

Di Wang

Al Khawarizmi Building 1, Room 4243
King Abdullah University of Science and Technology
Thuwal Kingdom of Saudi Arabia, 23955-6900

Email: di.wang@kaust.edu.sa
<https://shao3wangdi.github.io/>
Tel: +966 (012) 8080645

RESEARCH INTERESTS

Broadly, my research lies in trustworthy machine learning, with a particular focus on the role of memorization in modern machine learning and generative AI systems. My work is guided by two central questions: (1) how to enable controllable and editable memorization across data, knowledge, and high-level concepts via rigorous, mechanistic, and principled ways; and (2) how to leverage such memorization to improve efficiency, utility, and trustworthiness.

- Data Memorization: Differential privacy, adversarial training, machine unlearning, training data attribution, copyright, and personally identifiable information.
- Knowledge Memorization: Knowledge editing and knowledge unlearning.
- Concept Memorization: Mechanistic interpretability, explainable AI, fairness, and concept erasure.

WORK EXPERIENCE

King Abdullah University of Science and Technology	Thuwal, Saudi Arabia
Computer Science Program	<i>January 2021-Current</i>
Division of CEMSE	
Assistant Professor	
Director of Provable Responsible AI and Data Analytics (PRADA) Lab	
Statistics Program (Affiliated Member)	
Center of Excellence on Generative AI (Affiliated Member)	
SDAIA-KAUST AI center (Affiliated Member)	

EDUCATION

State University of New York at Buffalo	Buffalo, NY, United States
Ph.D. in Computer Science and Engineering	<i>August 2020</i>
Advisor: Dr. Jinhui Xu	
Dissertation: Some Fundamental Machine Learning Problems in the Differential Privacy Model	
Western University	London, ON, Canada
M.S. in Mathematics	<i>October 2015</i>
Shandong University	Jinan, Shandong, China
B.S. in Mathematics and Applied Mathematics	<i>June 2014</i>

HONORS and AWARDS

-
- Honorable Mention Paper Award, USENIX Security Symposium 2025
 - Best Paper Award, AAAI 2025 workshop on Connecting Low-Rank Representations in AI
 - Top 0.5% Scholar by ScholarGPS, 2024

- Best Paper Award, Asian Conference on Machine Learning, 2022
- Invited to The ACM Transactions on Database Systems special issue on Best of PODS 2022
- CSE Best Doctoral Dissertation Award in 2020, SUNY at Buffalo.
- SEAS Dean's Graduate Achievement Award in 2019, SUNY at Buffalo.
- Best CSE Graduate Research Award in 2018, SUNY at Buffalo.

RESEARCH EXPERIENCE

University of Helsinki Finnish Center for Artificial Intelligence (FCAI) Visiting Professor. Hosted by: Antti Honkela	Helsinki, Finland August 2022
--	----------------------------------

University of California at Berkeley Simons Institute for the Theory of Computing Data Privacy: Foundations and Applications Visiting Graduate Student	Berkeley, CA <i>Spring 2019</i>
---	------------------------------------

Harvard University Harvard University Privacy Tools Project Research Graduate	Cambridge, MA <i>June to August 2018</i>
---	---

Boston University Visiting Student Mentor: Dr. Adam D. Smith	Boston, MA <i>June to August 2018</i>
--	--

TEACHING EXPERIENCE

- **Instructor.** CS 226/294A: Trustworthy Machine Learning. Spring 2025-2026, KAUST
- **Instructor.** CS 325/394: Private Data Analysis. Fall 2021-2025, KAUST
- **Instructor.** CS 229: Machine Learning. Spring 2022-2024, KAUST
- **Instructor.** Short Course: Selected Topics in Differentially Private Machine Learning and Statistics, 5th-7th January 2021, School of Computer Science and Technology, East China Normal University.
- **Instructor.** CSE 574/474: Introduction to Machine Learning, Summer 2019, State University of New York at Buffalo.
- **Teaching Assistant.** CSE 574/474: Introduction to Machine Learning, Spring 2018, State University of New York at Buffalo.
- **Teaching Assistant.** CSE 531/431: Analysis of Algorithm, Fall 2017, Spring 2017, Fall 2016, Spring 2016, State University of New York at Buffalo.
- **Teaching Assistant.** CSE 115: Introduction to Computer Science for Majors I, Fall 2015, State University of New York at Buffalo.
- **Teaching Assistant.** MATH 1229A: Methods of Matrix Algebra, Summer 2015, Winter 2015, Western University.
- **Teaching Assistant.** MATH 1225B: Methods of Calculus, Fall 2014, Western University.

RESEARCH FUNDS

- \$100,000 USD (PI), KAUST AI Initiative Fund, "Private and Fair Learning Algorithms for Healthcare", Joint with Xin Gao (KAUST, Co-I), 2021-2022.
- \$1,050,000 USD (PI), KAUST CRG 2021 Grant, "Modern Privacy-preserving Learning Algorithms for Biomedical Data", Joint with Xin Gao (KAUST, Co-I) and Jinhui Xu (State University of New York at Buffalo, Co-I), 2022-2025.
- \$200,000 SAR (PI), SDAIA-KAUST Center of Excellence in Data Science and AI, "Efficient Privacy-Preserving Machine Learning Algorithms for Small Data", 2022-2023.
- \$2,160,000 USD (Co-I), KAUST CCF Grant, "Computational Bioscience Research Center", 2022-2023.
- \$300,000 USD (Co-I), KAUST Smart Health Initiative fund, "Nanophotonic chips for smart colorimetric histology". Joint with Qiaoqiang Gan (KAUST, PI), Jasmeen Merzaban (KAUST, Co-I), 2022-2024.
- \$997,787 USD (Co-I), KAUST Near Term Grand Challenge (NTGC), "Artificial-intelligent nanophotonic chips for colorimetric biosensing and imaging", Joint with Qiaoqiang Gan (KAUST, PI), Jasmeen Merzaban (KAUST, Co-I), 2023-2025.
- \$787,500 USD (Co-I), KAUST CRG 2022 Grant, "Physics-Based and Space-Time Statistical Machine Learning Models for Sustainable Development in Saudi Arabia". Joint with Marc G. Genton (KAUST, PI), Georgiy Stenchikov (KAUST, Co-I), Ying Sun (KAUST, Co-I), Paola Crippa (University of Notre Dame, Co-I), Stefano Castruccio (University of Notre Dame, Co-I), David Richter (University of Notre Dame, Co-I), 2023-2026.
- \$200,000 SAR USD (Co-I), SDAIA-KAUST Center of Excellence in Data Science and AI, "Optoelectronic Hardware Acceleration for Variational Autoencoder". Joint with Yating Wan (KAUST, PI), 2023-2024.
- \$200,000 SAR (PI), SDAIA-KAUST Center of Excellence in Data Science and AI, "Towards Faithful Transformers and Attention Mechanisms", 2023-2024.
- \$200,000 USD (PI), KAUST Opportunity Fund Program, "Rigorous Approaches for Robust and Private Machine Learning", 2024-2025.
- \$20,000 USD (PI), Google Seed Grant, "Rigorous Node-level Privacy-preserving Approaches for Graph Neural Networks", 2024-2025.
- \$249,000 USD (PI), Aramco Grant. "Call-Go: Continuous, Automatic LLM-Guardrail Generator and Optimizer". 2025-2027.
- \$75,000 USD (PI), GenAI CoE Google Gift Postdoctoral Funding. "Enabling Unlearning in Federated Learning as a Service Systems". 2025-2026.
- \$100,000 USD (PI), KAUST small Translational Research Grant (sTRG). "Scalable Fine-Tuning for Extremely Large Language Models with Limited GPU Memory". 2026-2027. Joint with Jian Weng (KAUST, Co-I).
- \$11,000,000 USD (Theme PI), Center of Excellence for Generative AI, 2024-2029.
- \$50,000 USD in Google Cloud credits (PI), Google TPU Research & Education Awards. "Dist-FlashDP: Efficient Differentially Private Training for Large Language Models on TPU Clusters". 2026-2027.
- 30,000 GPU hour (PI), Shaheen III GPU Grand Challenge Project. "Scaling Laws and Optimization Dynamics of Looped Transformers: Toward Efficient and High-Capacity Language Models". 2026-2027.

SELECTED PUBLICATIONS

1. [IEEE S&P 2027] Zihang Xiang, Tianhao Wang, Hanshen Xiao, Yuan Tian, **Di Wang**. Tight Privacy Audit in One Run. IEEE Symposium on Security and Privacy.
2. [NeurIPS 2026] Meng Ding, Mingxi Lei, Jie Zhang, Jinyan Liu, **Di Wang**. Differentially Private Sparse Reward Estimation with Preference Feedback. Conference on Neural Information Processing Systems
3. [ICLR 2026] Shaopeng Fu, **Di Wang**. Understanding and Improving LLMs' Continuous Adversarial Training via In-context Learning Theory. International Conference on Learning Representations.
4. [NeurIPS 2025] Shaopeng Fu, Liang Ding, Jingfeng Zhang, **Di Wang**. Short-length Adversarial Training Helps LLMs Defend Long-length Jailbreak Attacks: Theoretical and Empirical Evidence. Conference on Neural Information Processing Systems.
5. [USENIX 2025] Zihang Xiang, Tianhao Wang, **Di Wang**. Privacy Audit as Bits Transmission: (Im)possibilities for Audit by One Run. USENIX Security Symposium.
6. [NeurIPS 2025] Liangyu Wang, Junxiao Wang, Jie Ren, Zihang Xiang, David Keyes, **Di Wang**. Private Training Large-scale Models with Efficient DP-SGD. Conference on Neural Information Processing Systems.
7. [CoLM 2025] Liangyu Wang, Jie Ren, Hang Xu, Junxiao Wang, David E. Keyes, **Di Wang**. Scalable Zeroth-Order Fine-Tuning for Extremely Large Language Models with Limited GPU Memory. Conference on Language Modeling.
8. [IEEE S&P 2024] Zihang Xiang, Tianhao Wang, **Di Wang**. Preserving Node-level Privacy in Graph Neural Networks. IEEE Symposium on Security and Privacy.
9. [JMLR] Jinyan Su, Lijie Hu, **Di Wang**. Faster Rates of Differentially Private Stochastic Convex Optimization. Journal of Machine Learning Research.
10. [JMLR] **Di Wang***, Lijie Hu*, Huanyu Zhang, Marco Gaboardi, Jinhui Xu. Generalized Linear Models in Non-interactive Local Differential Privacy with Public Data. Journal of Machine Learning Research.

