Xueru Zhang

CONTACT INFORMATION

595 Dreese Laboratories
2015 Neil Avenue
Columbus, OH 43210

Phone: +1 (734) 548-1967
E-mail: zhang.12807@osu.edu
Homepage: xueruzhang.github.io

APPOINTMENTS

The Ohio State University, Columbus, OH

- Assistant Professor, Department of Computer Science & Engineering *Since 09/2021*
- Faculty Affiliate, Translational Data Analytics Institute *Since 10/2021*

EDUCATION

University of Michigan, Ann Arbor, MI

- Ph.D. in Electrical Engineering and Computer Science *01/2017 - 08/2021*

  Advisor: Mingyan Liu
  Thesis: *Socially Responsible Machine Learning: On the Preservation of Individual Privacy and Fairness*
  Committee: Yiling Chen, Alfred Hero, Mingyan Liu, Atul Prakash, Aaron Roth
- M.Sc. in Electrical Engineering and Computer Science *09/2015 - 12/2016*

Beihang University (BUAA), Beijing, China

- B.Eng. in Electronic and Information Engineering *09/2011 - 06/2015*

RESEARCH INTERESTS

- Socially responsible machine learning (e.g., fairness, privacy, security, robustness, interpretability)
- Learning in uncertain and dynamic environments (e.g., strategic classification, out-of-distribution generalization)
- Distributed optimization (e.g., federated learning)
- AI for science (e.g., healthcare, earth sciences).

AWARDS

- **President's Research Excellence Accelerator Award**, OSU *2022, 2024*
- **ProQuest Distinguished Dissertation Award**, Finalist, University of Michigan *2021*
- **Caltech Young Investigators Forum**, Engineering and Applied Science, Caltech *2021*
- **Towner Prize for Outstanding Ph.D. Research**, Finalist, University of Michigan *2020*
- **S. Lipschitz, M. A. Host and A. O. Smith Awards**, Finalist, University of Michigan *2020*
- **EECS Rising Stars 2020**, University of California, Berkeley *2020*
- **Rackham Predoctoral Fellowship**, University of Michigan *2020*
- **ITA Graduation Day Invited Talk**, University of California, San Diego *2020*
- **Outstanding Graduate of Beijing (Top 5%)**, Beijing, China *2015*
- **First-Class Academic Scholarship**, BUAA, China *2012, 2013, 2014*
- **Merit Student of Beijing (1/295)**, Beijing, China *2014*
- **Baosteel Education Scholarship (1/3591)**, China *2013*
- **National Scholarship (Top 2%)**, China *2012*

CONFERENCE PUBLICATIONS

† indicates the students I advise; ∗ indicates equal contribution

1. Automating Data Annotation under Strategic Human Agents: Risks and Potential Solutions.
   T. Xie† and **X. Zhang**
   *In the 38th Conference on Neural Information Processing Systems **(NeurIPS)**, 2024.*
   Acceptance rate: 25.8%

2. Non-linear Welfare-Aware Strategic Learning.
   T. Xie† and **X. Zhang**
   *In the 7th AAAI/ACM Conference on AI, Ethics, and Society **(AIES)**, 2024*
   Acceptance rate: 31.8%

3. Algorithmic Decision-Making under Agents with Persistent Improvement.
   T. Xie†, X. Tan† and **X. Zhang**
   *In the 7th AAAI/ACM Conference on AI, Ethics, and Society **(AIES)**, 2024.* [**Oral presentation**]
   Acceptance rate: 31.8%

4. Privacy-Aware Randomized Quantization via Linear Programming.
   Z. Cai†, **X. Zhang** and M. Khalili
   *In the 40th Conference on Uncertainty in Artificial Intelligence **(UAI)**, 2024*
   Acceptance rate: 27%

5. Non-stationary Domain Generalization: Theory and Algorithm.
   T. Pham, **X. Zhang** and P. Zhang
   *In the 40th Conference on Uncertainty in Artificial Intelligence **(UAI)**, 2024*
   Acceptance rate: 27%

