12. First place in the NYU Polytechnic School of Engineering's CSAW Best Applied Security Paper, 2015

13. Human Longevity, Inc. Award for Secure Multiparty Computing, 2015
14. Finalist (Top 10) in the NYU Polytechnic School of Engineering's CSAW Best Applied Security Paper, 2014
15. UMD Dean's fellowship 2013 - 2014
16. HKUST Academic Achievement Medal, Highest academic honor (top 1%), 2013
17. HKUST Outstanding Students Award, 2013
18. The Cheng Foundation Scholarships for Chinese Mainland Undergraduate Students, 2013
19. HKUST Academic Achievement Award for Graduating Students, 2013
20. HKUST Dean's list, all semesters, 2011 - 2013
21. National Scholarship, Ministry of Education (top 0.2%), 2009, 2010

Research Support

Sponsored support: 3.69M to NU (personal share: 2.28M). Non-sponsored support: 563K. Unless indicated otherwise, I am the sole PI at NU on the award.

Sponsored Research Projects

1. "CNS Core: Medium: Privacy-Preserving and Censorship-Resistant Domain Name Service" from **NSF**. With Aleksandar Kuzmanovic. 2023 - 2026. Total award to NU : $750K. My share (co-PI): $ 375K.
2. "Collaborative Research: FMitF: Track I: Automating and Synthesizing Parallel Zero-Knowledge Protocols" from **NSF**. 2023 - 2027. Total award: $300K.
3. "CAREER: Pushing the Practicality of Secure Multiparty Computation" from **NSF**. 2023 - 2028. Total award: $578K.
4. "Bringing Auditability to Privacy Preserving Electronic Health Record Aggregation using Zero Knowledge Proofs" from **DARPA**. Subcontract from Stealth Software Technologies, with Abel Kho and Jennie Rogers. 2023 - 2024. Total award to NU : $411K. My share (co-PI): $ 8K.

   Extension of the SIEVE grant below; most funding used for real-world MPC deployment at Feinberg School of Medicine.
5. "AFRL RESCU Cloud Secure and Verifiable SQL for the Zero Trust Cloud" from **AFRL**. With Jennie Rogers. 2021 - 2024. Total award to NU: $660K. My share (co-PI): $ 330K.
6. "Wizkit: Wide-Scale Zero-Knowledge Interpreter Toolkit" from **DARPA**. Subcontract from Stealth Software Technologies under Securing Information for Encrypted Verification and Evaluation (SIEVE), 2020 - 2024. Total award: $391K.
7. "Collaborative Research: SaTC: CORE: Medium: Quicksilver: A Write-oriented, Private, Outsourced Database Management System" from **NSF**. With Ashwin Machanavajjhala, Kartik Nayak, and Jennie Rogers. 2020 - 2024. Total award to NU: $600K. My share (co-PI): $300K.

Non-sponsored Research Awards

1. "Bridging Fiat and DeFi Services via Attested TLS" from **JPMorgan Chase Faculty Research Award**, 2023. Total award: $ 70K.
2. "Zero-Knowledge Proofs for Private and Transparent Machine Learning" from **Google Research Scholar Program**, 2023. Total award: $ 60K.
3. "Beyond FL: Truly Decentralized ML with Privacy and Robustness" from **Meta**. With Nicolas Papernot and Somesh Jha. 2022. Total award to NU: $33.3K.
4. "Privacy and Data Protection Office (PDPO) Faculty Award" from **Google**, 2021. Total award: $70K.

5. "Advance Existing 3rd Party Open Source PETs Software: EMP-toolkit" from **Facebook**, 2021. Total award: $160K.
6. " Chainlink Community Grants Program Research Award" from **ChainLink**, 2020. Total award: $30K.
7. "Machine Learning Based on Secure Multi-Party Computation" from **PlatON Network**, 2019. Total award: $140K.

Publications

Journal Articles

[6] Xiling Li, Chenkai Weng, Yongxin Xu, Xiao Wang, and Jennie Rogers. ZKSQL: Verifiable and Efficient Query Evaluation with Zero-Knowledge Proofs. In *Proceedings of the VLDB Endowment (PLVDB)*, 2023

[5] Adam Dziedzic, Christopher A. Choquette-Choo, Natalie Dullerud, Vinith Suriyakumar, Ali Shahin Shamsabadi, Muhammad Ahmad Kaleem, Somesh Jha, Nicolas Papernot, and Xiao Wang. Private Multi-Winner Voting for Machine Learning. In *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2023

[4] Xiao Lan, Hongjian Jin, Hui Guo, and Xiao Wang. Efficient and Secure Quantile Aggregation of Private Data Streams. In *IEEE Transactions on Information Forensics and Security (TIFS)*, 2023