PUBLICATIONS

(* equally contributed co-first authors, '_____' students/postdocs/interns supervised by me)

Peer-Refereed Conference Papers

1. [IEEE S&P 2027] Zihang Xiang, Tianhao Wang, Hanshen Xiao, Yuan Tian, **Di Wang**. Tight Privacy Audit in One Run. IEEE Symposium on Security and Privacy.
2. [NeurIPS 2026] Meng Ding, Mingxi Lei, Jie Zhang, Jinyan Liu, **Di Wang**. Differentially Private Sparse Reward Estimation with Preference Feedback. Conference on Neural Information Processing Systems
3. [NeurIPS 2026] Zhihao Liu, Zixiong Guo, Shuo Shao, Yu He, Wenli Wang, Meihui Chen, **Di Wang**, Yuke Hu. Ask in the Crowd: Differentially Private LLM Inference via Dummy-Augmented Shuffling. Conference on Neural Information Processing Systems
4. [NeurIPS 2026] Junchi Yao, Lokranjan Lakshminathan, Annie Zhao, Danielle Zhao, Shu Yang, Zikang Ding, **Di Wang**, Lijie Hu. Hearing is Believing? Evaluating and Analyzing Audio Language Model Sycophancy with SYAUDIO. Conference on Neural Information Processing Systems
5. [EMNLP Findings 2026] Guanqiao Chen, **Di Wang**, Lijie Hu. SFAD: Speculative Factuality-Aware Decoding. Conference on Empirical Methods in Natural Language Processing.
6. [EMNLP Findings 2026] Shaolong Chen, Youming Tao, Shuzhen Chen, Falko Dressler, Qingqing Ye, **Di Wang**. FedSubMuon: Communication-Efficient Federated LLM Fine-Tuning via Structured Subspace Muon. Conference on Empirical Methods in Natural Language Processing.

7. [EMNLP Findings 2026] Guijia Zhang, Shu Yang, Xilin Gong, **Di Wang**. STARS: Skill Triage via Activation Risk Scoring for LLM Agents. Conference on Empirical Methods in Natural Language Processing.
8. [EMNLP Findings 2026] Xinyan Jiang, Wenjing Yu, **Di Wang**, Lijie Hu. Global Evolutionary Steering: Refining Activation Steering Control via Cross-Layer Consistency. Conference on Empirical Methods in Natural Language Processing.
9. [EMNLP 2026] Wenshuo Dong, Qingsong Yang, Shu Yang, Lijie Hu, Meng Ding, Wanyu Lin, Tianhang Zheng, **Di Wang**. Understanding and Mitigating Cross-lingual Privacy Leakage via Language-specific and Universal Privacy Neurons. Conference on Empirical Methods in Natural Language Processing.
10. [EMNLP 2026] Xiangxiang Cui, Shu Yang, Tianjin Huang, Wanyu Lin, Lijie Hu, **Di Wang**. LLMs Regret Before They Say It: Early Detection and Compositional Architecture of Regret in Hidden States. Conference on Empirical Methods in Natural Language Processing.
11. [ICML 2026] Difei Xu, Youming Tao, Meng Ding, Chenglin Fan, **Di Wang**. Finding Differentially Private Second Order Stationary Points in Stochastic Minimax Optimization. International Conference on Machine Learning.
12. [ICML 2026] Jingyu Hu, Shu Yang, Xilin Gong, Hongming Wang, Weiru Liu, **Di Wang**. Real-Time Monitoring and Calibration of Chain-of-Thought Sycophancy in Large Reasoning Models. International Conference on Machine Learning.
13. [ICML 2026] Jiaming Zhang, Meng Ding, Shaopeng Fu, Jingfeng Zhang, **Di Wang**. Benign Overfitting in Adversarial Training for Vision Transformers. International Conference on Machine Learning.
14. [ICML 2026] Meng Ding, Mingxi Lei, Shaopeng Fu, Shaowei Wang, **Di Wang**, Jinhui Xu. Understanding Private Learning From Feature Perspective. International Conference on Machine Learning.
15. [ICML 2026] Wenshuo Dong*, Jiaming Zhang*, Shaopeng Fu, Hongbin Lin, **Di Wang**, Lijie Hu. Algorithmic Recourse of In-Context Learning for Tabular Data. International Conference on Machine Learning.
16. [ICML 2026] Zhuoran Zhang, Tengyue Wang, Xilin Gong, Yang Shi, Haotian Wang, **Di Wang**, Lijie Hu. Beyond Fixed Biases: Decoding the Role of Reasoning Uncertainty in MLLM Modality Conflicts. International Conference on Machine Learning.
17. [ICML 2026] Xinyan Jiang, Ninghao Liu, **Di Wang**, Lijie Hu. Beyond Scalars: Evaluating and Understanding LLM Reasoning via Geometric Progress and Stability. International Conference on Machine Learning.
18. [ICML 2026] Hengliang Wu, Jiale Yang, Youming Tao, Shuzhen Chen, **Di Wang**, Dongxiao Yu. Trajectory-Aware Certified Decentralized Unlearning via SGD Stability. International Conference on Machine Learning.
19. [ACL Findings 2026] Liangyu Wang, Huanyi Xie, **Di Wang**. High-Throughput and Memory-Efficient Zeroth-Order Fine-tuning LLMs with Distributed Parallel Computing. Findings of Annual Meeting of the Association for Computational Linguistics.
20. [ACL Findings 2026] Jiaye Lin, Mengdi Li, Xufeng Zhao, Wenhao Lu, Peilin Zhao, Stefan Wermter, **Di Wang**. Curriculum-RLAIF: Curriculum Alignment with Reinforcement Learning from AI Feedback. Findings of Annual Meeting of the Association for Computational Linguistics.
21. [ACL Findings 2026] Shu Yang, Jingyu Hu, Tong Li, Hanqi Yan, Wenxuan Wang, **Di Wang**. AutoMonitor-Bench: Evaluating the Reliability of LLM-Based Misbehavior Monitor. Findings of Annual Meeting of the Association for Computational Linguistics.
22. [ACL 2026] Wenrui Zhou, Mohamed Hendy, Shu Yang, Qingsong Yang, Zikun Guo, Yuyu Luo, **Di Wang**. Flattery in Motion: Benchmarking and Analyzing Sycophancy in Video-LLMs. Annual Meeting of the Association for Computational Linguistics.

23. **[ACL 2026]** Jiayi Zhang*, Shu Yang*, Junchao Wu, Derek F. Wong, **Di Wang**. Understanding and Mitigating Political Stance Cross-topic Generalization in Large Language Models. Annual Meeting of the Association for Computational Linguistics.
24. **[ACL 2026]** Qishun Yang*, Shu Yang*, Lijie Hu, **Di Wang**. Visual Self-Fulfilling Alignment: Shaping Safety-Oriented Personas via Threat-Related Images. Annual Meeting of the Association for Computational Linguistics.
25. **[ACL 2026]** Qi Li*, Cheng-Long Wang*, Yinzhi Cao, **Di Wang**. CoLA: A Choice Leakage Attack Framework to Expose Privacy Risks in Subset Training. Annual Meeting of the Association for Computational Linguistics.
26. **[CVPR 2026]** Hongji Li, Manjiang Yu, Junchi Yao, Priyanka Singh, Xue Li, **Di Wang**, Lijie Hu. Towards Reasoning-Preserving Unlearning in Multimodal Large Language Models. IEEE/CVF Conference on Computer Vision and Pattern Recognition.
27. **[ICLR 2026]** Jiahao Zhang*, Zeqing Zhang*, **Di Wang**, Lijie Hu. Controlling Repetition in Protein Language Models. International Conference on Learning Representations.
28. **[ICLR 2026]** Ziquan Zhu, Hanruo Zhu, Si-Yuan Lu, Xiang Li, Yanda Meng, Yunxiao Zhang, Gaojie Jin, Lu Yin, Lijie Hu, **Di Wang**, Lu Liu, Tianjin Huang. Dual-Kernel Adapter: Expanding Spatial Horizons for Data-Constrained Medical Image Analysis. International Conference on Learning Representations.
29. **[ICLR 2026]** Wenjie Sun, **Di Wang**, Lijie Hu. The Price of Amortized inference in Sparse Autoencoders. International Conference on Learning Representations.
30. **[ICLR 2026]** Chenyang Ren*, Huanyi Xie*, Shu Yang, Meng Ding, Dongrui Liu, Lijie Hu, **Di Wang**. Evaluating Data Influence in Meta Learning. International Conference on Learning Representations.
31. **[ICLR 2026]** Huanyi Xie*, Chenyang Ren*, Khoulood Saadi, Shu Yang, Zhen Tan, Jingfeng Zhang, Lijie Hu, **Di Wang**. Dissecting Representation Misalignment in Contrastive Learning via Influence Function. International Conference on Learning Representations.
32. **[ICLR 2026]** Huanyi Xie, Yubin Chen, Liangyu Wang, Lijie Hu, **Di Wang**. Predicting LLM Output Length via Entropy-Guided Representations. International Conference on Learning Representations.
33. **[ICLR 2026]** Shaopeng Fu, **Di Wang**. Understanding and Improving LLMs' Continuous Adversarial Training via In-context Learning Theory. International Conference on Learning Representations.
34. **[WWW 2026]** Manjiang Yu*, Hongji Li*, Priyanka Singh, Xue Li, **Di Wang**, Lijie Hu. PIXEL: Adaptive Steering Via Position-wise Injection with eXact Estimated Levels under a Subspace Constraint. The ACM Web Conference.
35. **[AAMAS 2026 (EA Track)]** Jiawei Guo, Hongjie Nie, Qianbo Zang, Shu Yang, Shuodi Liu, Yiwei Ru, Liuyu Xiang, **Di Wang**, Zhaofeng He. The Web Tool Trap: Understanding and Mitigating Over-Reliance in Browsing Agents. International Conference on Autonomous Agents and Multiagent Systems (Extend Abstract).
36. **[AAMAS 2026 (EA Track)]** Hanpu Shen*, Cheng-Long Wang*, Zihang Xiang, Yiming Ying, **Di Wang**. Differentially Private Non-convex Learning: From Generalized Linear Models to Multi-layer Neural Networks. International Conference on Autonomous Agents and Multiagent Systems (Extend Abstract).
37. **[NDSS 2026]** Zihang Xiang, Tianhao Wang, Cheng-Long Wang, **Di Wang**. Revisiting Differentially Private Hyper-parameter Tuning. Network and Distributed System Security Symposium.
38. **[AAAI 2026]** Keyu Wang*, Jin Li*, Shu Yang, Zhuoran Zhang, **Di Wang**. When Truth Is Overridden: Uncovering the Internal Origins of Sycophancy in Large Language Models. AAAI Conference on Artificial Intelligence.