6. Performative Federated Learning: A Solution to Model-Dependent and Heterogeneous Distribution Shifts.
   K. Jin, T. Yin, Z. Chen, Z. Sun, **X. Zhang**, Y. Liu and M. Liu
   *In the 38th AAAI Conference on Artificial Intelligence **(AAAI)**, 2024.* [**Oral presentation**]
   Acceptance rate: 23.75%

7. Counterfactually Fair Representation.
   Z. Zuo†, M. Khalili and **X. Zhang**
   *In the 37th Conference on Neural Information Processing Systems **(NeurIPS)**, 2023.*
   Acceptance rate: 26.1%

8. Loss Balancing for Fair Supervised Learning.
   M. Khalili, **X. Zhang** and M. Abroshan
   *In the 40th International Conference on Machine Learning **(ICML)**, 2023.*
   Acceptance rate: 27.9%

9. Fairness and Accuracy under Domain Generalization.
   T. Pham, **X. Zhang**, P. Zhang
   *In the 11th International Conference on Learning Representations **(ICLR)**, 2023.*
   Acceptance rate: 31.8%

10. Fairness Interventions as (Dis)incentives for Strategic Manipulation.
    X. Zhang, M. Khalili, K. Jin, P. Naghizadeh and M. Liu
    *In the 39th International Conference on Machine Learning **(ICML)**, 2022.*
    Acceptance rate: 21.9%

11. Incentive Mechanisms for Strategic Classification and Regression Problems.
    K. Jin, **X. Zhang**, M. Khalili, P. Naghizadeh and M. Liu
    *In ACM Conference on Economics and Computation **(EC),** 2022.*
    Acceptance rate: 27%
    Contributed Talk in ICLR Workshop on Socially Responsible Machine Learning, 2022.

12. Fair Sequential Selection Using Supervised Learning Models.
    M. Khalili, **X. Zhang**, M. Abroshan
    *In the 35th Conference on Neural Information Processing Systems **(NeurIPS)**, 2021.*
    Acceptance rate: 26%

13. Cardiac Complication Risk Profiling for Cancer Survivors via Multi-View Multi-Task Learning.

T. Pham, C. Yin, L. Mehta, **X. Zhang**, and P. Zhang
*In the IEEE International Conference on Data Mining **(ICDM)**, regular paper, 2021.*
Acceptance rate: 9.9%

14. Improving Fairness and Privacy in Selection Problems.
M. Khalili, **X. Zhang**, M. Abroshan and S. Sojoudi
*In the 35th AAAI Conference on Artificial Intelligence **(AAAI)**, 2021.*
Acceptance rate: 21%

15. How Do Fair Decisions Fare in Long-Term Qualification?
X. Zhang*, R. Tu*, Y. Liu, M. Liu, H. Kjellström, K. Zhang and C. Zhang
*In the 34th Conference on Neural Information Processing Systems **(NeurIPS)**, 2020.*
Acceptance rate: 20%

16. A Robust Energy and Emissions Conscious Cruise Controller for Connected Vehicles with Privacy Considerations.
C. Huang, **X. Zhang**, R. Salehi, T. Ersal and A. Stefanopoulou
ASME Automotive and Transportation Systems **Best Paper Award Finalist**
*In 2020 American Control Conference **(ACC)**, 2020.*

17. Group Retention when Using Machine Learning in Sequential Decision Making: the Interplay between User Dynamics and Fairness.
X. Zhang*, M. Khalili*, C. Tekin and M. Liu
*In the 33rd Conference on Neural Information Processing Systems **(NeurIPS)**, 2019.*

18. Contract Design for Purchasing Private Data Using a Biased Differentially Private Algorithm.
M. Khalili*, **X. Zhang*** and M. Liu
*In the 14th Workshop on the Economics of Networks, Systems and Computation **(NetEcon)**, 2019.*

19. Incentivizing Effort in Interdependent Security Games Using Resource Pooling.
M. Khalili, **X. Zhang** and M. Liu
*In the 14th Workshop on the Economics of Networks, Systems and Computation **(NetEcon)**, 2019.*

