Tianhao Wang

☎ +1-765-409-2725 • ✉ tianhao@virginia.edu • 🌐 tianhao.wang

Professional Experience

University of Virginia
Assistant Professor in Computer Science and Data Science — *Jan 2022–*

Carnegie Mellon University — **Mentor: Elaine Shi**
Post Doctoral Fellow — *May 2021–Dec 2021*

Education

Purdue University — **Advisor: Ninghui Li**
PhD in Computer Science, GPA 4.00/4.00 — *Aug 2015–May 2021*

Fudan University — **Advisor: Yunlei Zhao**
BS in Software Engineering, GPA 3.79/4.00 (Rank 1/79) — *Sep 2011–July 2015*

Publication

Conference Papers

1. **Privacy Audit as Bits Transmission: (Im)possibilities for Audit by One Run** (**USENIX'25**)
Zihang Xiang, Tianhao Wang, Di Wang

2. **White-box Membership Inference Attacks against Diffusion Models** (**PETS'25**)
Yan Pang, Xuhui Kang, Mengdi Huai, Yang Zhang, Tianhao Wang

3. **SPAS: Continuous Release of Data Streams under w-Event Differential Privacy** (**SIGMOD'25**)
Xiaochen Li, Tianyu Li, Yitian Cheng, Chen Gong, Kui Ren, Zhan Qin, Tianhao Wang

4. **Data-adaptive Differentially Private Prompt Synthesis for In-Context Learning** (**ICLR'25**)
Fengyu Gao, Ruida Zhou, Tianhao Wang, Cong Shen, Jing Yang

5. **Towards Understanding Unsafe Video Generation** (**NDSS'25**)
Yan Pang, Aiping Xiong, Yang Zhang, Tianhao Wang

6. **Black-box Membership Inference Attacks against Fine-tuned Diffusion Models** (**NDSS'25**)
Yan Pang, Tianhao Wang

7. **Trajdeleter: Enabling Trajectory Forgetting in Offline Reinforcement Learning Agents** (**NDSS'25**)
Chen Gong, Kecen Li, Jin Yao, Tianhao Wang

8. **Revisiting EM-based Estimation for Locally Differentially Private Protocols** (**NDSS'25**)
Yutong Ye, Tianhao Wang, Min Zhang, Dengguo Feng

9. **Delay-allowed Differentially Private Data Stream Release** (**NDSS'25**)
Xiaochen Li, Zhan Qin, Kui Ren, Chen Gong, Shuya Feng, Yuan Hong, Tianhao Wang

10. **NetDPSyn: Synthesizing Network Traces under Differential Privacy** (**IMC'24 (Short Paper Track)**)
Danyu Sun, Joann Qiongna Chen, Chen Gong, Tianhao Wang, Zhou Li

11. **Benchmarking Secure Sampling Protocols for Differential Privacy (CCS'24)**
Yucheng Fu, Tianhao Wang

12. **PreCurious: How Innocent Pre-Trained Language Models Turn into Privacy Traps (CCS'24)**
Ruixuan Liu, Tianhao Wang, Yang Cao, Li Xiong

13. **Machine Unlearning of Pre-trained Large Language Models (ACL'24)**
Jin Yao, Eli Chien, Minxin Du, Xinyao Niu, Tianhao Wang, Zezhou Cheng, Xiang Yue

14. **Towards Certified Unlearning for Deep Neural Networks (ICML'24)**
Binchi Zhang, Yushun Dong, Tianhao Wang, Jundong Li

15. **PrivImage: Differentially Private Synthetic Image Generation using Diffusion Models with Semantic-Aware Pretraining (USENIX'24)**
Kecen Li, Chen Gong, Zhixiang Li, Yuzhong Zhao, Xinwen Hou, Tianhao Wang

16. **BAFFLE: Hiding Backdoors in Offline Reinforcement Learning Datasets (SP'24)**
Chen Gong, Zhou Yang, Yunpeng Bai, Jieke Shi, Junda He, Kecen Li, Bowen Xu, Arunesh Sinha, Xinwen Hou, David Lo, Tianhao Wang

17. **Preserving Node-level Privacy in Graph Neural Networks (SP'24)**
Zihang Xiang, Tianhao Wang, Di Wang

18. **Backdoor Attacks via Machine Unlearning (AAAI'24)**
Zihao Liu, Tianhao Wang, Mengdi Huai, Chenglin Miao

