Di Wang

Al Khawarizmi Building 1, Room 4341
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

WORK EXPERIENCE

King Abdullah University of Science and Technology — Thuwal, Saudi Arabia
Computer Science Program — *January 2021-Current*
Statistics Program (Affiliated Member)
Division of CEMSE
Assistant Professor
Director of Privacy-Awareness
Responsibility and Trustworthy Lab

EDUCATION

State University of New York at Buffalo — Buffalo, NY, United States
Ph.D. in Computer Science and Engineering — *August 2020*
Advisor: Dr. Jinhui Xu
Dissertation: Some Fundamental Machine Learning Problems in the Differential Privacy Model

Western University (University of Western Ontario) — London, ON, Canada
M.S. in Mathematics — *October 2015*

Shandong University — Jinan, Shandong, China
B.S. in Mathematics and Applied Mathematics — *June 2014*

CURRENT STATUS

Citizen of China

RESEARCH INTERESTS

Private Data Analytics

Differential privacy, privacy-preserving machine learning, privacy-preserving data mining, privacy attack

Trustworthy Machine Learning

Robust estimation, fairness in machine learning, machine unlearning interpretable machine learning, causality

Statistical Learning Theory

Large scale optimization, high dimensional optimization, statistical estimation, learning theory, quantum machine learning

Biomedicine and Healthcare

Trustworthy issues in digital healthcare, biomedical imaging and bioinformatics

RESEARCH EXPERIENCE

University of California at Berkeley — Berkeley, CA
Simons Institute for the Theory of Computing — *Spring 2019*
Data Privacy: Foundations and Applications
Visiting Graduate Student

Harvard University — Cambridge, MA
Harvard University Privacy Tools Project — *June to August 2018*
Research Graduate

Boston University — Boston, MA
Visiting Student — *June to August 2018*
Mentor: Dr. Adam D. Smith

State University of New York at Buffalo — Buffalo, NY
Research Assistant — *August 2015 to December 2020*
Supervisor: Dr. Jinhui Xu

HONORS and AWARDS

- 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.
- ICML Travel Award, 2019.
- NeurIPS/NIPS Travel Award, 2019, 2018, 2017.
- Western Graduate Research Scholarship, Western University, 2014-2015.
- Algebraic Geometry Summer School Scholarship, ECNU, Shanghai, 2013.

TEACHING EXPERIENCE

- **Instructor.** CS229: Machine Learning. Spring 2022, KAUST
- **Instructor.** CS394S: Contemporary Topics on Computer Security: Differential Privacy. Fall 2021, 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.** CSE574/474: Introduction to Machine Learning, Summer 2019, State University of New York at Buffalo.
- **Teaching Assistant.** CSE574/474: Introduction to Machine Learning, Spring 2018, State University of New York at Buffalo.
- **Teaching Assistant.** CSE531/431: Analysis of Algorithm, Fall 2017, Spring 2017, Fall 2016, Spring 2016, State University of New York at Buffalo.
- **Teaching Assistant.** CSE115: 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.

Fundings

- $1,600,000 USD (PI), KAUST Baseline Research Grant, 2021-2026
- $100,000 USD (PI), KAUST AI Initiative Fund, "Private and Fair Learning Algorithms for Healthcare", Joint with Xin Gao (KAUST, Co-PI), 2021-2022
- $1,050,000 USD (PI), CRG2021 Grant, "Modern Privacy-preserving Learning Algorithms for Biomedical Data", Joint with Xin Gao (KAUST, Co-PI) and Jinhui Xu (State University of New York at Buffalo, Co-PI), 2022-2025