[3] Chun Guo, Francois-Xavier Standaert, Weijia Wang, Xiao Wang, and Yu Yu. Provable Security of SP Networks with Partial Non-Linear Layers . In *IACR Transactions on Symmetric Cryptology (ToSC)*, 2021

[2] Johes Bater, Yongjoo Park, Xi He, Xiao Wang, and Jennie Rogers. SAQE: Practical Privacy-Preserving Approximate Query Processing for Data Federations. In *Proceedings of the VLDB Endowment (PLVDB)*, 2020

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

Articles in Refereed Conferences

[43] Yuyang Sang, Ning Luo, Samuel Judson, Ben Chaimberg, Timos Antonopoulos, Xiao Wang, Ruzica Piskac, and Zhong Shao. Ou: Automating the Parallelization of Zero-Knowledge Protocols. In *ACM Conference on Computer and Communications Security (CCS)*, 2023

[42] Xiaojie Guo, Kang Yang, Xiao Wang, Wenhao Zhang, Xiang Xie, Jiang Zhang, and Zheli Liu. Half-Tree: Halving the Cost of Tree Expansion in COT and DPF. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt)*, 2023

[41] Hongrui Cui, Xiao Wang, Kang Yang, and Yu Yu. Actively Secure Half-Gates with Minimum Overhead under Duplex Networks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt)*, 2023

[40] Ali Shahin Shamsabadi, Sierra Calanda Wyllie, Nicholas Franzese, Natalie Dullerud, Sebastien Gambs, Nicolas Papernot, Xiao Wang, and Adrian Weller. Confidential-PROFITT: Confidential PROof of FaIr Training of Trees . In *International Conference on Learning Representations (ICLR)*, 2023, **notable top 5%**

[39] Chenxi Liu, Lixu Wang, Lingjuan Lyu, Chen Sun, Xiao Wang, and Qi Zhu. Deja Vu: Continual Model Generalization for Unseen Domains . In *International Conference on Learning Representations (ICLR)*, 2023

[38] Vladimir Kolesnikov, Stanislav Peceny, Ni Trieu, and Xiao Wang. Fast ORAM with Server-aided Preprocessing and Pragmatic Privacy-Efficiency Trade-off. In *International Symposium on Cyber Security Cryptography and Machine Learning (CSCML)*, 2023

[37] Chenkai Weng, Kang Yang, Zhaomin Yang, Xiang Xie, and Xiao Wang. AntMan: Interactive Zero-Knowledge Proofs with Sublinear Communication. In *ACM Conference on Computer and Communications Security (CCS)*, 2022

[36] Ning Luo, Timos Antonopoulos, William Harris, Ruzica Piskac, Eran Tromer, and Xiao Wang. Proving UNSAT in Zero Knowledge . In *ACM Conference on Computer and Communications Security (CCS)*, 2022, **Distinguished Paper Award**

[35] Ning Luo, Samuel Judson, Timos Antonopoulos, Ruzica Piskac, and Xiao Wang. ppSAT: Towards Two-Party Private SAT Solving. In *USENIX Security*, 2022

[34] Kang Yang and Xiao Wang. Non-Interactive Zero-Knowledge Proofs to Multiple Verifiers. In *Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt)*, 2022

[33] Ran Canetti, Pratik Sarkar, and Xiao Wang. Triply Adaptive UC NIZK. In *Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt)*, 2022

[32] Lixu Wang, Shichao Xu, Ruiqi Xu, Xiao Wang, and Qi Zhu. Non-Transferable Learning: A New Approach for Model Ownership Verification and Applicability Authorization. In *International Conference on Learning Representations (ICLR)*, 2022

[31] Jiahua Dong, Lixu Wang, Zhen Fang, Gan Sun, Shichao Xu, Xiao Wang, and Qi Zhu. Federated Class-Incremental Learning. In *Conference on Computer Vision and Pattern Recognition (CVPR)*, 2022

[30] Kang Yang, Pratik Sarkar, Chenkai Weng, and Xiao Wang. QuickSilver: Efficient and Affordable Zero-Knowledge Proofs for Circuits and Polynomials over Any Field. In *ACM Conference on Computer and Communications Security (CCS)*, 2021, **Best Paper Award Runner-up**

[29] Nicholas Franzese, Jonathan Katz, Steve Lu, Rafail Ostrovsky, Xiao Wang, and Chenkai Weng. Constant-Overhead Zero-Knowledge for RAM Programs. In *ACM Conference on Computer and Communications Security (CCS)*, 2021