19. **GlucoSynth: Generating Differentially-Private Synthetic Glucose Traces (Neurips'23)**
Josephine Lamp, Mark Derdzinski, Christopher Hannemann, Joost van der Linden, Lu Feng, Tianhao Wang, and David Evans

20. **Mitigating Membership Inference Attacks via Weighted Smoothing (ACSAC'23)**
Mingtian Tan, Xiaofei Xie, Jun Sun, Tianhao Wang

21. **Differentially Private Resource Allocation (ACSAC'23)**
Joann Qiongna Chen, Tianhao Wang, Zhikun Zhang, Yang Zhang, Somesh Jha, Zhou Li

22. **Securely Sampling Discrete Gaussian Noise for Multi-Party Differential Privacy (CCS'23)**
Chengkun Wei, Ruijing Yu, Yuan Fan, Wenzhi Chen, Tianhao Wang

23. **DP-Forward: Fine-tuning and Inference on Language Models with Differential Privacy in Forward Pass (CCS'23)**
Minxin Du, Xiang Yue, Sherman Chow, Tianhao Wang, Chenyu Huang, Huan Sun

24. **Practical Differentially Private and Byzantine-resilient Federated Learning (SIGMOD'23)**
Zihang Xiang, Tianhao Wang, Wanyu Lin, Di Wang

25. **Differentially Private Vertical Federated Clustering (VLDB'23)**
Zitao Li, Tianhao Wang, Ninghui Li

26. **FACE-AUDITOR: Data Auditing in Facial Recognition Systems (USENIX'23)**
Min Chen, Zhikun Zhang, Tianhao Wang, Michael Backes, Yang Zhang

27. **PrivTrace: Differentially Private Trajectory Synthesis by Adaptive Markov Model** (**USENIX’23**)
Haiming Wang, Zhikun Zhang, Tianhao Wang, Shibo He, Michael Backes, Jiming Chen, Yang Zhang

28. **A Plot is Worth a Thousand Words: Model Information Stealing Attacks via Scientific Plots** (**USENIX’23**)
Boyang Zhang, Xinlei He, Yun Shen, Tianhao Wang, Yang Zhang

29. **Is Adversarial Training Really a Silver Bullet for Mitigating Data Poisoning?** (**ICLR’23**)
Rui Wen, Zhengyu Zhao, Zhuoran Liu, Michael Backes, Tianhao Wang, Yang Zhang

30. **FLORAS: Differentially Private Wireless Federated Learning Using Orthogonal Sequences** (**ICC’23**)
Xizixiang Wei, Tianhao Wang, Ruiquan Huang, Cong Shen, Jing Yang, Vincent Poor

31. **Memorization in NLP Fine-tuning Methods** (**EMNLP’22**)
Fatemehsadat Mireshghallah, Archit Uniyal, Tianhao Wang, David Evans, Taylor Berg-Kirkpatrick

32. **Federated Boosted Decision Trees with Differential Privacy** (**CCS’22**)
Samuel Maddock, Graham Cormode, Tianhao Wang, Carsten Maple, Somesh Jha

33. **Graph Unlearning** (**CCS’22**)
Min Chen, Zhikun Zhang, Tianhao Wang, Michael Backes, Mathias Humbert, Yang Zhang

34. **Locally Differentially Private Sparse Vector Aggregation** (**SP’22**)
Zhou, Mingxun, Tianhao Wang, Hubert Chan, Giulia Fanti, and Elaine Shi

35. **Continuous Release of Data Streams under both Centralized and Local Differential Privacy** (**CCS’21**)
Tianhao Wang, Joann Chen, Zhikun Zhang, Dong Su, Yueqiang Cheng, Zhou Li, Ninghui Li, Somesh Jha

36. **When Machine Unlearning Jeopardizes Privacy** (**CCS’21**)
Min Chen, Zhikun Zhang, Tianhao Wang, Michael Backes, Mathias Humbert, Yang Zhang

37. **PrivSyn: Differentially Private Data Synthesis** (**USENIX’21**)
Zhikun Zhang, Tianhao Wang, Jean Honorio, Ninghui Li, Michael Backes, Shibo He, Jiming Chen, Yang Zhang

38. **Answering Multi-Dimensional Range Queries under Local Differential Privacy** (**VLDB’21**)
Jianyu Yang, Tianhao Wang, Ninghui Li, Xiang Cheng, Sen Su

