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*

Publications

Conference Papers

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

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

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

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

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

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

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

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

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

10. **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

11. **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

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

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

14. **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

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

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

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

18. **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

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

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

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

22. **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

23. **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

24. **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

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

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

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

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

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

30. **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

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

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

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

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

35. **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

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

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

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

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

40. **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

41. **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

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

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

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

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

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

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

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

Journal Articles

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

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

51. **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

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

53. **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

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

Grant

1. **NSF: SaTC: CORE: Small: Security and Privacy in Machine Unlearning (PI)**
2. **CCI NoVa CATAPULT: Privacy-preserving Synthetic Data Generation (PI)**
3. **CCI Commercialization and Innovation: Privacy-preserving Synthetic Data Generation (PI)**
4. **NSF: CICI:TCR: Enhancing Security and Privacy of Community Cyberinfrastructures for Collaborative Research (Co-PI)**
5. **NSF: IMR: MM-1B: Foundations for Differentially Private Internet Measurement (Lead PI)**
6. **NSF: PPoSS: LARGE: Co-designing Hardware, Software, and Algorithms to Enable Extreme-Scale Machine**

Learning Systems (Senior Personnel)
7. **NSF: CCRI: New: A Scalable Hardware and Software Environment Enabling Secure Multi-party Learning (Co-PI)**

Teaching

Fall 2024: CS 3710 Intro to CyberSecurity (140 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*
Songwei Dong: working on AI *2024-now*
Yucheng Fu: working on DP and Applied Crypto *2024-now*
Han Yang: working on Generative AI Privacy and Security *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:
2022: NSF SaTC Panelist×2, NSF TTP Ad-hoc Reviewer, NSERC Discovery Grant External Reviewer, US-UK PETs Prize Challenge Reviewer
PC Member:
2025: NDSS, IEEE SP, USENIX Security, SaTML
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:
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)

Awards

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*

Invited Talks

Meta Central Applied Science PPML Group Seminar: DP-Forward on Language Models *Aug 2024*
Chinese Academy of Science Seminar: Topics in Differentially Private Machine Learning *May 2023*
Zhejiang University Seminar: Topics in Differentially Private Machine Learning *May 2023*
UVA Statistics Seminar: Byzantine Resilient Differentially Private Machine Learning *April 2023*
AAAI-23 Bridge: AI and Law: Opening Remarks about Privacy in AI *Feb 2023*
UCL Privacy and Security in ML Seminars: Data Streams Release under Differential Privacy *Oct 2022*
Rutgers System Research Seminar: Supporting Database Systems with Differential Privacy *Dec 2020*
UC Irvine ECE Seminar: Answering Multi-Dimensional Queries under Local Differential Privacy *Feb 2020*
CISPA Helmholtz Center for Information Security: Collecting Data with Local Differential Privacy *July 2019*
Baidu Security Lab: Differential Privacy and Local Differential Privacy Tutorial *Dec 2017*
Purdue CERIAS Security Seminar: Locally Differential Private Protocols for Frequency Estimation *Oct 2017*