20. Effective Premium Discrimination for Designing Cyber Insurance Policies with Rare Losses.
M. Khalili, **X. Zhang** and M. Liu
*In the 10th Conference on Decision and Game Theory for Security **(GameSec)**, 2019.*

21. Improving the Privacy and Accuracy of ADMM-based Distributed Algorithms.
X. Zhang, M. Khalili and M. Liu
*In the 35th International Conference on Machine Learning **(ICML)**, 2018.*

22. Recycled ADMM: Improve Privacy and Accuracy with Less Computation in Distributed Algorithms.
X. Zhang, M. Khalili and M. Liu
*In the 56th Annual Allerton Conference on Communication, Control, and Computing **(Allerton)**, 2018.*

23. Public Good Provision Games on Networks with Resource Pooling.
M. Khalili, **X. Zhang** and M. Liu
*In the International Conference on Network Games Control and Optimization **(NetGCoop)**, 2018.*

Journal Publications

1. Learning under Imitative Strategic Behavior with Unforeseeable Outcomes
T. Xie†, Z. Zuo†, M. Khalili and **X. Zhang**
*In Transactions on Machine Learning Research **(TMLR)**, 2024.*

2. Federated Learning with Reduced Information Leakage and Computation.
T. Yin*, X. Tan†,*, **X. Zhang***, M. Khalili and M. Liu
*In Transactions on Machine Learning Research **(TMLR)**, 2024.*

3. A Fair and Interpretable Network for Clinical Risk Prediction: A Regularized Multi-view Multi-task

Learning Approach.
T. Pham, C. Yin, L. Mehta, **X. Zhang**, P. Zhang
*In Knowledge and Information Systems **(KAIS)**, 2022.*

4. Differentially Private Real-Time Release of Sequential Data.
X. Zhang, M. Khalili and M. Liu
*In ACM Transactions on Privacy and Security **(TOPS)**, 2022.*

5. Designing Contracts for Trading Private and Heterogeneous Data Using a Biased Differentially Private Algorithm.
M. Khalili*, **X. Zhang*** and M. Liu
In IEEE Access, 2021.

6. Resource Pooling for Shared Fate: Incentivizing Effort in Interdependent Security Games through Cross-investments.
M. Khalili, **X. Zhang** and M. Liu
*In IEEE Transactions on Control of Network Systems **(TCNS)**, 2020.*

7. Recycled ADMM: Improving the Privacy and Accuracy of Distributed Algorithms.
X. Zhang, M. Khalili and M. Liu
*In IEEE Transactions on Information Forensics and Security **(TIFS)**, 2019.*

8. Predictive Cruise Control with Private Vehicle-to-Vehicle Communication for Improving Fuel Consumption and Emissions.
X. Zhang*, C. Huang*, M. Liu, A. Stefanopoulou and T. Ersal
In IEEE Communications Magazine, 2019.

9. Long-Term Impacts of Fair Machine Learning.
X. Zhang, M. Khalili and M. Liu
In Ergonomics in Design: The Quarterly of Human Factors Applications, 2019.

Book Chapters

1. Fairness in Learning-Based Sequential Decision Algorithms: A Survey.
X. Zhang and M. Liu
Springer Studies in Systems, Decision and Control, Handbook on RL and Control, 2021.

Grants

1. **(Lead PI)** NSF Safe Learning-Enabled Systems Program *09/2024 - 10/2027*
Long-Term Safety for Human-AI Ecosystem
with Dr. Yang Liu. Total award amount: $800,000. My share: $400,000

2. **(PI)** OSU President's Research Excellence Accelerator Award *07/2024 - 06/2025*
User-Aligned Fair Machine Learning for Automated Hiring
with Dr. Bingjie Liu. Total award amount: $50,000

3. **(PI)** Translational Data Analytics Institute (TDAI) Pilot Award *07/2024 - 06/2025*
Towards Fair Automated Hiring in Practice
with Dr. Kaifeng Jiang. Total award amount: $50,000

