Tianhao Wang

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

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*

Professional Experience

University of Virginia
Assistant Professor *Jan 2022–*

Facebook
Consultant *Aug 2021–May 2022*

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

Tumult Labs **Mentor: Ashwin Machanavajjhala**
Research Intern *May 2020–Aug 2020*

Alibaba **Mentor: Bolin Ding**
Research Intern *Aug 2018–Jan 2019*

Publications

Conference Papers

1. **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

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

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

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

5. **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

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

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

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

9. **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

10. **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

11. **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

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

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

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

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

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

17. **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

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

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

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

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

22. **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

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

24. **Towards Effective Differential Privacy Communication for User Data Sharing Decision and Comprehen-**

sion (SP’20)
Aiping Xiong, Tianhao Wang, Ninghui Li, Somesh Jha

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

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

27. **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

28. **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

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

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

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

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

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

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

Journal Articles

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

36. **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

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

38. **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

Tutorials

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

Grant

1. **NSF: CICI:TCR: Enhancing Security and Privacy of Community Cyberinfrastructures for Collaborative Research (Co-PI)**
2. **NSF: IMR: MM-1B: Foundations for Differentially Private Internet Measurement (Lead PI)**
3. **NSF: PPoSS: LARGE: Co-designing Hardware, Software, and Algorithms to Enable Extreme-Scale Machine Learning Systems (Senior Personnel)**
4. **NSF: CCRI: New: A Scalable Hardware and Software Environment Enabling Secure Multi-party Learning (Co-PI)**

Teaching

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)
Spring 2022: SDS 6011 Data Science Capstone (12 Students)

Students

Yan Pang working on Generative AI Security	*2023-now*
Chen Gong working on Generative AI Security	*2023-now*
Mingtian Tan working on Generative AI Security	*2022-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:

2024: IEEE SP, NDSS, VLDB
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: Committee for Systems PhD Curriculum (for SDS)
2022-23: Committee for Faculty Search, Colloquium Series, Computing Resources, Data Justice Academy Program (for SDS)

Awards

ACM CCS Best Reviewer Award	*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*

Graduate Star: 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

Shandong University Seminar Topics in Differentially Private Machine Learning *Oct 2023*

Chinese Academy of Science Seminar Topics in Differentially Private Machine Learning *May 2023*

Renmin University of China 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*