39. **Differential Privacy for Text Analytics via Natural Text Sanitization** (**ACL’21 Findings**)
Xiang Yue, Minxin Du, Tianhao Wang, Yaliang Li, Huan Sun, Sherman Chow

40. **Improving Utility and Security of the Shuffler-based Differential Privacy** (**VLDB’20**)
Tianhao Wang, Bolin Ding, Min Xu, Zhicong Huang, Cheng Hong, Jingren Zhou, Ninghui Li, Somesh Jha

41. **Collecting and analyzing data jointly from multiple services under local differential privacy** (**VLDB’20**)
Min Xu, Bolin Ding, Tianhao Wang, Jingren Zhou

42. **Towards Effective Differential Privacy Communication for User Data Sharing Decision and Comprehension** (**SP’20**)
Aiping Xiong, Tianhao Wang, Ninghui Li, Somesh Jha

43. **Recovering Distributions under Local Differential Privacy** (**SIGMOD’20**)
Zitao Li, Tianhao Wang, Milan Lopuhaä-Zwakenberg, Ninghui Li, Boris Skoric

44. **Consistent and Accurate Frequency Oracles under Local Differential Privacy** (**NDSS'20**)
Tianhao Wang, Milan Lopuhaä-Zwakenberg, Zitao Li, Ninghui Li, Boris Skoric

45. **Koinonia: Verifiable E-Voting with Long-term Privacy** (**ACSAC'19**)
Huangyi Ge, Sze Yiu Chau, Victor E Gonsalves, Huian Li, Tianhao Wang, Xukai Zou, Ninghui Li

46. **Answering Multi-Dimensional Analytical Queries under Local Differential Privacy** (**SIGMOD'19**)
Tianhao Wang, Bolin Ding, Jingren Zhou, Cheng Hong, Zhicong Huang, Ninghui Li, Somesh Jha

47. **Privacy at Scale: Local Differential Privacy in Practice** (**SIGMOD'18**)
Graham Cormode, Somesh Jha, Tejas Kulkarni, Ninghui Li, Divesh Srivastava, Tianhao Wang (alphabetical order)

48. **Locally Differentially Private Frequent Itemset Mining** (**SP'18**)
Tianhao Wang, Ninghui Li, Somesh Jha

49. **Marginal Release via Local Differential Privacy** (**CCS'18**)
Zhikun Zhang, Tianhao Wang (co-first author), Ninghui Li, Shebo He, Jiming Chen

50. **Locally Differentially Private Protocols for Frequency Estimation** (**USENIX'17**)
Tianhao Wang, Jeremiah Blocki, Ninghui Li, Somesh Jha

51. **On the Security and Usability of Segment-based Visual Cryptographic Authentication Protocols** (**CCS'16**)
Tianhao Wang, Huangyi Ge, Omar Chowdhury, Hemanta Maji, Ninghui Li

52. **Secure Dynamic SSE via Access Indistinguishable Storage** (**AsiaCCS'16**)
Tianhao Wang, Yunlei Zhao

53. **Weight Balancing on Boundaries and Skeletons** (**SoCG'14**)
..., Tianhao Wang, ... (alphabetical order)

Journal Articles

54. **Edge-Protected Triangle Count Estimation under Relationship Local Differential Privacy** (**TKDE'24**)
Yuhan Liu, Tianhao Wang, Yixuan Liu, Hong Chen, Cuiping Li

55. **Locally Differentially Private Heavy Hitters Identification** (**TDSC'21**)
Tianhao Wang, Ninghui Li, Somesh Jha

56. **PURE: A Framework for Analyzing Proximity-based ContactTracing Protocols** (**CSUR'21**)
Fabrizio Cicala, Weicheng Wang, Tianhao Wang, Ninghui Li, Elisa Bertino, Faming Liang, Yang Yang

57. **DPSyn: Experiences in the NIST Differential Privacy Data Synthesis Challenges** (**JPC'21**)
Ninghui Li, Zhikun Zhang, Tianhao Wang

58. **A Simple Algorithm for Finding All k-edge-connected Components** (**PLoS ONE'15**)
Tianhao Wang, Yong Zhang, Francis Y. L. Chin, Hing-Fung Ting, Yung H. Tsin, Sheung-Hung Poon

Contributed Book Chapters

59. **Handbook of Sharing Confidential Data: Differential Privacy, Secure Multiparty Computation, and Synthetic Data** (**CRC Press, 2024**)
Jörg Drechsler, Daniel Kifer, Jerome Reiter, Aleksandra Slavković