4. **(PI)** College of Engineering Strategic Research Initiative Grant *02/2024 - 01/2025*
Trustworthy Machine Learning in Dynamic Environments
with Dr. Mahdi Khalili and Dr. Aylin Yener. Total award amount: $100,000

5. **(PI)** Translational Data Analytics Institute (TDAI) Pilot Award *07/2023 - 06/2024*
Towards Trustworthy Machine Learning for Never-Before-Seen Illness
with Dr. Ping Zhang and Dr. Jeffrey Caterino. Total award amount: $50,000

6. **(Co-PI)** Translational Data Analytics Institute (TDAI) Pilot Award *07/2023 - 06/2024*
   Exploring Fairness Interventions in Diversity Hiring by Using Machine Learning Models
   with Dr. Kaifeng Jiang. Total award amount: $47,667
7. **(Co-PI)** Translational Data Analytics Institute (TDAI) Pilot Award *07/2023 - 06/2024*
   Interpretable Data-Driven Prediction of Droughts at a Seasonal-to-Subseasonal Time Scale
   with Dr. Yanlan Liu. Total award amount: $40,000
8. **(PI)** Cisco Research *01/2023 - 12/2023*
   Federated Learning with Edge Dynamics
   with Dr. Aylin Yener. Total award amount: $200,000
9. **(Lead PI)** NSF CISE Core Program *10/2022 - 09/2025*
   Long-Term Impact of Fair Machine Learning under Strategic Individual Behavior
   with Dr. Mohammad Mahdi Khalili. Total award amount: $600,000. My share: $346,500
10. **(PI)** Clinical and Translation Science (CCTS) Pilot Award *10/2022 - 09/2023*
    with Dr. Ping Zhang and Dr. Jeffrey Caterino and Dr. Laxmi Mehta
    Total award amount: $50,000
11. **(PI)** OSU President's Research Excellence Accelerator Award *07/2022 - 06/2023*
    Fair Machine Learning Adaptable to Deployment Environments in Healthcare
    with Dr. Ping Zhang and Dr. Jeffrey Caterino. Total award amount: $50,000

Teaching

Instructor, The Ohio State University
- CSE 3521: Survey of Artificial Intelligence I: Basic Techniques *Fall 2022*
- CSE 5523: Machine Learning and Statistical Pattern Recognition *Spring 2022, 2023, 2024*
- CSE 5539: Fairness in Machine Learning *Fall 2021, Spring 2024*

Guest Lecturer
- CSE 6521: Artificial Intelligence, The Ohio State University *Fall 2021*

Graduate Student Instructor, University of Michigan
- EECS 501: Probability and Random Processes *Winter 2020*

Mentoring

Ph.D. Students
- Xuwei Tan *2022-*
- Tian Xie *2022-*
- Zhiqun Zuo *2022-*
- Zhongteng Cai *2023-*
- Xiukun Wei *2024-*

M.Sc. Students
- Wenhan Zhou (Female) *2022-2024*
- Rahul Mukthineni *2022-2024*
  Thesis: Leveraging Microsoft Azure Cognitive Services to Unlock Insights from Free-Text Veterinary Medical Records

B.Sc. Students
- Pavan Rauch *2024*
- Zhao Liu *2024*
- Yixuan Huang *2023*
- Yunqing Qiu (Female) *2022*
- Yizhi Wang (Female) *2022*
- Chris Liu *2021*