39. **[ICSE 2026]** Zhaoyang Chu, Yao Wan, Zhikun Zhang, **Di Wang**, Zhou Yang, Hongyu Zhang, Pan Zhou, Xuanhua Shi, Hai Jin, David Lo. Scrub It Out! Erasing Sensitive Memorization in Code Language Models via Machine Unlearning. IEEE/ACM International Conference on Software Engineering.
40. **[BIBM 2025]** Ziwen Cui, Muhammad Asif Ali, Ruigang Liu, Wen Zhang, Huan Wang, **Di Wang**. Enhancing Drug-Drug Interaction Prediction via Drug-Centric Hierarchical Augmentation. IEEE International Conference on Bioinformatics and Biomedicine.
41. **[NeurIPS 2025]** Xiaochuan Gou*, Ziyue Li*, Tian Lan, Junpeng Lin, Zhishuai Li, Bingyu Zhao, Chen Zhang, **Di Wang**, Xiangliang Zhang. TrafficDent: A Dataset for Understanding the Interplay Between Traffic Dynamics and Incidents. Conference on Neural Information Processing Systems (Datasets and Benchmarks Track).
42. **[NeurIPS 2025]** Liangyu Wang, Junxiao Wang, Jie Ren, Zihang Xiang, David Keyes, **Di Wang**. Private Training Large-scale Models with Efficient DP-SGD. Conference on Neural Information Processing Systems.
43. **[NeurIPS 2025]** Shaopeng Fu, Liang Ding, Jingfeng Zhang, **Di Wang**. Short-length Adversarial Training Helps LLMs Defend Long-length Jailbreak Attacks: Theoretical and Empirical Evidence. Conference on Neural Information Processing Systems.
44. **[NeurIPS 2025]** Youming Tao, Zuyuan Zhang, Dongxiao Yu, Xiuzhen Cheng, Falko Dressler, **Di Wang**. Second-Order Convergence in Private Stochastic Non-Convex Optimization. Conference on Neural Information Processing Systems.
45. **[NeurIPS 2025]** Lin Zhang, Wenshuo Dong, Zhuoran Zhang, Shu Yang, Lijie Hu, Ninghao Liu, Pan Zhou, **Di Wang**. EAP-GP: Mitigating Saturation Effect in Gradient-based Automated Circuit Identification. Conference on Neural Information Processing Systems.
46. **[EMNLP Findings 2025]** Yi Su*, Jiayi Zhang*, Shu Yang, Xinhai Wang, Lijie Hu, **Di Wang**. Understanding How Value Neurons Shape the Generation of Specified Values in LLMs. Findings of Conference on Empirical Methods in Natural Language Processing.
47. **[EMNLP Findings 2025]** Tong Li*, Shu Yang*, Junchao Wu, Jiyao Wei, Lijie Hu, Mengdi Li, Derek F. Wong, Joshua R. Oltmanns, **Di Wang**. Can Large Language Models Identify Implicit Suicidal Ideation? An Empirical Evaluation. Findings of Conference on Empirical Methods in Natural Language Processing.
48. **[CoLM 2025]** Jiaming Zhang*, Mingxi Lei*, Meng Ding, Mengdi Li, Zihang Xiang, Difei Xu, Jinhui Xu, **Di Wang**. Towards User-level Private Reinforcement Learning with Human Feedback. Conference on Language Modeling.
49. **[CoLM 2025]** Liangyu Wang, Jie Ren, Hang Xu, Junxiao Wang, Huanyi Xie, David E. Keyes, **Di Wang**. Scalable Zeroth-Order Fine-Tuning for Extremely Large Language Models with Limited GPU Memory. Conference on Language Modeling.
50. **[ICCV 2025]** Lijie Hu*, Tianhao Huang*, Huanyi Xie, Xilin Gong, Chenyang Ren, Zhengyu Hu, Lu Yu, Ping Ma, and **Di Wang**. Semi-supervised Concept Bottleneck Model. International Conference on Computer Vision.
51. **[ECML-PKDD 2025]** Lijie Hu*, Songning Lai*, Yuan Hua*, Shu Yang, Jingfeng Zhang, **Di Wang**. Stable Vision Concept Transformers for Medical Diagnosis. European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases.
52. **[ECML-PKDD 2025]** Xizhi Tian, Meng Ding, Youming Tao, Zihang Xiang, **Di Wang**. Differentially Private Sparse Linear Regression with Heavy-tailed Responses. European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases.
53. **[ACL Findings 2025]** Shu Yang*, Shenzhe Zhu*, Zeyu Wu, Keyu Wang, Junchao Wu, Lijie Hu, Mengdi Li, Derek F. Wong, **Di Wang**. Fraud-R1 : A Comprehensive Benchmark for Assessing LLM Robustness Against Fraud and Phishing Inducement. Findings of Annual Meeting of the Association for Computational Linguistics.

54. **[ACL Findings 2025]** Keyuan Cheng*, Xudong Shen*, Yihao Yang*, Tengyue Wang, Yang Cao, Muhammad Asif Ali, Hanbin Wang, Lijie Hu, **Di Wang**. Benchmarking Large Language Models on Code Migration. Findings of Annual Meeting of the Association for Computational Linguistics.
55. **[ACL Findings 2025]** Keyuan Cheng*, Zijian Kan*, Zhixian He, Zhuoran Zhang, Muhammad Asif Ali, Ke Xu, Lijie Hu, **Di Wang**. CompKE: Complex Question Answering under Knowledge Editing. Findings of Annual Meeting of the Association for Computational Linguistics.
56. **[ACL Findings 2025]** Junchi Yao*, Shu Yang*, Jianhua Xu, Lijie Hu, Mengdi Li, **Di Wang**. Understanding and Mitigating the Repeat Curse in Large Language Models from a Feature Perspective. Findings of Annual Meeting of the Association for Computational Linguistics.
57. **[UAI 2025]** Meng Ding, Mingxi Lei, Shaowei Wang, Tianhang Zheng, **Di Wang**, and Jinhui Xu. Nearly Optimal Differentially Private ReLU Regression. Conference on Uncertainty in Artificial Intelligence.
58. **[ICML 2025]** Lijie Hu, Chenyang Ren, Zhengyu Hu, Hongbin Lin, Cheng-Long Wang, Zhen Tan, Weimin Lyu, Jingfeng Zhang, Hui Xiong, **Di Wang**. Editable Concept Bottleneck Models. International Conference on Machine Learning.
59. **[ICML 2025]** Zhuoran Zhang, Yongxiang Li, Zijian Kan, Keyuan Cheng, Lijie Hu, **Di Wang**. Locate-then-edit for Multi-hop Factual Recall under Knowledge Editing. International Conference on Machine Learning.
60. **[IJCAI 2025]** Yifan Hong, Muhammad Asif Ali, Huan Wang, Junyang Chen, **Di Wang**. ABNets: Mitigating Sample Imbalance in Anomaly Detection within Dynamic Graphs. International Joint Conference on Artificial Intelligence.
61. **[NAACL Findings 2025]** Lin Zhang, Lijie Hu, **Di Wang**. Mechanistic Unveiling of Transformer Circuits: Self-Influence as a Key to Model Reasoning. Findings of Annual Conference of the Nations of the Americas Chapter of the Association for Computational Linguistics.
62. **[WWW 2025]** Ruohan Yang*, Muhammad Asif Ali*, Huan Wang, Junyang Chen, **Di Wang**. LUSTER: Link Prediction Utilizing Shared-Latent Space Representation in Multi-Layer Networks. The ACM on Web Conference.
63. **[USENIX 2025]** Cheng-Long Wang, Qi Li, Zihang Xiang, Yinzhi Cao, **Di Wang**. Towards Lifecycle Unlearning Commitment Management: Measuring Sample-level Approximate Unlearning Completeness. USENIX Security Symposium.
64. **[USENIX 2025]** Zihang Xiang, Tianhao Wang, **Di Wang**. Privacy Audit as Bits Transmission: (Im)possibilities for Audit by One Run. USENIX Security Symposium.
65. **[USENIX 2025]** Shaowei Wang, Changyu Dong, Xiangfu Song, Jin Li, Zhili Zhou, **Di Wang**, Han Wu. Beyond Statistical Estimation: Differentially Private Individual Computation in the Shuffle Model. USENIX Security Symposium.