Teaching

Spring 2025: CS 6501 Data Privacy (35 Students)
Fall 2024: CS 3710 Intro to CyberSecurity (138 Students)
Fall 2023: DS 6559 Security & Privacy Elective (PhD Course, 3 Students)
Spring 2023: CS 6161 Design & Analysis of Algorithms (47 Students)
Fall 2022: CS 4501 Data Privacy (52 Students)
Spring 2022: CS 6501 Data Privacy (31 Students), DS 6011 Data Science Capstone (12 Students)

Students

Xiaochen Li: working on DP (PostDoc Fellow) *2024-now*
Yucheng Fu: working on DP and Applied Crypto *2024-now*
Kai Chen: working on DP and AI *2024-now*
Yan Pang: working on Generative AI Privacy and Security *2023-now*
Chen Gong: working on AI Privacy and Security *2023-now*

Services

Proposal Reviewer:
2025: NSF SaTC CRII Panelist
2024: NSERC Discovery Grant External Reviewer
2022: NSF SaTC Panelist×2, NSF TTP Ad-hoc Reviewer, NSERC Discovery Grant External Reviewer
PC Member:
2025: ACM CCS, NDSS, IEEE SP, USENIX Security, SaTML, PPAI
2024: ACM CCS, NDSS, IEEE SP, VLDB, TPDP, AISec, PPAI
2023: ACM CCS, NDSS, PETS, VLDB, ICDE, AAAI, WWW, TPDP, PPAI
2022: ACM CCS, PETS, AsiaCCS, ESORICS, EUROSP, Neurips, ICML, EMNLP, AAAI (Senior PC), CIKM, AISec
2021: ACM CCS, PETS, AsiaCCS, ESORICS, AISec, TPDP
Department Service:
2024-25: Colloquium Series
2023-24: Faculty Search, Colloquium Series, Diversity, Equity, and Inclusion, Systems PhD Curriculum (for SDS)
2022-23: Faculty Search, Colloquium Series, Computing Resources, Data Justice Academy Program (for SDS)

Grant

1. **CCI CVN SEAS Research: Distributed Differentially Private Tabular Data Synthesis (PI)**
2. **NSF: SaTC: CORE: Small: Security and Privacy in Machine Unlearning (PI)**
3. **CCI NoVa CATAPULT: Privacy-preserving Synthetic Data Generation (PI)**
4. **CCI CVN SEAS Commercialization and Innovation: Privacy-preserving Synthetic Data Generation (PI)**
5. **NSF: CICI:TCR: Enhancing Security and Privacy of Community Cyberinfrastructures for Collaborative Research (Co-PI)**
6. **NSF: IMR: MM-1B: Foundations for Differentially Private Internet Measurement (Lead PI)**
7. **NSF: PPoSS: LARGE: Co-designing Hardware, Software, and Algorithms to Enable Extreme-Scale Machine Learning Systems (Senior Personnel)**
8. **NSF: CCRI: New: A Scalable Hardware and Software Environment Enabling Secure Multi-party Learning (Co-PI)**

Awards

CSAW Applied Research Competition Finalist	*2024*
VLDB Distinguished Reviewers	*2024*
ACM CCS Best Reviewer Award	*2022*
UVA Institute for Practical Ethics Faculty Fellowships for Courses in Ethics	*2022*
CERIAS Diamond Award: Only One in University	*2021*
NIST Challenge for a Better Meter Stick for Differential Privacy: 1st place	*2021*
NIST Differential Privacy Temporal Map Challenge: 2nd, 4th, and 3rd places in three phases	*2021*
iDASH Secure Genome Analysis Competition (Track III): 2nd place	*2020*
Bilsland Dissertation Fellowship: 1 of 3 in Department	*2019*
NIST Differential Privacy Synthetic Data Challenge: 2nd place in all three phases	*2019*
Symantec Research Labs Graduate Fellowship: Finalist	*2019*
NIST Unlinkable Data Challenge: Runner-up and Pepple's choice	*2018*
Emil Stefanov Memorial Fellowship: Only One in Department	*2018*
CERIAS Best Poster Award: 2nd place	*2016*
Excellent Graduation Thesis: Only One in School	*2015*
Excellent Graduate Award: 1 of 20 in University	*2015*
Google Excellence Scholarship: 1 of 58 nationwide (undergrads and grads combined)	*2014*
Outstanding Student: 1 of 10 in University	*2014*
National Scholarship: Only One in School	*2012*