SELECTED PUBLICATIONS

1. Youming Tao*, Yulian Wu*, Peng Zhao and **Di Wang**. Optimal Rates of (Locally) Differentially Private Heavy-tailed Multi-Armed Bandit. Submitted to *The 25th International Conference on Artificial Intelligence and Statistics (AISTATS 2022).*
2. Jinyan Su, Lijie Hu and **Di Wang**. Faster Rates of Differentially Private Stochastic Convex Optimization. *Submitted to The Conference on Algorithmic Learning Theory (ALT 2022).*
3. Lijie Hu, Shuo Ni, Hanshen Xiao and **Di Wang**. High Dimensional Differentially Private Heavy-tailed Stochastic Convex Optimization. *The 41st ACM Symposium on Principles of Database Systems (PODS 2022).*
4. **Di Wang** and Jinhui Xu. On Sparse Linear Regression in the Local Differential Privacy Model. *IEEE Transactions on Information Theory*, Volume 67, No. 2, Pages 1182-1200, Feb. 2021.
5. **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,* Volume 21, 200 (2020), Pages 1-39.
6. **Di Wang***, **Huanyu Zhang***, Marco Gaboardi and Jinhui Xu. Estimating Smooth GLMs in Non-interactive Local Differential Privacy Model with Public Unlabeled Data. *The 32nd International Conference on Algorithmic Learning Theory (ALT 2021),* Paris, France, March 16-19, 2021. (*** equally contributed co-first authors**)
7. **Di Wang***, **Hanshen Xiao***, Srinivas Devadas and Jinhui Xu. On Differentially Private Stochastic Convex Optimization with Heavy-tailed Data. *The 37th International Conference on Machine Learning (ICML 2020)*, Vienna, Austria, July 12-18, 2020. (*** equally contributed co-first authors**)
8. Yunus Esencayi, Marco Gaboardi, Shi Li and **Di Wang**. Facility Location Problem in Differential Privacy Model Revisited. *Advances in Neural Information Processing Systems (NeurIPS 2019)*, Vancouver, BC, Canada, December 08-14, 2019. (**Authors are alphabetically ordered**)
9. **Di Wang** and Jinhui Xu. On Sparse Linear Regression in the Local Differential Privacy Model. *The 36th International Conference on Machine Learning (ICML 2019)*, Long Beach, CA, USA, June 9-15, 2019.
10. **Di Wang**, Changyou Chen and Jinhui Xu. Differentially Private Empirical Risk Minimization with Non-convex Loss Functions. *The 36th International Conference on Machine Learning (ICML 2019)*, Long Beach, CA, USA, June 9-15, 2019.
11. **Di Wang**, Marco Gaboardi and Jinhui Xu. Empirical Risk Minimization in Non-interactive Local Differential Privacy Revisited. *Advances in Neural Information Processing Systems (NeurIPS 2018)*, Montreal, QC, Canada, December 03-08, 2018.
12. **Di Wang**, Mingwei Ye and Jinhui Xu. Differentially Private Empirical Risk Minimization Revisited: Faster and More General. *Advances in Neural Information Processing Systems (NeurIPS 2017)*, Long Beach, CA, USA, 4-9 December 2017.

PUBLICATIONS

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

Peer-Refereed Conference Papers

1. Youming Tao*, Yulian Wu*, Peng Zhao and **Di Wang**. Optimal Rates of (Locally) Differentially Private Heavy-tailed Multi-Armed Bandit. Submitted to *The 25th International Conference on Artificial Intelligence and Statistics (AISTATS 2022).*

2. Yunus Esencayi, Chenglin Fan, Di Wang, Marco Gaboardi, Vincent Cohen-Addad and Shi Li. On Facility Location Problem in the Local Differential Privacy Model. Submitted to *The 25th International Conference on Artificial Intelligence and Statistics (AISTATS 2022).*

3. Jinyan Su, Lijie Hu and **Di Wang**. Faster Rates of Differentially Private Stochastic Convex Optimization. *Submitted to The Conference on Algorithmic Learning Theory (ALT 2022).*

4. Lijie Hu, Shuo Ni, Hanshen Xiao and **Di Wang**. High Dimensional Differentially Private Heavy-tailed Stochastic Convex Optimization. *The 41st ACM Symposium on Principles of Database Systems (PODS 2022).*

5. Zhiyu Xue*, Shaoyang Yang*, Mengdi Huai and **Di Wang**. Differentially Private Pairwise Learning Revisited. *The 30th International Joint Conference on Artificial Intelligence (IJCAI 2021),* Montreal, Canada, August 21-26, 2021.

6. **Di Wang***, **Huanyu Zhang***, Marco Gaboardi and Jinhui Xu. Estimating Smooth GLMs in Non-interactive Local Differential Privacy Model with Public Unlabeled Data. *The 32nd International Conference on Algorithmic Learning Theory (ALT 2021),* Online, March 16-19, 2021.