Selected as honorable mention paper

66. **[AAAI 2025]** Zihao Luo*, Xilie Xu*, Feng Liu, Yun Sing Koh, **Di Wang**, Jingfeng Zhang. Privacy-Preserving Low-Rank Adaptation against Membership Inference Attacks for Latent Diffusion Models. AAAI Conference on Artificial Intelligence.

Best Paper Award, Workshop on Connecting Low-Rank Representations in AI

67. **[AAAI 2025]** Jia Li*, Lijie Hu*, Tianhang Zheng, Jingfeng Zhang, Hua Zhang, **Di Wang**. Fair Text-to-Image Diffusion via Fair Mapping. AAAI Conference on Artificial Intelligence.

Selected as an oral paper

68. **[AAAI 2025]** Ruijia Zhang*, Mingxi Lei*, Meng Ding, Zihang Xiang, Jinhui Xu, **Di Wang**. Differentially Private Non-convex and Strongly Concave Minimax Optimization. AAAI Conference on Artificial Intelligence.

69. [COLING 2025] Muhammad Asif Ali, Nawal Daftardar, Mutayyba Waheed, Jianbin Qin, **Di Wang**. MQA-KEAL: Multi-hop Question Answering under Knowledge Editing for Arabic Language. International Conference on Computational Linguistics.
70. [NeurIPS 2024] Liyang Zhu, Amina Manseur, Jinyan Liu, **Di Wang**. Truthful High Dimensional Sparse Linear Models. Conference on Neural Information Processing Systems.
71. [NeurIPS 2024] Meng Ding, Mingxi Lei, Liyang Zhu, Shaowei Wang, **Di Wang**, Jinhui Xu. Revisiting Differentially Private ReLU Regression. Conference on Neural Information Processing Systems.
72. [NeurIPS 2024] Keyi Kong, Xilie Xu, **Di Wang**, Jingfeng Zhang, Mohan Kankanhalli. Perplexity-aware Correction for Robust Alignment with Noisy Preferences. Conference on Neural Information Processing Systems.
73. [NeurIPS 2024] Lijie Hu*, Songning Lai*, Wenshuo Chen*, Hongru Xiao, Hongbin Lin, Lu Yu, Jingfeng Zhang, **Di Wang**. Towards Multi-dimensional Explanation Alignment for Medical Classification. Conference on Neural Information Processing Systems.
74. [EMNLP 2024] Yihuai Hong, Yuelin Zou, Lijie Hu, Ziqian Zeng, **Di Wang**, Haiqin Yang. Dissecting Fine-Tuning Unlearning in Large Language Models. Conference on Empirical Methods in Natural Language Processing.
Selected as an oral paper
75. [EMNLP 2024] Tianhao Huang*, Tao Yang*, Ivan Habernal, Lijie Hu, **Di Wang**. Private Language Models via Truncated Laplacian Mechanism. Conference on Empirical Methods in Natural Language Processing (EMNLP 2024).
Selected as an oral paper
76. [CoLM 2024] Keyuan Cheng*, Gang Lin*, Haoyang Fei*, Yuxuan Zhai, Lu Yu, Muhammad Asif Ali, Lijie Hu, **Di Wang**. Multi-hop Question Answering under Temporal Knowledge Editing. Conference on Language Modeling.
77. [CoLM 2024] Shu Yang*, Muhammad Asif Ali*, Lu Yu, Lijie Hu, and **Di Wang**. Model Autophagy Analysis to Explicate Self-consumption within Human-AI Interactions. Conference on Language Modeling.
78. [ACL Findings 2024] Jiahuan Pei, Irene Viola, Haochen Huang, Junxiao Wang, Moonisa Ahsan, Fanghua Ye, Yiming Jiang, Yao Sai, **Di Wang**, Zhumin Chen, Pengjie Ren, Pablo Cesar. Autonomous Workflow For Multimodal Fine-Grained Training Assistants Towards Mixed Reality. Findings of Annual Meeting of the Association for Computational Linguistics.
79. [ICML 2024] Lijie Hu*, Yinxin Liu*, Ninghao Liu, Mengdi Huai, Lichao Sun, **Di Wang**. Improving Interpretation Faithfulness for Vision Transformers. International Conference on Machine Learning.
Selected as a spotlight paper.
80. [ICML 2024] Mudit Gaur, Amrit Bedi, **Di Wang**, Vaneet Aggarwal. Closing the Gap: Achieving Global Convergence (Last Iterate) of Actor-Critic under Markovian Sampling with Neural Network Parametrization. International Conference on Machine Learning.
Selected as a spotlight paper
81. [ICML 2024] Meng Ding, Kaiyi Ji, **Di Wang**, Jinhui Xu. Understanding Forgetting in Continual Learning with Linear Regression. International Conference on Machine Learning.
82. [IEEE SP 2024] Zihang Xiang, Tianhao Wang and **Di Wang**. Preserving Node-level Privacy in Graph Neural Networks. IEEE Symposium on Security and Privacy.
83. [EACL Findings 2024] Muhammad Asif Ali, Yan Hu, Jianbin Qin and **Di Wang**. Antonym vs Synonym Distinction using Interlaced Encoder NETWORKS (ICE-NET). Findings of Conference of the European Chapter of the Association for Computational Linguistics.
84. [EACL Findings 2024] Lijie Hu, Ivan Habernal, Lei Shen, **Di Wang**. Differentially Private Natural Language Models: Recent Advances and Future Directions. Findings of Conference of the European Chapter of the Association for Computational Linguistics.

85. [ICLR 2024] Xilie Xu, Keyi Kong, Ning Liu, Lizhen Cui, **Di Wang**, Jingfeng Zhang, Mohan Kankanhalli. LLMs Can Fool Itself: A Prompt-based Adversarial Attack. International Conference on Learning Representations.
86. [ICLR 2024] Songning Lai*, Lijie Hu*, Junxiao Wang, Laure Berti, **Di Wang**. Faithful Vision-Language Interpretation via Concept Bottleneck Models. International Conference on Learning Representations.
87. [ICLR 2024] Shaopeng Fu, **Di Wang**. Theoretical Analysis of Robust Overfitting for Wide DNNs: An NTK Approach. International Conference on Learning Representations.
88. [ICLR 2024] Liyang Zhu*, Meng Ding*, Vaneet Aggarwal, Jinhui Xu, **Di Wang**. Improved Analysis of Sparse Linear Regression in Local Differential Privacy Model. International Conference on Learning Representations.
89. [VLDB 2024] Shaowei Wang, Yun Peng, Jin Li, Zikai Wen, Zhipeng Li, Shiyu Yu, **Di Wang**, and Wei Yang. Privacy Amplification via Shuffling: Unified, Simplified, and Tightened. International Conference on Very Large Databases.
90. [VLDB 2024] Youming Tao*, Cheng-Long Wang*, Miao Pan, Dongxiao Yu, Xiuzhen Cheng, **Di Wang**. Communication Efficient and Provable Federated Machine Unlearning. International Conference on Very Large Databases.
91. [ArabicNLP 2023] Muhammad Asif Ali, Maha Alshamrani, Jianbin Qin, Yan Hu, **Di Wang**. GARI: Graph Attention for Relative Isomorphism of Arabic Word Embeddings. Arabic Natural Language Processing Conference.
92. [ENMLP Findings 2023] Jinyan Su, Terry Yue Zhuo, Di Wang, Preslav Nakov. DetectLLM: Leveraging Log-Rank Information for Zero-Shot Detection of Machine-Generated Text. Findings of Conference on Empirical Methods in Natural Language Processing.
93. [ENMLP Findings 2023] Muhammad Asif Ali, Yan Hu, Jianbin Qin and **Di Wang**. GRI: Graph-based Relative Isomorphism of Word Embedding Spaces. Findings of Conference on Empirical Methods in Natural Language Processing.
94. [NeurIPS 2023] Yulian Wu*, Xingyu Zhou*, Youming Tao, **Di Wang**. On Robust and Private Multi-Armed Bandits. Conference on Neural Information Processing Systems.
95. [ECAI 2023] **Di Wang***, Jiahao Ding*, Lijie Hu, Zejun Xie, Miao Pan, Jinhui Xu. Finite Sample Statistical Guarantees of Private Expectation Maximization Algorithm. European Conference on Artificial Intelligence (ECAI 2023).
96. [UAI 2023] Jinyan Su, Changhong Zhao, **Di Wang**. Differentially Private Stochastic Convex Optimization in (Non)-Euclidean Space Revisited. Conference on Uncertainty in Artificial Intelligence.
97. [ICML 2023] Yulian Wu, Xingyu Zhou, Sayak Ray Chowdhury, **Di Wang**. Differentially Private Episodic Reinforcement Learning with Heavy-tailed Rewards. International Conference on Machine Learning.
98. [USENIX 2023] Cheng-Long Wang, Mengdi Huai, **Di Wang**. Inductive Graph Unlearning. USENIX Security Symposium.
99. [IEEE SP 2023] Hanshen Xiao*, Zihang Xiang*, **Di Wang**, Srini Devadas. A Theory to Instruct Differentially-Private Learning via Clipping Bias Reduction. IEEE Symposium on Security and Privacy.
100. [MobiSys 2023] Rui Chen, Qiyu Wan, Xinyue Zhang, Xiaoqi Qin, Yanzhao Hou, **Di Wang**, Xin Fu, Miao Pan. EEFL: High-Speed Wireless Communications Inspired Energy Efficient Federated Learning over Mobile Devices. ACM International Conference on Mobile Systems, Applications, and Services.
101. [SIGMOD 2023] Zihang Xiang, Tianhao Wang, Wanyu Lin, **Di Wang**. Practical Differentially Private and Byzantine-resilient Federated Learning. International Conference on Management of Data.

