Di Wang *Curriculum vitae*

CONTACT INFORMATION

State University of New York at Buffalo
Department of Computer Science and Engineering
338 Davis Hall
Buffalo, NY 14260-2500 USA

Work: +1-716-730-9826
E-mail: dwang45@buufalo.edu
Website:
www.acsu.buffalo.edu/dwang45/

RESEARCH INTERESTS

Private Data Analysis, Machine Learning and Algorithmic Fairness: differential privacy, private machine learning, privacy-preserving data mining, robust estimation, large scale/high dimension optimization, adversarial machine learning, fairness in machine learning

PROFESSIONAL EXPERIENCE

University of California at Berkekey, Berkeley, CA

Visiting Graduate Student **Spring 2019**

- Data Privacy: Foundations and Applications
- Simons Institute for the Theory of Computing

Harvard University, Cambridge, MA

Research Intern **June to September 2018**

- Harvard University Privacy Tools Project
- School of Engineering and Applied Science
  - Mentor: Professor Adam D. Smith

State University of New York at Buffalo, Buffalo, NY

Research Assistant **Fall 2018 to now**

- Department of Computer Science and Engineering
  - Mentor: Professor Jinhui Xu

Teaching Assistant **Fall 2015 to Fall 2018**

- Department of Computer Science and Engineering
  - Mentor: Professor Jinhui Xu

EDUCATION

State University of New York at Buffalo, Buffalo, NY, USA

Ph.D., Computer Science and Engineering, June 2020 (expected)

- Adviser: Professor Jinhui Xu

University of Western Ontario, London, ON, Canada

M.S., Mathematics, August 2015

Shandong University, Jinan, Shandong, China

B.S., Mathematics and Applied Mathematics, June 2014

SUBMITTED PAPERS

[1] **Mengdi Huai***, **Di Wang***, Chenglin Miao, Jinhui Xu and Aidong Zhang. Pairwise Learning with Differential Privacy Guarantees. (***equal contribution**).

[2] **Di Wang***, **Xiangyu Guo***, Shi Li and Jinhui Xu. Robust Estimation of High Dimensional Latent Variable Models via Trimmed EM Algorithm. (* **equal contribution**).

[3] **Yunus Esencayi***, **Marco Gaboardi*** , **Shi Li*** and **Di Wang***. Facility Location in the Differential Privacy Model Revisit. (* **alphabetical order**).

[4] **Di Wang***, **Huanyu Zhang***, Marco Gaboardi and Jinhui Xu. (***equal contribution**). Learning GLMs in Non-interative Local Differential Privacy Model with Public Unlabeled Data.

[5] Mengdi Huai, Chenglin Miao, Di Wang, Jinhui Xu and Aidong Zhang. Towards Interpretation of Pairwise Learning.

[6] **Di Wang***, **Mengdi Huai***, Chenglin Miao, Aidong Zhang and Jinhui Xu. (***equal contribution**). Inferring Ground Truth From Crowdcourcing Data Under Local Differential Privacy.

JOURNAL PUBLICATIONS

[7] **Di Wang** and Jinhui Xu. (Near) Optimal Principal Component Analysis in Locally Differential Privacy Model. *Submitted to Theoretical Computer Science*.
Short version has appeared in IJCAI 2019.

[8] **Di Wang** and Jinhui Xu. Lower Bound of Sparse Covariance Matrix Estimation in Local Differential Privacy Model. *Submitted to Theoretical Computer Science*.
Short version has appeared in IJCAI 2019.

[9] **Di Wang** and Jinhui Xu. On the Locally Differentially Private Sparse Linear Regession. *Submitted to IEEE Transactions on Information Theory.*
Short version has appeared in ICML 2019.

[10] **Di Wang** and Jinhui Xu. Differentially Private High Dimensional Sparse Covariance Matrix Estimation. *Submitted to Theoretical Computer Science*.
Short version has appeared in CISS 2019.

[11] **Di Wang** and Jinhui Xu. Gradient Complexity and Non-stationary Views of Differentially Private Empirical Risk Minimization. *Submitted to IEEE Transactions on Pattern Analysis and Machine Intelligence*.
Short versions have appeared in NIPS 2017 and AAAI 2019.

[12] **Di Wang**, Marco Gaboardi, Adam Smith and Jinhui Xu. On the Empirical Risk Minimization in the Non-interactive Local Differential Privacy Model *Submitted to Journal of Machine Learning Research.*
Short versions have appeared in NeurIPS 2018 and ALT 2019.

[13] **Di Wang** and Jinhui Xu. Faster Large Scale Linear Regression via a Two Step Preconditioning Method. *Submitted to Neurocomputing*.
Short version has appeared in AAAI 2018.