7. Mengdi Huai, Chenglin Miao, Jinduo Liu, Di Wang, Jingyuan Chou, and Aidong Zhang. Global Interpretation for Pairwise Learning. *The IEEE International Conference on Bioinformatics and Biomedicine 2020 (BIBM 2020)*, Online, December 16-19, 2020. (**Selected as Regular Paper, Acceptance Rate: 19.4%**).

8. **Di Wang** and Jinhui Xu. Escaping Saddle Points of Empirical Risk Privately and Scalably via DP-Trust Region Method. *2020 European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Database (ECML-PKDD 2020),* Ghent, Belgium, September 14-18, 2020.

9. **Di Wang***, **Hanshen Xiao***, Srinivas Devadas and Jinhui Xu. On Differentially Private Stochastic Convex Optimization with Heavy-tailed Data. *The 37th International Conference on Machine Learning (ICML 2020)*, Vienna, Austria, July 12-18, 2020.

10. **Mengdi Huai***, **Di Wang***, Chenglin Miao, Jinhui Xu and Aidong Zhang. Pairwise Learning with Differential Privacy Guarantees. *The Thirty-Fourth AAAI Conference on Artificial Intelligence (AAAI 2020)*, New York, USA, February 7-12, 2020.

11. **Di Wang***, **Xiangyu Guo***, Chaowen Guan, Shi Li and Jinhui Xu. Scalable Estimating Stochastic Linear Combination of Non-linear Regressions. *The Thirty-Fourth AAAI Conference on Artificial Intelligence (AAAI 2020)*, New York, USA, February 7-12, 2020.

12. Mengdi Huai, Di Wang, Chenglin Miao and Aidong Zhang. Learning to Explain Pairwise Algorithms. *The Thirty-Fourth AAAI Conference on Artificial Intelligence (AAAI 2020)*, New York, USA, February 7-12, 2020.

13. Yunus Esencayi, Marco Gaboardi, Shi Li and **Di Wang**. Facility Location Problem in Differential Privacy Model Revisited. *Advances in Neural Information Processing Systems (NeurIPS 2019)*, Vancouver, BC, Canada, December 08-14, 2019. (**Authors are alphabetically ordered**)

14. Mengdi Huai, Di Wang, Chenglin Miao, Jinhui Xu and Aidong Zhang. Privacy-aware Synthesizing for Crowdsourced Data. *The Twenty-Eighth International Joint Conference on Artificial Intelligence (IJCAI 2019)*, August 10-16, 2019, Macao, China.

15. **Di Wang** and Jinhui Xu. Principal Component Analysis in the Local Differential Privacy Model. *The Twenty-Eighth International Joint Conference on Artificial Intelligence (IJCAI 2019)*, August 10-16, 2019, Macao, China.
16. **Di Wang** and Jinhui Xu. Lower Bound of Locally Differentially Private Sparse Covariance Matrix Estimation. *The Twenty-Eighth International Joint Conference on Artificial Intelligence (IJCAI 2019)*, August 10-16, 2019, Macao, China.
17. **Di Wang** and Jinhui Xu. On Sparse Linear Regression in the Local Differential Privacy Model. *The 36th International Conference on Machine Learning (ICML 2019)*, Long Beach, CA, USA, June 9-15, 2019. (**Selected as Long Talk, Acceptance Rate: 140/3424= 4.1%**)
18. **Di Wang**, Changyou Chen and Jinhui Xu. Differentially Private Empirical Risk Minimization with Non-convex Loss Functions. *The 36th International Conference on Machine Learning (ICML 2019)*, Long Beach, CA, USA, June 9-15, 2019.
19. **Di Wang**, Jinhui Xu and Yang He. Estimating Sparse Covariance Matrix Under Differential Privacy via Thresholding. *The 53rd Annual Conference on Information Sciences and Systems (CISS 2019)*, Baltimore, MD, USA, March 20-22 2019.
20. **Di Wang**, Adam Smith and Jinhui Xu. Noninteractive Locally Private Learning of Linear Models via Polynomial Approximations. *Algorithmic Learning Theory (ALT 2019)*, March 22-24, 2019, Chicago, IL, USA.
21. **Di Wang** and Jinhui Xu. Differentially Private Empirical Risk Minimization with Smooth Non-Convex Loss Functions: A Non-Stationary View. *The Thirty-Third AAAI Conference on Artificial Intelligence (AAAI 2019)*, Honolulu, Hawaii, USA, January 27-February 1, 2019. (**Selected as Oral Presentation, Acceptance Rate: 460/7095=6.5%**)
22. **Di Wang**, Marco Gaboardi and Jinhui Xu. Empirical Risk Minimization in Non-interactive Local Differential Privacy Revisited. *Advances in Neural Information Processing Systems (NeurIPS 2018)*, Montreal, QC, Canada, December 03-08, 2018.
23. **Di Wang**, Mengdi Huai and Jinhui Xu. Differentially Private Sparse Inverse Covariance Estimation. *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP 2018)*, Anaheim, California, USA, November 26-29, 2018.
24. **Di Wang** and Jinhui Xu. Large Scale Constrained Linear Regression Revisited: Faster Algorithms via Preconditioning. *The Thirty-Second AAAI Conference on Artificial Intelligence (AAAI 2018)*, New Orleans, Louisiana, USA, February 2-7, 2018. (**Selected as Oral Presentation, Acceptance Rate: 411/3800=10.8%**)
25. **Di Wang**, Mingwei Ye and Jinhui Xu. Differentially Private Empirical Risk Minimization Revisited: Faster and More General. *Advances in Neural Information Processing Systems (NIPS 2017)*, Long Beach, CA, USA, 4-9 December 2017.