102. [AISTATS 2023] Lijie Hu*, Zihang Xiang*, Jiabin Liu, **Di Wang**. Privacy-preserving Sparse Generalized Eigenvalue Problem. International Conference on Artificial Intelligence and Statistics.
103. [AAAI 2023] Lijie Hu*, Yixin Liu*, Mengdi Huai, Ninghao Liu, Lichao Sun and **Di Wang**. SEAT: Stable and Explainable Attention. AAAI Conference on Artificial Intelligence.
Selected as an oral paper
104. [WINE 2022] Yuan Qiu, Jinyan Liu, **Di Wang**. Truthful Generalized Linear Models. Conference on Web and Internet Economics.
105. [ACML 2022] Jinyan Su, Jinhui Xu and **Di Wang**. On PAC Learning Halfspaces in Non-interactive Local Privacy Model with Public Unlabeled Data. Asian Conference on Machine Learning.
Best Paper Award of ACML 2022
106. [ISIT 2022] **Di Wang**, Jinhui Xu. Differentially Private ℓ_1 -norm Linear Regression with Heavy-tailed Data. IEEE International Symposium on Information Theory.
107. [IJCAI-ECAI 2022] Youming Tao, Yulian Wu, Xiuzhen Cheng, **Di Wang**. Private Stochastic Convex Optimization and Sparse Learning with Heavy-tailed Data Revisited. International Joint Conference on Artificial Intelligence.
108. [AISTATS 2022] Youming Tao*, Yulian Wu*, Peng Zhao, **Di Wang**. Optimal Rates of (Locally) Differentially Private Heavy-tailed Multi-Armed Bandits. International Conference on Artificial Intelligence and Statistics.
Selected as an oral paper
109. [AISTATS 2022] Vincent Cohen-Addad, Yunus Esencayi, Chenglin Fan, Marco Gaboardi, Shi Li, **Di Wang**. On Facility Location Problem in the Local Differential Privacy Model. International Conference on Artificial Intelligence and Statistics. (**Authors are alphabetically ordered**)
110. [ALT 2022] Jinyan Su, Lijie Hu, **Di Wang**. Faster Rates of Private Stochastic Convex Optimization. International Conference on Algorithmic Learning Theory.
111. [PODS 2022] Lijie Hu, Shuo Ni, Hanshen Xiao, **Di Wang**. High Dimensional Differentially Private Stochastic Optimization with Heavy-tailed Data. ACM Symposium on Principles of Database Systems (PODS 2022).
Invited to The ACM Transactions on Database Systems special issue on Best of PODS 2022.
112. [IJCAI 2021] Zhiyu Xue*, Shaoyang Yang*, Mengdi Huai, **Di Wang**. Differentially Private Pairwise Learning Revisited. International Joint Conference on Artificial Intelligence.
113. [ALT 2021] **Di Wang***, Huanyu Zhang*, Marco Gaboardi, Jinhui Xu. Estimating Smooth GLM in Non-interactive Local Differential Privacy Model with Public Unlabeled Data. International Conference on Algorithmic Learning Theory.
114. [BIBM 2020] Mengdi Huai, Chenglin Miao, Jinduo Liu, **Di Wang**, Jingyuan Chou, Aidong Zhang. Global Interpretation for Patient Similarity Learning. IEEE International Conference on Bioinformatics and Biomedicine.
115. [ECML-PKDD 2020] **Di Wang**, Jinhui Xu. Escaping Saddle Points of Empirical Risk Privately and Scalably via DP-Trust Region Method. European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Database.
116. [ICML 2020] **Di Wang***, Hanshen Xiao*, Srinivas Devadas, Jinhui Xu. On Differentially Private Stochastic Convex Optimization with Heavy-tailed Data. International Conference on Machine Learning.
117. [AAAI 2020] Mengdi Huai*, **Di Wang***, Chenglin Miao, Jinhui Xu, Aidong Zhang. Pairwise Learning with Differential Privacy Guarantees. AAAI Conference on Artificial Intelligence.
118. [AAAI 2020] **Di Wang***, Xiangyu Guo*, Chaowen Guan, Shi Li, Jinhui Xu. Estimating Stochastic Linear Combination of Non-Linear Regressions. AAAI Conference on Artificial Intelligence.

119. [AAAI 2020] Mengdi Huai, **Di Wang**, Chenglin Miao, Aidong Zhang. Towards Interpretation of Pairwise Learning. AAAI Conference on Artificial Intelligence.
120. [NeurIPS 2019] Yunus Esencayi, Marco Gaboardi, Shi Li, **Di Wang**. Facility Location Problem in Differential Privacy Model Revisited. Conference on Neural Information Processing Systems. (Authors are alphabetically ordered)
121. [IJCAI 2019] Mengdi Huai, **Di Wang**, Chenglin Miao, Jinhui Xu, Aidong Zhang. Privacy-aware Synthesizing for Crowdsourced Data. International Joint Conference on Artificial Intelligence
122. [IJCAI 2019] **Di Wang**, Jinhui Xu. Principal Component Analysis in the Local Differential Privacy Model. International Joint Conference on Artificial Intelligence
123. [IJCAI 2019] **Di Wang**, Jinhui Xu. Lower Bound of Locally Differentially Private Sparse Covariance Matrix Estimation. International Joint Conference on Artificial Intelligence.
124. [ICML 2019] **Di Wang**, Jinhui Xu. On Sparse Linear Regression in the Local Differential Privacy Model. International Conference on Machine Learning.
Selected as a long talk paper
125. [ICML 2019] **Di Wang**, Changyou Chen, Jinhui Xu. Differentially Private Empirical Risk Minimization with Non-convex Loss Functions. International Conference on Machine Learning.
126. [CISS 2019] **Di Wang**, Jinhui Xu, Yang He. Estimating Sparse Covariance Matrix Under Differential Privacy via Thresholding. Annual Conference on Information Sciences and Systems.
127. [ALT 2019] **Di Wang**, Adam Smith, Jinhui Xu. Noninteractive Locally Private Learning of Linear Models via Polynomial Approximations. International Conference on Algorithmic Learning Theory.
128. [AAAI 2019] **Di Wang**, Jinhui Xu. Differentially Private Empirical Risk Minimization with Smooth Non-Convex Loss Functions: A Non-Stationary View. AAAI Conference on Artificial Intelligence.
Selected as an oral paper
129. [NeurIPS 2018] **Di Wang**, Marco Gaboardi, Jinhui Xu. Empirical Risk Minimization in Non-interactive Local Differential Privacy Revisited. Conference on Neural Information Processing Systems.
130. [GlobalSIP 2018] **Di Wang**, Mengdi Huai, Jinhui Xu. Differentially Private Sparse Inverse Covariance Estimation. IEEE Global Conference on Signal and Information Processing.
131. [AAAI 2018] **Di Wang**, Jinhui Xu. Large Scale Constrained Linear Regression Revisited: Faster Algorithms via Preconditioning. AAAI Conference on Artificial Intelligence.
Selected as an oral paper
132. [NeurIPS 2017] **Di Wang**, Mingwei Ye, Jinhui Xu. Differentially Private Empirical Risk Minimization Revisited: Faster and More General. Conference on Neural Information Processing Systems.

Peer-Refereed Journal Papers

133. [IANDC] Jinyan Su*, Difei Xu*, Changhong Zhao, **Di Wang**. Revisiting Differentially Private Stochastic Convex Optimization in (Non)-Euclidean Space. Information and Computation.
134. [JSTQE] Jacob Rada, Jiajun Li, Xiaochuan Gou, Aditya Chivate, Haifeng Hu, Murali Gedda, **Di Wang**, Qiwen Zhan, Chi Zhou, Qiaoqiang Gan. Microscale-concave-interface-induced Moiré fringes for smart spectral reconstruction. IEEE Journal of Selected Topics in Quantum Electronics.
135. [TMLR] Junchi Liao, Weimin Lyu, Lijie Hu, Shaopeng Fu, Tianhao Huang, Shu Yang, Jie Li, **Di Wang**. Towards Representation Backdoor on CLIP via Concept Confusion. Transactions on Machine Learning Research.
136. [TMLR] Huanyi Xie, Lijie Hu, Lu Yu, Tianhao Huang, Longfei Li, Meng Li, Jun Zhou, **Di Wang**. Efficient Text-Attributed Graph Learning through Selective Annotation and Graph Alignment. Transactions on Machine Learning Research.