Academic Services

Ph.D. Thesis Defense & Candidacy Exam Committee Member

- Yufeng Yang, CSE, OSU (Advisor: DeLiang Wang) *11/2024*
- Xinyu Zhou, CSE, OSU (Advisor: Raef Bassily) *10/2024*
- Tong Liang, CSE, OSU (Advisor: Jim Davis) *04/2024*
- Thai-Hoang Pham, CSE, OSU (Advisor: Ping Zhang) *04/2024*
- Yuntian He, CSE, OSU (Advisor: Srinivasan Parthasarathy) *12/2023*
- Tongxin Yin, ECE, Umich (Advisor: Mingyan Liu) *11/2023*
- Changchang Yin, CSE, OSU (Advisor: Ping Zhang) *11/2023*
- Ju-Seung Byun, CSE, OSU (Advisor: Andrew Perrault) *10/2023*
- Ruoqi Liu, CSE, OSU (Advisor: Ping Zhang) *04/2023*
- Michael Menart, CSE, OSU (Advisor: Raef Bassily) *04/2023*
- Yifan Yang, ISE, OSU (Advisor: Parinaz Naghizadeh) *11/2022*
- Tai-Yu Daniel Pan, CSE, OSU (Advisor: Wei-Lun Chao) *07/2022*
- Hong-You Chen, CSE, OSU (Advisor: Wei-Lun Chao) *07/2022*
- Tianchen Zhou, ECE, OSU (Advisor: Jia Liu) *04/2022*

Master Thesis Defense Committee Member

- Rahul Mukthineni, OSU *04/2024*

Undergraduate Thesis Defense Committee Member

- Ian Thompson, OSU (Advisor: Parinaz Naghizadeh) *04/2023*
- Daniel Szoke, OSU (Advisor: Aylin Yener) *04/2023*

Program Committee

- Workshop on Algorithmic Fairness through the Lens of Metrics and Evaluation *2024*
- IEEE Secure and Trustworthy Machine Learning (SaTML) *Since 2024*
- Transactions on Machine Learning Research (TMLR) *Since 2023*
- Midwest Machine Learning Symposium *2023*
- Frontiers in Big Data *Since 2022*
- International Conference on Artificial Intelligence and Statistics (AISTATS) *Since 2022*
- IEEE Journal on Selected Areas in Communications (JSAC) *Since 2022*
- Journal of Machine Learning Research (JMLR) *Since 2022*
- International Conference on Machine Learning (ICML) *Since 2021*
- AAAI Conference on Artificial Intelligence (AAAI) *Since 2021*
- International Conference on Learning Representations (ICLR) *Since 2021*
- IEEE Access *Since 2021*
- IET Intelligent Transport Systems *Since 2021*
- American Control Conference (ACC) *Since 2022*
- Conference on Decision and Game Theory for Security (GameSec) *Since 2021*
- IEEE Transaction on Information Forensics and Security (TIFS) *Since 2020*
- Conference on Neural Information Processing Systems (NeurIPS) *Since 2020*
- IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI) *Since 2019*
- Conference on Decision and Control (CDC) *Since 2019*

Session Chair/Leader

- **Roundtable lead:** NeurIPS 2023 Workshop on Algorithmic Fairness through the Lens of Time *12/2023*
- **Session chair:** Fairness and bias in ML and NLP session *07/2020*
  Women in Machine Learning (WiML) Workshop, ICML
- **Session chair:** People, AI, and Fairness, Physics and Machine Learning *02/2020*
  Information Theory and Applications (ITA) Workshop, UCSD

Workshop Organizer

- Workshop on Machine Learning under Strategic Behavior and Social Dynamics
  TDAI interdisciplinary research fall forum, The Ohio State University *11/2024*
- TDAI Foundations CoP Deep Learning Summer School, The Ohio State University *06/2022*
- Workshop on Socially Responsible Machine Learning
  International Conference on Learning Representations (ICLR) *04/2022*
  International Conference on Machine Learning (ICML) *07/2021*

Panelist

- ShowOHI/O Panel Discussion, Ohio State's Tech Entrepreneurship Showcase *04/2024*
- Session "Data Science and the Social and Behavioral Sciences," TDAI Fall Forum, OSU *11/2022*
- Faculty Panel Discussion, New Faculty Orientation, College of Engineering, OSU *08/2022*
- CogFest 2022, Center for Cognitive Brain Sciences, OSU *04/2022*