Peer-Refereed Journal Papers

26. **Di Wang** and Jinhui Xu. Differentially Private High Dimensional Sparse Covariance Matrix Estimation. *Theoretical Computer Science,* Volume 865, 14 April 2021, Pages 119-130.
27. **Di Wang** and Jinhui Xu. Inferring Ground Truth for Crowdsourcing Data Under Local Attribute Differential Privacy. *Theoretical Computer Science,* Volume 865, 14 April 2021, Pages 85-98.
28. **Di Wang** and Jinhui Xu. Sparse Linear Regression in the Local Model of Differential Privacy. *IEEE Transactions on Information Theory*, Volume 67, No. 2, Pages 1182-1200, Feb. 2021.
29. **Di Wang***, **Xiangyu Guo***, Shi Li and Jinhui Xu. Robust High Dimensional Expectation Maximization Algorithm via Trimmed Hard Thresholding. *Machine Learning* 109, 2283-2311 (2020).
30. **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,* Volume 21, 200 (2020), Pages 1-39.

31. **Di Wang***, **Xiangyu Guo***, Chaowen Guan, Shi Li and Jinhui Xu. Estimating Stochastic Linear Combination of Non-linear Regressions Efficiently and Scalably. *Neurocomputing*, Volume 399, 25 July 2020, Pages 129-140.
32. **Di Wang** and Jinhui Xu. Tight Lower Bound of Sparse Covariance Matrix Estimation in the Local Differential Privacy Model. *Theoretical Computer Science,* Volume 815, 2 May 2020, Pages 47-59.
33. **Di Wang** and Jinhui Xu. Principal Component Analysis in Local Differential Privacy Model. *Theoretical Computer Science,* Volume 809, 24 February 2020, Pages 296-312.
34. **Di Wang** and Jinhui Xu. Faster Constrained Linear Regression via Two-step Preconditioning. *Neurocomputing,* Volume 364, 28 October 2019, Pages 280-296.

Hosted Visiting Scholar

1. Vaneet Aggarwal, Associate Professor at Purdue University, 07/2022-06/2023

Postdocs

1. Yan Hu, 12/2021-
2. Sultan J. Majeed, 08/2022-

Students

1. Lijie Hu (CS PhD) 01/2021-
2. Zihang Xiang (CS PhD) 01/2021-
3. Yulian Wu (CS PhD) 09/2021-
4. Chenglong Wang (CS PhD) 09/2021-
5. Xiaochuan Gou (CS PhD, Co-advised with Xiangliang Zhang), 09/2020-