137. [ToN] Youming Tao, Zuyuan Zhang, **Di Wang**, Dongxiao Yu, Xiuzhen Cheng, Falko Dressler. Byzantine-Robust Machine Learning under Heterogeneity and Heavy-Tailed Noise. *IEEE Transactions on Networkings*.
138. [ToN] Youming Tao, Weijun Yin, Huanyi Xie, Yanqing Yao, Dongxiao Yu, Xiuzhen Cheng, **Di Wang**, Falko Dressler. One-Shot Federated Model Editing for Device Dynamics at the Edge. *IEEE Transactions on Networking*.
139. [ToN] Rui Chen, Qiyu Wan, Xinyue Zhang, Xiaoqi Qin, Yanzhao Hou, **Di Wang**, Xin Fu, Miao Pan. Wireless Aware Energy Efficient Federated Learning over Mobile Devices via Algorithm and Hardware Co-Design. *IEEE Transactions on Networking*.
140. [Advanced Science] Qizhe Chen*, Yifei Ren*, Lijie Hu*, Yanyan Li, Wenyue Liang, Jin Wang, Han Gao, Xinhai Wang, Jiajun Li, Qiutao He, Yingfeng Zhu, Haifeng Hu, Qiwen Zhan, Imed Gallouzi, Jasmine Merzaban, **Di Wang**, Zunguo Du, Xiaodong Gu, Qiaoqiang Gan. Intelligent Stain-free Histology on Structural Colorimetric Nanocavities. *Advanced Science*.
141. [AP] Zhican Zhou*, William He*, Xuhao Wu, Xiangpeng Ou, Xinhai Wang, Hanguang Liao, Ying Shi, Yuxuan Xie, **Di Wang**, Atif Shamim, John E. Bowers, Yating Wan. Integrated Quantum Dot Lasers for Parallelized Photonic Edge Computing. *Advanced Photonics*.
142. [CJE] Youming Tao, **Di Wang***, Xiuzhen Cheng*. Nearly-Tight Bounds for Private Stochastic Convex Optimization and Sparse Learning under Heavy Tails. *Chinese Journal of Electronics*.
143. [TWEB] Ruohan Yang, Muhammad Asif Ali, Anyu Xue, Huan Wang, Junyang Chen, **Di Wang**. Generative Regularities in Multi-Layer Networks: A Shared-Latent Space Representation Approach. *ACM Transactions on the Web*.
144. [TACL] Shu Yang, Junchao Wu, Xin Chen, Yunze Xiao, Xinyi Yang, Derek F. Wong, **Di Wang**. Understanding Aha Moments: from External Observations to Internal Mechanisms. *Transactions of the Association for Computational Linguistics*.
145. [TKDE] Ruohan Yang*, Muhammad Asif Ali*, Huan Wang, Zhongfei Zhang, Junyang Chen, **Di Wang**. PRISM: Link Prediction in Attributed Networks with Uncertain Modalities. *IEEE Transactions on Knowledge and Data Engineering*.
146. [ACS] Jiayi Wang*, Chunwei Dong*, Xiaochuan Gou, Shaopeng Fu, Peng Yuan, Xin Song, Boduzzaman Mohammad, Wanyu Lin, **Di Wang**, Osman Bakr. Deep Learning Framework for Atomic-Level Design and Presynthesis Prediction of Coinage-Metal Nanoclusters. *ACS Central Science*.
147. [TACL] Xin Chen, Junchao Wu, Shu Yang, Runzhe Zhan, **Di Wang**, Ziyang Luo, Lidia S. Chao, Derek F. Wong. RepreGuard: Detecting LLM-Generated Text by Revealing Hidden Representation Patterns. *Transactions of the Association for Computational Linguistics*.
148. [JECE] Chongchong Qi*, Tao Hu*, Mengting Wu, Ping Zhang, Sybil Derrible, **Di Wang**, Yong Sik Ok, Zhang Lin. Machine Learning and Soil Spectra Enable Rapid Identification of Multiple Heavy Metals at the Continental Scale. *Journal of Environmental Chemical Engineering*.
149. [TIT] Shaopeng Fu, **Di Wang**. Theoretical Analysis of Robust Overfitting for Wide DNNs: An NTK Approach. *IEEE Transactions on Information Theory*.
150. [TIFS] Shaowei Wang, Jin Li, Changyu Dong, Jin Li, Zhili Zhou, **Di Wang**, Zikai Wen. Side-channel Attacks and New Principles in the Shuffle Model of Differential Privacy. *IEEE Transactions on Information Forensics and Security*.
151. [TMLR] Difei Xu, Meng Ding, Zihang Xiang, Jinhui Xu, **Di Wang**. Beyond ordinary Lipschitz constraints: Differentially Private Optimization with TNC. *Transactions on Machine Learning Research*.
152. [TMLR] Lijie Hu*, Tianhao Huang*, Lu Yu, Wanyu Lin, Tianhang Zheng, **Di Wang**. Faithful Interpretation for Graph Neural Networks. *Transactions on Machine Learning Research*.

153. [TKDE] Huan Wang, Junyang Chen, Yirui Wu, Victor C. M. Leung, **Di Wang**. EPM: Evolutionary Perception Method for Anomaly Detection in Noisy Dynamic Graphs. *IEEE Transactions on Knowledge and Data Engineering*.
154. [TKDE] Lijie Hu*, Xinhai Wang*, Yixin Liu*, Ninghao Liu, Mengdi Huai, Lichao Sun, **Di Wang**. Towards Stable and Explainable Attention Mechanisms. *IEEE Transactions on Knowledge and Data Engineering*.
155. [TIFS] Jian Chen, Zehui Lin, Wanyu Lin, Wenlong Shi, Xiaoyan Yin, **Di Wang**. FedMUA: Exploring the Vulnerabilities of Federated Learning to Malicious Unlearning Attacks. *IEEE Transactions on Information Forensics and Security*.
156. [NC] Puyu Wang, Yunwen Lei, **Di Wang**, Yiming Ying, Ding-Xuan Zhou. Generalization Guarantees of Gradient Descent for Shallow Neural Networks. *Neural Computation*.
157. [TCS] **Di Wang**, Jinhui Xu. Private Least Absolute Deviations with Heavy-tailed Data. *Theoretical Computer Science*.
158. [IPM] Guanghua Liu, Jia Zhang, Peng Lv, Chenlong Wang, Huan Wang, **Di Wang**. TAAD: Time-varying Adversarial Anomaly Detection in Dynamic Graphs. *Information Processing and Management*.
159. [TBD] Wen Zhang, Haitao Fu, Huan Wang, Zhiguo Gong, Pan Zhou, **Di Wang**. 3A Multi-classification Division-aggregation Framework for Fake News Detection. *IEEE Transactions on Big Data*.
160. [IANDC] Yuan Qiu, Jinyan Liu, **Di Wang**. Truthful and Privacy-preserving Generalized Linear Models. *Information and Computation*.
161. [TKDD] Yidong Wang*, Meng Ding*, Jinhui Xu, **Di Wang**. Fair Single Index Models. *ACM Transactions on Knowledge Discovery from Data*.
162. [TCSS] Yifan Hong, Chuanqi Shi, Junyang Chen, Huan Wang, **Di Wang**. Multitask Asynchronous Meta-learning for Few-shot Anomalous Node Detection in Dynamic Networks. *IEEE Transactions on Computational Social Systems*.
163. [TMC] Youming Tao, Shuzhen Chen, Congwei Zhang, **Di Wang**, Dongxiao Yu, Xiuzhen Cheng, and Falko Dressler. Private Over-the-Air Federated Learning at Band-Limited Edge. *IEEE Transactions on Mobile Computing*.
164. [JMLR] Jinyan Su, Lijie Hu, **Di Wang**. Faster Rates of Differentially Private Stochastic Convex Optimization. *Journal of Machine Learning Research*.
165. [TMLR] Minghua Wang, Yan Hu, Ziyun Huang, **Di Wang**, Jinhui Xu. Persistent Local Homology in Graph Learning. *Transactions on Machine Learning Research*.
166. [LNET] Washim Uddin Mondal, Veni Goyal, Satish V. Ukkusuri, Goutam Das, **Di Wang**, Mohamed-Slim Alouini, Vaneet Aggarwal. Near-perfect Coverage Manifold Estimation in Cellular Networks via Conditional GAN. *IEEE Networking Letters*.
167. [SA] Juexiao Zhou*, Siyuan Chen*, Yulian Wu*, Haoyang Li, Bin Zhang, Longxi Zhou, Yan Hu, Zihang Xiang, Zongxiao Li, Ningning Chen, Wenkai Han, **Di Wang**, Xin Gao. PPML-Omics: a Privacy-Preserving Federated Machine Learning System Protects Patients Privacy from Omic Data. *Science Advances*.
168. [CBM] Juexiao Zhou*, Longxi Zhou*, **Di Wang**, Xiaopeng Xu, Haoyang Li, Yuetan Chu, Wenkai Han, and Xin Gao. Personalized and Privacy-preserving Federated Heterogeneous Medical Image Analysis with PPPML-HMI. *Computers in Biology and Medicine*.
169. [JCSS] Jinyan Su, Jinhui Xu, **Di Wang**. PAC Learning Halfspaces in Non-interactive Local Differential Privacy Model with Public Unlabeled Data. *Journal of Computer and System Sciences*.
170. [TKDE] Lijie Hu*, Zihang Xiang*, Jiabin Liu, **Di Wang**. Nearly Optimal Rates of Privacy-Preserving Sparse Generalized Eigenvalue Problem. *IEEE Transactions on Knowledge and Data Engineering*.