Guest Editor

- Special Issue: Game Theory for Cybersecurity and Privacy, *Games*

Others

- **Mentor**, VESSL AI student-faculty-industry meet up at NeurIPS 2023 *12/2023*
- **Judge**, OSU HackAI, OSU *02/2024*
- **Event Organizer**, CSE prospective student visit day, OSU *02/2023*
- **Ethics Circle Fellow**, OSU *2022*
- **Presenter**, AI Research Expo, OSU *11/2022*
- **Judge**, CSE graduate student poster competition, OSU *02/2022*
- **Judge**, poster session, TDAI Fall Forum, OSU *11/2021*
- **Mentee**, Drake Institute Faculty Foundation, Impact, Transformation (FIT) Program, OSU *2021*
- **Discussant**, *ECE Communications and Signal Processing Seminar*, University of Michigan *2020*
  - Enabling Fast and Robust Federated Learning
  - Connections between Online Learning and Differential Privacy

Invited Talks

How Do Models Fare when Retrained with Human Strategic Feedback?

- **Midwest Machine Learning Symposium** *04/2024*

Ethical Machine Learning under Social Dynamics

- **ShowOHI/O Keynote Speaker**

Tackling Exogenous and Endogenous Distribution Shifts in Machine Learning *02/2024*

- **ByteDance**

Strategic Classification with Random Manipulation Outcomes *05/2023*

- **Midwest Machine Learning Symposium**

Towards Ethical AI: Improving Model Fairness and Privacy in Online Marketing and Advertising *06/2022*

- **Walmart Global Tech**

Fair Machine Learning under Social Dynamics *03/2022*

- **AI Club**, OSU

Long-Term Impact of Fair Machine Learning *12/2021*

- **Machine Learning Symposium**, Computer Science Department, USC

Fair Machine Learning with Human in Feedback Loops *06/2021*

- **Caltech Young Investigators Forum**, Engineering and Applied Science, Caltech

Trustworthy Machine Learning: On the Preservation of Individual Privacy and Fairness *2021*

- Emory University, *Department of Computer Science*
- Ohio State University, *Department of Computer Science & Engineering*
- Purdue University, *School of Industrial Engineering*
- Purdue University, *Department of Computer Science*
- Pennsylvania State University, *College of Information Sciences & Technology*
- University of California, Santa Cruz, *Department of Computer Science & Engineering*
- University of Maryland, College Park, *Department of Electrical & Computer Engineering*
- University of Notre Dame, *Department of Computer Science & Engineering*
- Virginia Polytechnic Institute and State University, *Department of Computer Science*
- Washington University in St. Louis, *Department of Computer Science & Engineering*

Human-Centric Machine Learning: On the Preservation of Individual Privacy and Fairness *07/2020*

- Shanghai Jiao Tong University, China

Human-Centric Machine Learning *02/2020*

- **Graduation Day**, *Information Theory and Applications Workshop*, UCSD

Workshop and Poster

How Do Fair Decisions Fare in Long-Term Qualification?

- *Engineering Graduate Symposium (EGS)*, University of Michigan *02/2021*

- *NeurIPS Workshop*, Consequential Decision Making in Dynamic Environments *12/2020*
- *EECS Rising Stars Workshop*, UC Berkeley *11/2020*
- Conference on Neural Information Processing Systems (NeurIPS) *12/2020*

Group Retention when Using Machine Learning in Sequential Decision Making: the Interplay between User Dynamics and Fairness

- *ICML Workshop*, Women in Machine Learning (WiML) *07/2020*
- *Information Theory and Applications Workshop*, UCSD *02/2020*
- Conference on Neural Information Processing Systems (NeurIPS), Vancouver *12/2019*

Long Term Impact of Fair Machine Learning in Sequential Decision Making: Representation Disparity and Group Retention

- ACM conference on Economics and Computation (EC), Phoenix *06/2019*
- *EC Workshop*, Mechanism Design for Social Good (MD4SG), Phoenix *06/2019*

Using Resource Pooling to Obtain More Efficient Equilibrium in Interdependent Security Games

- ACM conference on Economics and Computation (EC), Phoenix *06/2019*

Improving the Privacy and Accuracy of ADMM-Based Distributed Algorithms

- International Conference on Machine Learning (ICML), Stockholm *07/2018*

Differential Privacy of ADMM-based Distributed Machine Learning Algorithms

- *Engineering Graduate Symposium (EGS)*, University of Michigan *11/2017*