Visiting Students/Research Intern

1. Zejun Xie (Undergraduate at Renmin University of China), 07/2020-08/2020. Current a PhD student in CS at **Rutgers University**.
2. Zhiyu Xue (Undergraduate at University of Electronic Science and Technology of China), 08/2020-10/2020. Current a PhD student in CS at **Michigan State University**.
3. Shaoyang Yang (Undergraduate at Harbin Institute of Technology), 08/2020-10/2020.
4. Xingyu Jiang (Undergraduate at Harbin Institute of Technology Weihai), 01/2021-05/2021
5. Shuo Ni (Master student at University of South California), 01/2021-08/2021
6. Junren Chen (Undergraduate at Sun Yat-Sen University), 05/2021-08/2021. Current a PhD student in Mathematics at **Hong Kong University**.
7. Mingyi Zhou (Master student at University of Electronic Science and Technology of China), 04/2021-08/2021
8. Danya Alnajar (Undergraduate at University at Jeddah), 06/2021-08/2021
9. Farah Albishri (Undergraduate at University at Jeddah), 06/2021-08/2021
10. Djidenou Hans Amos Montcho (Master student at University of São Paulo-Federal University of São Carlos), 09/2021-12/2021
11. Peng Zhao (PhD student at Nanjing University), 09/2021-03/2022
12. Xiangyu Guo (PhD student at University at Buffalo), 09/2021-03/2022

13. Tianhang Zheng (PhD student at University of Toronto), 10/2021-04/2022
14. Mengdi Huai (PhD student at University of Virginia), 10/2021-04/2022
15. Hanpu Shen (Undergraduate at Southern University of Science and Technology), 05/2021-
16. Yuan Qiu (Undergraduate at Sun Yat-Sen University), 09/20201-
17. Tao Yang (Undergraduate at Nankai University), 09/2021-
18. Binlan Wu (Master Student at Technical University of Munich), 09/2021-
19. Jinyan Su (Undergraduate at University of Electronic Science and Technology of China), 03/2021-12/2022.
20. Youming Tao (Undergraduate at Shandong University), 01/2021-. Current a Master student in CS at **Shandong University**.

TALKS

INVITED TALKS

1. STAT Graduate Seminar, KAUST, November 2021
2. Interdisciplinary Research Center of Intelligent Secure Systems, King Fahd University of Petroleum and Minerals, November 2021
3. AMCS/STAT Graduate Seminar, KAUST, September 2021
4. Vision And Learning SEminar, Online, June 2021
5. Computer Science Graduate Seminar, KAUST, April 2021
6. KAUST Conference on Artificial Intelligence, April 2021
7. School of Cyber Science and Technology, Zhejiang University, September 2020
8. School of Computing and Information Systems, University of Melbourne, April 2020
9. Department of Computer Science and Engineering, Chinese University of Hong Kong, April 2020
10. Department of Computer Science, Dalhousie University, April 2020
11. CISPA-Helmholtz Center for Information Security, April 2020
12. Department of Computing, Hong Kong Polytechnic University, April 2020
13. Department of Computer Science, University of Memphis, Apirl 2020
14. School of Computer Science, University of Sydney, April 2020
15. Department of Computing, Imperial College London, March 2020
16. King Abdullah University of Science and Technology, March 2020
17. Department of Computing and Software, McMaster University, March 2020
18. Department of Computer Science, City University of Hong Kong, March 2020
19. School of Information System, Singapore Management University, March 2020
20. Department of Computer Science, University College London, UK, March 2020
21. Department of Computer Science, University of Warwick, UK, March 2020
22. School of Computer Science, University of Birmingham, UK, March 2020
23. Department of Computer Science and Engineering, Hong Kong University of Science and Technology, February 2020
24. Department of Computer Science, McGill University, February 2020

25. Department of Computer Science, University of Surrey, UK, February 2020
26. Department of Computer Science, University of Science and Technology of China, November 2019
27. Department of Computer Science, Nanjing University, China, November 2019
28. Department of Computer Science, University of Alberta, November 2019

CONFERENCE TALKS

1. Differentially Private Pairwise Learning Revisited. IJCAI 2021, Onine.
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