171. [TCS] **Di Wang**, Jinhui Xu. Gradient complexity and non-stationary views of differentially private empirical risk minimization. Theoretical Computer Science.
172. [TIT] Junren Chen, Michael Kwok Po NG, **Di Wang**. Quantizing Heavy-Tailed Data in Statistical Estimation: (Near) Minimax Rates, Covariate Quantization, and Uniform Recovery. IEEE Transactions on Information Theory.
173. [TIT] Junren Chen, Cheng-Long Wang, Michael Kwok Po NG, **Di Wang**. High Dimensional Statistical Estimation Under Uniformly Dithered One-Bit Quantization. IEEE Transactions on Information Theory.
174. [JMLR] **Di Wang***, **Lijie Hu***, Huanyu Zhang, Marco Gaboardi, Jinhui Xu. Generalized Linear Models in Non-interactive Local Differential Privacy with Public Data. Journal of Machine Learning Research.
175. [TCS] **Di Wang**, Jinhui Xu. Differentially Private High Dimensional Sparse Covariance Matrix Estimation. Theoretical Computer Science.
176. [TCS] **Di Wang**, Jinhui Xu. Inferring Ground Truth for Crowdsourcing Data Under Local Attribute Differential Privacy. Theoretical Computer Science.
177. [TIT] **Di Wang**, Jinhui Xu. On Sparse Linear Regression in the Local Differential Privacy Model. IEEE Transactions on Information Theory.
178. [JMLR] **Di Wang**, Marco Gaboardi, Adam Smith and Jinhui Xu. Empirical Risk Minimization in the Non-interactive Local Model of Differential Privacy. Journal of Machine Learning Research.
179. [MLJ] **Di Wang***, Xiangyu Guo*, Shi Li, Jinhui Xu. Robust High Dimensional Expectation Maximization Algorithm via Trimmed Hard Thresholding. Machine Learning.
180. [NEUCOM] **Di Wang***, Xiangyu Guo*, Chaowen Guan, Shi Li, Jinhui Xu. Estimating Stochastic Linear Combination of Non-linear Regressions Efficiently and Scalably. Neurocomputing.
181. [TCS] **Di Wang**, Jinhui Xu. Tight Lower Bound of Sparse Covariance Matrix Estimation in the Local Differential Privacy Model. Theoretical Computer Science.
182. [TCS] **Di Wang**, Jinhui Xu. Principal Component Analysis in the Local Differential Privacy Model. Theoretical Computer Science.
183. [NEUCOM] **Di Wang**, Jinhui Xu. Faster Constrained Linear Regression via Two-step Preconditioning. Neurocomputing.

PRESS COVERAGE

PPML-Omics protects patientss privacy in omic data

- Algorithm Proposed to Protect Patient Privacy, [Inside Precision Medicine](#)
- An integrated shuffler optimizes the privacy of personal genomic data used for machine learning, [Tech Xplore](#)
- Shuffling the deck for privacy, [Newswise](#)
- Shuffling the deck for privacy, [EurekAlert](#)
- Novel Privacy-Preserving Machine-Learning Method Developed for Genomics Data, [Biocompare](#)
- Shuffling The Deck For Privacy, [Eurasia Review](#)
- Revolutionizing Medical Research: Scientists Develop Groundbreaking Privacy-Preserving AI, [SciTech-Daily](#)

Intelligent Stain-free Histology on Structural Colorimetric Nanocavities

- New Imaging Technology Could Speed Up Cancer Diagnosis, [Clinical Lab Products](#)
- Silicon-slide imaging could speed cancer diagnosis with 99% agreement, no dyes needed, [Medical Xpress](#)
- KAUST researchers develop technology that could make cancer diagnosis faster, [KAUST News](#)
- KAUST Develops New Technology to Advance AI-Powered Cancer Diagnosis, [The Saudi Times](#)
- KAUST researchers develop technology that could make cancer diagnosis faster, [Al Arabiya TV](#)

RESEARCH SUPERVISION

Postdoc Researcher

1. Fengpeng Li, 04/2026-
2. Yuke Hu, 04/2026-
3. Peng Ye, 07/2026-

Students

1. Jiayi Wang (MSE PhD, Co-advised with Osman Bakr), 05/2023-06/2027
2. Shaopeng Fu (CS PhD), 09/2023-06/2027
3. Khouloud Saadi (CS PhD), 09/2024-
4. Shu Yang (CS PhD), 09/2024-
5. Difei Xu (STAT MS/PhD), 09/2024-
6. Huanyi Xie (CS MS/PhD), 09/2025-
7. Anis Oueslati (CS PhD), 09/2025-

ALUMNI

PhD Students

1. Liangyu Wang (CS PhD), 01/2023-09/2026
Next placement: Research Scientist, Qwen Team
2. Cheng-Long Wang (CS PhD), 09/2021-04/2026
Next placement: Research Scientist, Huawei 2012 Lab
3. Lijie Hu (CS PhD) 01/2021-06/2025, PhD student
Next placement: Tenure-track Assistant Professor, Mohamed bin Zayed University of Artificial Intelligence (MBZUAI).
4. Zihang Xiang (CS PhD) 01/2021-06/2025, PhD student
Next placement: Postdoc Researcher at University of California, Los Angeles.
5. Xiaochuan Gou, 09/2020-06/2025, PhD student
Next placement: Associate Professor at Dalian Maritime University

Master Students

1. Liyang Zhu (CS MS) 09/2022-08/2024, Master student
Next placement: PhD student in Computer Science at Duke University.

Postdoc Researcher

1. Mengdi Li, 09/2024-09/2025
Next placement: Research Scientist, Horizon Robotics
2. Junxiao Wang, 02/2023-01/2025
Next placement: Associate Professor at Guangzhou University.
3. Xiaodong Miao, 08/2023-01/2025, Postdoc Researcher
Next placement: Associate Professor at Nanjing Tech University.
4. Huan Wang, 09/2023-08/2025, Postdoc Researcher
Next placement: Associate Professor at Huazhong Agricultural University.
5. Muhammad Asif Ali, 01/2023-08/2024
Next placement: Postdoc Researcher at KAUST.
6. Yan Hu, 12/2021-12/2023, Postdoc Researcher
Next placement: Research Associate at The Chinese University of Hong Kong, Shenzhen
Current placement: Scientist at National Health Data Institute (Shenzhen), The Chinese University of Hong Kong, Shenzhen.

INVITED SPEAKER

Invited Talk

1. KAUST AI Symposium, April 2025
2. School of Informatics, Huazhong Agricultural University, January 2025
3. West Lake Forum on Cybersecurity, January 2025
4. School of Computer Science, Hunan University, December 2024
5. School of Artificial Intelligence, University of Science and Technology China, December 2024
6. School of Cybersecurity, Southeast University, December 2024
7. School of Computer Science, Harbin Institute of Technology, Shenzhen, December 2024
8. School of Computer Science, Sichuan University, November 2024
9. The KAUST Red Sea Research Conference on Frontier Technology, KAUST, November 2024
10. CS Graduate Seminar, KAUST, September 2024
11. School of Computer Science, Shanghai Jiao Tong University, June 2024
12. CS Graduate Seminar, KAUST, March 2024
13. School of Computer Science, University of Science and Technology China, June 2024
14. School of Cybersecurity, Huazhong University of Science and Technology, January 2024
15. KAUST-SFDA First Joint International Conference: Trends in Microbiome and Digital One Health, November 2023
16. CS Graduate Seminar, KAUST, November 2024
17. Royal Statistical Society 2023 Conference, September 2023
18. School of Cybersecurity, Zhejiang University, July 2023
19. School of Artificial Intelligence, Nanjing University, July 2023
20. School of Computer Science, Shandong University, June 2023
21. School of Computer Science, Beijing Institute of Technology, June 2023

22. KAUST 2022 Workshop on Statistics, KAUST, November 2022
23. Shenzhen Institute of Artificial Intelligence and Robotics for Society, October 2022
24. Department of Computer Science, University of Helsinki, August 2022
25. Computer Science Graduate Seminar, KAUST, April 2022
26. Analysis and Data Science Seminar, State University of New York at Albany, March 2022
27. STAT Graduate Seminar, KAUST, November 2021
28. Interdisciplinary Research Center of Intelligent Secure Systems, King Fahd University of Petroleum and Minerals, November 2021
29. Alumni Talks, State University of New York at Buffalo, October 2021
30. AMCS/STAT Graduate Seminar, KAUST, September 2021
31. Vision And Learning Seminar, Online, June 2021
32. Computer Science Graduate Seminar, KAUST, April 2021
33. KAUST Conference on Artificial Intelligence, April 2021
34. School of Cyber Science and Technology, Zhejiang University, September 2020
35. School of Computing and Information Systems, University of Melbourne, April 2020
36. Department of Computer Science and Engineering, Chinese University of Hong Kong, April 2020
37. Department of Computer Science, Dalhousie University, April 2020
38. CISPA-Helmholtz Center for Information Security, April 2020
39. Department of Computing, Hong Kong Polytechnic University, April 2020
40. Department of Computer Science, University of Memphis, April 2020
41. School of Computer Science, University of Sydney, April 2020
42. Department of Computing, Imperial College London, March 2020
43. King Abdullah University of Science and Technology, March 2020
44. Department of Computing and Software, McMaster University, March 2020
45. Department of Computer Science, City University of Hong Kong, March 2020
46. School of Information System, Singapore Management University, March 2020
47. Department of Computer Science, University College London, UK, March 2020
48. Department of Computer Science, University of Warwick, UK, March 2020
49. School of Computer Science, University of Birmingham, UK, March 2020
50. Department of Computer Science and Engineering, Hong Kong University of Science and Technology, February 2020
51. Department of Computer Science, McGill University, February 2020
52. Department of Computer Science, University of Surrey, UK, February 2020
53. Department of Computer Science, University of Science and Technology of China, November 2019
54. Department of Computer Science, Nanjing University, China, November 2019
55. Department of Computer Science, University of Alberta, November 2019