[28] Chenkai Weng, Kang Yang, Xiang Xie andJonathan Katz, and Xiao Wang. Mystique: Efficient Conversions for Zero-Knowledge Proofs with Applications to Machine Learning. In *USENIX Security*, 2021

[27] Chenkai Weng, Kang Yang, Jonathan Katz, and Xiao Wang. Wolverine: Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs for Boolean and Arithmetic Circuits. In *IEEE Symposium on Security and Privacy (S&P)*, 2021

[26] Christopher A. Choquette-Choo, Natalie Dullerud, Adam Dziedzic, Yunxiang Zhang, Somesh Jha, Nicolas Papernot, and Xiao Wang. CaPC Learning: Confidential and Private Collaborative Learning. In *International Conference on Learning Representations (ICLR)*, 2021

[25] Xiao Dong, David Randolph, Chenkai Weng, Abel Kho, Jennie Rogers, and Xiao Wang. Developing High Performance Secure Multi-Party Computation Protocols in Healthcare: A Case Study of Patient Risk Stratification. In *American Medical Informatics Association Informatics Summit (AMIA)*, 2021

[24] Lixu Wang, Shichao Xu, Xiao Wang, and Qi Zhu. Towards Class Imbalance in Federated Learning. In *AAAI Conference on Artificial Intelligence (AAAI)*, 2021

[23] Ran Canetti, Pratik Sarkar, and Xiao Wang. Efficient and round-optimal oblivious transfer and commitment with adaptive security. In *Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacypt)*, 2020

[22] Ran Canetti, Pratik Sarkar, and Xiao Wang. Blazing Fast OT for Three-Round UC OT Extension. In *Public-Key Cryptography (PKC)*, 2020

[21] Kang Yang, Chenkai Weng, Xiao Lan, Jiang Zhang, and Xiao Wang. Ferret: Fast Extension for coRRElated oT with small communication. In *ACM Conference on Computer and Communications Security (CCS)*, 2020

[20] Kang Yang, Xiao Wang, and Jiang Zhang. More Efficient MPC from Improved Triple Generation and Authenticated Garbling. In *ACM Conference on Computer and Communications Security (CCS)*, 2020

[19] Chun Guo, Jonathan Katz, Xiao Wang, Chenkai Weng, and Yu Yu. Better Concrete Security for Half-Gates Garbling (in the Multi-Instance Setting). In *International Cryptology Conference (CRYPTO)*, 2020

[18] 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

[17] 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

[16] Cheng Hong, Jonathan Katz, Vladimir Kolesnikov, Wen jie Lu, and Xiao Wang. Covert Security with Public Verifiability: Faster, Leaner, and Simpler. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt)*, 2019

[15] 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

[14] 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

[13] 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

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

[11] 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**

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

[9] Xiao Wang, Alex J. Malozemoff, and Jonathan Katz. Faster Secure Two-Party Computation in the Single-Execution Setting. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt)*, 2017

[8] 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

[7] 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

[6] 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

[5] 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

[4] 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

[3] 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

[2] 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

[1] 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

Other Publications

[3] Xiao Wang and Jennie Rogers. VaultDB: Facilitating Secure Analytics over Multiple Private Data Sources. In *Workshop on Privacy Enhancing Technologies for the Homeland Security Enterprise*, 2022

[2] Xi He, Jennie Rogers, Johes Bater, Ashwin Machanvajjhala, Chenghong Wang, and Xiao Wang. Tutorial: Practical Security and Privacy for Database Systems. In *ACM International Conference on Management of Data (SIGMOD)*, 2021

[1] Jennie Rogers, Johes Bater, Xi He, Ashwin Machanavajjhala, Madhav Suresh, and Xiao Wang. Privacy Changes Everything. In *POLY Workshop at VLDB*, 2019

Students and Vistors

Ph.D. students

1. Peter K Chan, J.D. + Ph.D. (2019 -)
2. Haotian Chu (2023 -)
3. Nicholas Franzese (2020 -) **Supported by NSF Graduate Research Fellowship**
4. Radhika (2022 -)
5. Yunqing Sun (2021 -)
6. Gefei Tan (2023 -)
7. Lixu Wang (co-advised with Qi Zhu, 2021 -) **Supported by IBM PhD Fellowship**
8. Chenkai Weng (2019 -) **Supported by J.P. Morgan AI Research Fellowship**
9. Wenhao Zhang (2022 -)