- Organizer:
  - PAIR2Graph: Privacy, Accountability, Interpretability, Robustness, Reasoning on Graph-Structured Data (ICLR 2022)
- Senior Committee Member/Area Chair:
  - Thirty-Sixth AAAI Conference on Artificial Intelligence (AAAI 2022)
- Technical Program Committee Member:
  - *The 27th European Symposium on Research in Computer Security (ESORICS), 2022*
  - AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI 2022)

  - NeurIPS 2021 workshop on Privacy in Machine Learning (PriML 2021)
  - *The 26th European Symposium on Research in Computer Security (ESORICS), 2021* (Poster Session)
  - *AAAI Conference on Artificial Intelligence (AAAI), 2021*
  - *Winter Conference on Applications of Computer Vision (WACV 2020)*
  - *European Conference on Machine Learning (ECML-PKDD 2020)*
  - *The 29th International Joint Conference on Artificial Intelligence (IJCAI-PRICAI 2020)*
  - *IEEE Symposium on Security and Privacy 2020* (Shadow PC)
  - *AAAI Conference on Artificial Intelligence (AAAI), 2020*

- Reviewer (Journals)
  - *Journal of 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*
  - *Information Processing Letters*
  - *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*

- Reviewer (Conferences)
  - *The 39th International Conference on Machine Learning (ICML 2022)*
  - *The 25th International Conference on Artificial Intelligence and Statistics (AISTATS 2022)*
  - *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2022)*
  - *IEEE Winter Conference on Applications of Computer Vision (WACV 2022)*
  - *2022 International Conference on Learning Representations (ICLR 2022)*
  - *Neural Information Processing Systems (NeurIPS/NIPS) 2021*
  - *2021 IEEE International Symposium on Information Theory (ISIT 2021)*
  - *IEEE International Conference on Computer Vision (ICCV 2021)*
  - *The 38th International Conference on Machine Learning (ICML 2021)*
  - *The 24th International Conference on Artificial Intelligence and Statistics (AISTATS 2021)*
  - *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2021)*
  - *2021 International Conference on Learning Representations (ICLR 2021)*

- *The 15th Asian Conference on Computer Vision (ACCV 2020)*
- *IEEE Winter Conference on Applications of Computer Vision (WACV 2021)*
- *Neural Information Processing Systems (NeurIPS/NIPS) 2020*
- *The 16th Annual Conference on Theory and Applications of Models of Computation (TAMC 2020)*
- *The 36th International Symposium on Computational Geometry (SoCG 2020)*
- *European Conference on Computer Vision (ECCV 2020)*
- *The 52nd ACM Symposium on Theory of Computing (STOC 2020)*
- *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2020)*
- *Neural Information Processing Systems (NeurIPS/NIPS) 2019*
- *IEEE International Conference on Distributed Computing Systems (ICDCS 2019)*
- *IEEE International Conference on Computer Vision (ICCV 2019)*
- *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2019)*
- *International Conference on Machine Learning (ICML) 2019*
- *International Conference on Artificial Intelligence and Statistics (AISTATS) 2019*
- *AAAI Conference on Artificial Intelligence (AAAI) 2018*
- *ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD) 2018*
- *AAAI Conference on Artificial Intelligence (AAAI) 2017*
- *International Symposium CompIMAGE'18-Computational Modeling of Objects Presented in Images: Fundamentals, Methods, and Applications*
- *International Workshop on Combinatorial Image Analysis (IWCIA) 2017*

KAUST SERVICE

- **2021 KAUST Gifted Student Programs Convocation**, February 2021
  - Sci Café: Dynamic presentation to showcase an area of KAUSTs innovative research, AI & Cyber Security.
  - Faculty Mentoring Meetings: Meet one-on-one with junior and senior KGSP students to provide guidance and feedback on the students professional and academic development, areas of strengths and weakness, and recommendations for future activities.

ACADEMIC THESIS COMMITEE

Master Thesis

1. Committee member, Igor Sokolov, AMCS, February 2022.
   Thesis title: Distributed non-convex stochastic optimization with biased gradient estimators
   Advisor: Prof. Peter Richtarick

PhD Thesis

1. Committee member, Zhuo Yang, CS, March 2022
   Thesis title: Antidote or Poison: the Two Sides of Label Dependency in Multi-Label Learning
   Advisor: Prof. Xiangliang Zhang