Conference Talk

1. Differentially Private Pairwise Learning Revisited. IJCAI 2021, Online.
2. Estimating Smooth GLMs in Non-interactive Local Differential Privacy Model with Public Unlabeled Data. ALT 2021, Online.
3. Robust High Dimensional Expectation Maximization Algorithm via Trimmed Hard Thresholding. ACML 2020, Online.
4. Escaping Saddle Points of Empirical Risk Privately and Scalably via DP-Trust Region Method. ECML-PKDD 2020, Online.
5. On the Differentially Private Stochastic Optimization with Heavy-tailed Data. ICML 2020, Online.
6. Principal Component Analysis in the Local Differential Privacy Model. IJCAI 2019. Macau, China, August, China (Online).
7. Lower Bound of Locally Differentially Private Sparse Covariance Matrix Estimation. IJCAI 2019. Macau, China, August, China (Online).
8. On the Locally Differentially Private Sparse Linear Regression. ICML 2019. Long Beach, CA, USA. June 2019.
9. Estimation Sparse Covariance Matrix Under Differential Privacy via Thresholding. CISS 2019. Baltimore, MD, USA. March 2019.
10. Empirical Risk Minimization in Non-interactive Local Model via Polynomial of Inner Product Approximation. ALT 2019. Chicago, IL, USA. March 2019.
11. Differentially Private Sparse Inverse Covariance Estimation. 2018 IEEE GlobalSIP Signal Processing for Adversarial Machine Learning. November, 2018.
12. Differentially Private Empirical Risk Minimization in the Non-interactive Local Model, Intern Presentation, Harvard University, June, 2018.
13. Large Scale Constrained Linear Regression Revisited Faster Algorithms via Preconditioning, The Thirty-Second Conference on Artificial Intelligence (AAAI), February, 2018.
14. Differentially Private Empirical Risk Minimization with Non-convex Loss Function, SUNY Buffalo CSE 50th Anniversary, University at Buffalo, September, 2017.

PROFESSIONAL SERVICE

Grant Review

- Swiss National Science Foundation
- GRF, Research Grants Council (RGC) of Hong Kong
- Deutsche Forschungsgemeinschaft (DFG)
- HBKU Student Innovation Fund
- FDS, Research Grants Council (RGC) of Hong Kong

Conference Organizer

- 1st ICLR International Workshop on Privacy, Accountability, Interpretability, Robustness, Reasoning on Structured Data

Senior Committee Member/Area Chair

- International Conference on Artificial Intelligence and Statistics (AISTATS 2023-2026)
- Neural Information Processing Systems (NeurIPS 2024-2026)
- AAAI Conference on Artificial Intelligence (AAAI 2022, 2026, 2027)
- International Conference on Machine Learning (ICML 2026)
- International Conference on Representation Learning (ICLR 2026, 2027)
- ACL ARR (2025 October, 2026 January, March)

Journal Editorial Board

- IEEE Computational Intelligence Letters, associate editor
- Theoretical Computer Science, associate editor
- ACM Transactions on Probabilistic Machine Learning, senior associate editor
- Journal of Machine Learning Research, editorial board of reviewers
- Transactions on Machine Learning Research, action editor
- Data-centric Machine Learning Research, action editor
- Neurocomputing

Technical Program Committee Member

- IEEE BigData 2026
- ACM Conference on Data and Application Security and Privacy (CODASPY 2024-2026)
- The 33rd International Joint Conference on Artificial Intelligence (IJCAI 2024)
- The ACM Conference on Computer and Communications Security (CCS 2023, 2024)
- 2024 SIAM International Conference on Data Mining (SDM 2024)
- AAAI Conference on Artificial Intelligence (AAAI 2020-2024)
- Privacy Enhancing Technologies Symposium (PETS), 2025
- The 32nd International Joint Conference on Artificial Intelligence Special Track On AI And Social Good (IJCAI 2023)
- The 15th International Workshop on Cyberspace Security and Artificial Intelligence (CAI 2023)
- European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD 2020, 2022, 2023)
- The 32nd International Joint Conference on Artificial Intelligence (IJCAI 2020, 2023)
- 2023 ACM Fairness, Accountability, and Transparency Conference (ACM FAccT 2023)
- AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI 2023)
- IEEE European Symposium on Security and Privacy 2023 (Euro S&P 2023)
- European Symposium on Research in Computer Security (ESORICS 2021, 2022, 2025)
- AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI 2022)
- NeurIPS 2021 workshop on Privacy in Machine Learning (PriML 2021)
- Winter Conference on Applications of Computer Vision (WACV 2020)
- IEEE Symposium on Security and Privacy 2020 (Shadow PC)

Reviewer (Journals)

- ACM Transactions on Algorithms
- IEEE Transactions on Computers
- Journal of Biomedical and Health Informatics
- Journal of Selected Topics in Signal Processing
- IEEE Transactions on Signal Processing
- IEEE Transactions on Machine Learning in Communications and Networking
- Machine Learning
- Computational Linguistics
- Statistics in Biosciences
- Bernoulli
- Technometrics
- Journal of Systems Architecture
- IEEE Transactions on Control of Network Systems
- ACM Transactions on Knowledge Discovery from Data
- Entropy
- IEEE Transactions on Knowledge and Data Engineering
- Transactions on Machine Learning Research
- IEEE Transactions on Dependable and Secure Computing
- Information Science
- Neurocomputing
- IEEE Transactions on Big Data
- ACM Computing Surveys
- IEEE Transactions on Information Forensics and Security
- IEEE Transactions on Pattern Analysis and Machine Intelligence
- Theoretical Computer Science
- Security and Communication Networks
- Patterns
- Frontiers of Information Technology & Electronic Engineering
- Computers & Security
- Artificial Intelligence
- Journal of the American Statistical Association
- Statistics and Probability Letters
- Computer Communications
- IEEE Transactions on Computational Social Systems
- European Journal of Operational Research

Reviewer (Conference)

- International Workshop on Combinatorial Image Analysis (IWCIA) 2017
- International Symposium CompIMAGE'18-Computational Modeling of Objects Presented in Images: Fundamentals, Methods, and Applications
- AAAI Conference on Artificial Intelligence (AAAI) 2017, 2018
- ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD) 2018, 2023, 2024
- International Conference on Artificial Intelligence and Statistics (AISTATS) 2019-2023
- International Conference on Machine Learning (ICML) 2019-2025
- IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR) 2019
- IEEE International Conference on Computer Vision (ICCV) 2019, 2021
- IEEE International Conference on Distributed Computing Systems (ICDCS) 2019
- Neural Information Processing Systems (NeurIPS) 2019-2023
- IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR) 2020-2026
- ACM Symposium on Theory of Computing (STOC) 2020
- European Conference on Computer Vision (ECCV) 2020-2026
- International Symposium on Computational Geometry (SoCG), 2020
- Annual Conference on Theory and Applications of Models of Computation (TAMC) 2020
- IEEE Winter Conference on Applications of Computer Vision (WACV), 2021-2024
- Asian Conference on Computer Vision (ACCV) 2020
- International Conference on Learning Representations (ICLR) 2021-2025,
- IEEE International Symposium on Information Theory (ISIT) 2021, 2026
- International Colloquium on Automata, Languages and Programming (ICALP) 2022
- Proceedings on Privacy Enhancing Technologies (PETs) 2023
- European Conference on Artificial Intelligence (ECAI) 2023
- Annual Conference on Learning Theory (COLT) 2024, 2025
- Conference on Language Modeling (CoLM) 2025
- CCF International Conference on Natural Language Processing and Chinese Computing (NLPCC) 2024

UNIVERSITY SERVICE AND OUTREACH

University Committees

- Student Admission Committee, Computer Science Program, 2023-2025
- Apple Fellowship Nomination Committee, 2025
- Divisional Internal Review Committee-KAUST Global Fellowship, 2025
- Hoster, CS 398: Graduate Seminar, Computer Science Program, 01/2024-12/2024

Outreach

- Saudi Research Science Institute (SRSI) Mentor
 1. Dewei Zhang (The Kaust School, SRSI), 07/2025-08/2025
 2. Saleh AlNassar (Al Tarbiyah Al Namouthajiyah International Schools, SRSI), 07/2025-08/2025
- Saudi Summer Internship Mentor
 1. Danya Alnajar (Undergraduate at University at Jeddah, SSI), 06/2021-08/2021
 2. Farah Albishri (Undergraduate at University at Jeddah, SSI), 06/2021-08/2021
 3. Maha Almuaikel (Undergraduate student at University of Jeddah, SSI), 06/2022-08/2022
 4. Maha Alshmrani (Undergraduate student at University of Tabuk, SSI), 06/2023-09/2023
 5. Nawal Daftardar (Undergraduate student at King Abdulaziz University, SSI), 06/2024-08/2024
 6. Lames Alrebeay (Undergraduate student at Umm Al-Qura University, SSI), 06/2025-08/2025
- KAUST Gifted Student Program (KGSP/KSIP) Mentor
 1. Ali Allail (Undergraduate student at Purdue University, KGSP), 06/2022-08/2022
 2. Ibraheem Alsaghier (Undergraduate at University of North Carolina at Chapel Hill, KGSP), 06/2022-08/2022
 3. Yazid Alhamed (Undergraduate student at New York University, KSIP), 06/2026-08/2026