Post-docs

1. Ning Luo (01/2023 -)

Undergraduate students

1. Andrew Su (Northwestern, 02/2022 - 06/2023) Bloomberg
2. Kevin Wu (Northwestern, 12/2020 - 12/2021) Ph.D. at Georgia Tech.
3. Radhika (IIT Roorkee, 09/2020 - 05/2022) Ph.D. at Northwestern
4. Haotian Chu (SJTU, 08/2022 - 05/2023) Ph.D. at Northwestern

Other visitors

1. Kaiyi Zhang, undergraduate visitor (08/2019 - 01/2020)
2. Xiao Lan, visitor (09/2019 - 08/2020)

Selected Talks

1. Google Research Talk: "Private Set Intersection for the Crowd", 2023
2. Bangalore Cryptography Seminar Series: "Efficient Zero-Knowledge Proofs Based on Vector-Oblivious Linear Evaluation", 2022
3. Workshop on Privacy Enhancing Technologies for the Homeland Security Enterprise: "VaultDB: Facilitating Secure Analytics over Multiple Private Data Sources", 2022
4. Invited Talk at International Conference on Coding and Cryptography (Virtual): "Efficient and Affordable Zero-Knowledge Proofs: ResNet Inference and RAM Computation", 2022
5. Monash Cybersecurity Seminar (Virtual, Australia): "Efficient and Affordable Zero-Knowledge Proofs: Trillion Gates and Beyond", 2021
6. Stanford Security Seminar (Virtual, CA): "Efficient and Affordable Zero-Knowledge Proofs: Trillion Gates and Beyond", 2021
7. NIST Workshop on Multi-Party Threshold Schemes (Virtual, MD): " Authenticated Garbling for Large-Scale MPC", 2020
8. DIMACS/MACS Workshop on Usable, Efficient, and Formally Verified Secure Computation (Boston, MA): "Efficient and Secure Multiparty Computation from Fixed-Key Block Ciphers", 2019
9. Cryptography and Information Security Seminars at MIT (Boston, MA): "Covert Security with Public Verifiability: Simpler, Faster, and Leaner, 2018
10. IBM Research Cryptography Seminar Series (Yorktown Heights, NY): "Authenticated Garbling: Efficient Maliciously Secure Two-Party Computation and Global-Scale Secure Multiparty Computation", 2018
11. Theory and Practice of Multi-Party Computation Workshop (Bristol, UK): "Authenticated Garbling and Efficient MaliciouslyzSecure 2PC and MPC", 2017.
12. Seminar talk at Bell Labs (Murray Hill, NJ): "Efficient Genome-Wide, Privacy-Preserving Similar Patient Query based on Private Edit Distance", 2017.
13. Invited talk at iDASH Privacy & Security Workshop (Chicago, IL): "Privacy Preserving Top-k Search on Genome Data", 2016.
14. DC Area Anonymity/Privacy/Security Seminar (Washington, D.C.): "Faster Two-Party Computation Secure Against Malicious Adversaries in the Single-Execution Setting", 2016.

Teaching

- COMP_SCI 212 *Mathematical Foundations of Computer Science* (Lecture): 22 Spring (Honor session), 23 Spring.
- COMP_SCI 396 *Introduction to Cryptography* (Lecture): 20 Winter, 20 Fall, 21 Fall, 22 Fall, 23 Fall.
- COMP_SCI 496 *Advanced Topics in Modern Cryptography* (Lecture): 19 Fall, 21 Winter, 22 Winter, 23 Winter.
- COMP_SCI 496 *Engineering Modern Cryptographic Protocols* (Seminar): 21 Spring.

Professional Activities

Program committees

- IEEE Symposium on Security and Privacy (S&P) 2020, 2021, 2023
- ACM Symposium on Computer and Communications Security (CCS) 2019, 2020, 2021, 2022, 2023
- USENIX Security 2023, 2024
- International Cryptology Conference (CRYPTO) 2019, 2022, 2024

- IEEE Conference on Secure and Trustworthy Machine Learning (SaTML), 2023
- ACM Asia Conference on Computer and Communications Security (AsiaCCS) 2020
- Information Security Conference (ISC) 2019
- IEEE Military Communications Conference (MILCOM) 2016 – 2018
- ACM Workshop on Privacy Preserving Machine Learning (PPML) 2019, 2021
- The AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI) 2020
- ACM Cloud Computing Security Workshop (CCSW) 2019

Workshops, Tutorials, and other activities

- Coach, CSGrad4US Mentoring Program, 2023
- Workshop Organizer of "Mentoring Workshop and Videos" at IACR Crypto 2021 (`https://mentor-crypto-2021.github.io/`)
- Tutorial Organizer of "Practical Security and Privacy for Database Systems" at SIGMOD 2021 (`https://sp-for-dbms.github.io/`).