CONFERENCE PUBLICATIONS

[14] Mengdi Huai, Di Wang, Chenglin Miao, Jinhui Xu and Aidong Zhang. Privacy-aware Synthesizing for Crowdsourced Data. In *Twenty-Eighth International Joint Conference on Artificial Intelligence, IJCAI 2019, August 10-16 2019, Macao, China.* (Acceptance Rate: 850/4752= 17.9%)

[15] **Di Wang** and Jinhui Xu. Locally Differentially Private Principal Component Analysis. In *Twenty-Eighth International Joint Conference on Artificial Intelligence, IJCAI 2019, August 10-16 2019, Macao, China.* (Acceptance Rate: 850/4752= 17.9%)

[16] **Di Wang** and Jinhui Xu. Lower Bound of Differentially Private Sparse Covariance Matrix Estimation. In *Twenty-Eighth International Joint Conference on Artificial Intelligence, IJCAI 2019, August 10-16 2019, Macao, China.* (Acceptance Rate: 850/4752= 17.9%)

[17] **Di Wang** and Jinhui Xu. On the Locally Differentially Private Sparse Linear Regession. In: *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. In: *36th International Conference on Machine Learning, ICML 2019, Long Beach, CA, USA, June 9-15, 2019.* (Acceptance Rate: 773/3424= 22.5%)

[19] **Di Wang**, Jinhui Xu and Yang He. Estimating Sparse Covariance Matrix Under Differential Privacy via Thresholding. In: *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. Empirical Risk Minimization in Non-interactive Local Model via Polynomial of Inner Product Approximation. In: *Algorithmic Learning Theory, ALT 2019, 22-24 March 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. In: *Proceedings of 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 Under Non-interactive Locally Differential Privacy Revisited. In *Advances in Neural Information Processing Systems 31: Annual Conference on Neural Information Processing Systems 2018 (NeurIPS 2018), Montreal, QC, Canada, December 03-08, 2018. (Acceptance Rate: 1011/4856=20.8%).*

[23] **Di Wang**, Mengdi Huai and Jinhui Xu. Differentially Private Sparse Inverse Covariance Estimation. In: *2018 IEEE Global Conference on Signal and Information Processing, GlobalSIP 2018, Anaheim, California, USA, November 26-29, 2018*. **Selected as Oral Presentation**.

[24] **Di Wang** and Jinhui Xu. Large Scale Constrained Linear Regression Revisited: Faster Algorithms via Preconditioning. In: *Proceedings of 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**, Minwei Ye and Jinhui Xu. Differentially Private Empirical Risk Minimization Revisited: Faster and More General. In: *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017 (NIPS 2017), Long Beach, CA, USA, 4-9 December 2017*. (Acceptance Rate: 678/3240=20.9%).

WORKSHOP PAPERS

[26] **Di Wang**, Adam Smith and Jinhui Xu. High Dimensional Sparse Linear Regression under Local Differential Privacy: Power and Limitations. In: *NIPS Workshop on Privacy Preserving Machine Learning, 2018.*

TEACHING EXPERIENCE

State University of New York at Buffalo , Buffalo, NY

Instructor **Summer 2019**

- CSE574/474: Introduction to Machine Learning

Teaching Assistant **September 2015 to May 2018**

- CSE574/474: Introduction to Machine Learning
  - Spring 2018
- CSE531/431: Analysis of Algorithm
  - Fall 2017, Spring 2017, Fall 2016, Spring 2016

- CSE115: Introduction to Computer Science for Majors I
  - Fall 2015

University of Western Ontario , London, ON, Canada

Teaching Assistant **September 2014 to Auguest 2015**

- MATH 1229A: Methods of Matrix Algebra
  - Summer 2015 and Winter 2015
- MATH 1225B: Methods of Calculus
  - Fall 2014

AWARDS

- SEAS Dean's Graduate Achievement Award in 2019, SUNY at Buffalo
- CSE Best Graduate Research Award in 2018, SUNY at Buffalo
- ICML Travel Award, 2019
- NIPS Travel Award, 2018, 2017
- Western Graduate Research Scholarship, Western University, 2014-2015
- Algebraic Geometry Summer School Scholarship, ENCU, Shanghai, 2013

TALKS

- On the Locally Differentially Private Sparse Linear Regession. ICML 2019. Long Beach, CA, USA. June 2019.
- Estimation Sparse Covariance Matrix Under Differential Privacy via Thresholding. CISS 2019. Baltimore, MD, USA. March 2019.
- Empirical Risk Minimization in Non-interactive Local Model via Polynomial of Inner Product Approximation. 2019 ALT. Chicago, IL, USA. March 2019.
- Differentially Private Empirical Risk Minimization with Smooth Non-convex Loss Functions: A Non-stationary View. AAAI 2019. Honolulu, Hawaii, February, 2019.
- Differentially Private Sparse Inverse Covariance Estimation. 2018 IEEE GlobalSIP Signal Processing for Adversarial Machine Learning. November, 2018.
- Differentially Private Empirical Risk Minimization in the Non-interactive Local Model, Intern Presentation, Harvard University, June, 2018.
- Large Scale Constrained Linear Regression Revisited Faster Algorithms via Preconditioning, The Thirty-Second Conference on Artificial Intelligence (AAAI), February, 2018.
- Differentially Private Empirical Risk Minimization with Non-convex Loss Function, SUNY Buffalo CSE 50th Anniversary, University at Buffalo, September, 2017

PROFESSIONAL SERVICE

Review Service

- *ACM Computing Surveys*
- *Neural Information Processing Systems 2019 (NeurIPS 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*
- *IEEE Transactions on Information Forensics and Security*
- *IEEE Transactions on Pattern Analysis and Machine Intelligence*
- *Theoretical Computer Science*
- *Information Processing Letters*
- *ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD) 2018*
- *AAAI Conference on Artificial Intelligence (AAAI) 2017, 2018*
- *International Symposium CompIMAGE'18-Computational Modeling of Objects Presented in Images: Fundamentals, Methods, and Applications*
- *International Workshop on Combinatorial Image Analysis (IWCIA) 2017*