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 *09/2021-*

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

- Societal Aspects of Artificial Intelligence (Privacy, Security, and Algorithmic Fairness)
- Machine Learning, Sequential Decision-Making, Distributed Optimization
- Economics, Game Theory

Awards

- **Caltech Young Investigators Forum**, Engineering and Applied Science, Caltech *2021*
- **Towner Prize for Outstanding Ph.D. Research**, Departmental Nominee *2020*
- **S. Lipschitz, M. A. Host and A. O. Smith Awards**, Departmental Nominee *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

1. 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.*

2. 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.*

3. 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.*

4. 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.*

5. 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.*

6. 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.*

7. 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.*

8. 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.*

9. 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.*

10. 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.*

11. 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.*

JOURNAL
PUBLICATIONS

12. 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.*

13. 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.

14. 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.

15. 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.*

16. 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.

BOOK
CHAPTERS

17. 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, 2020.

SUBMITTED PAPERS	18. Fairness Interventions as (Dis)incentives for Strategic Manipulation. **X. Zhang**, M. Khalili, K. Jin, P. Naghizadeh and M. Liu

18. Fairness Interventions as (Dis)incentives for Strategic Manipulation.
    X. Zhang, M. Khalili, K. Jin, P. Naghizadeh and M. Liu

19. Fair Online Selection Using Supervise Learning Models.
    M. Khalili and **X. Zhang**

20. Making Cheating Less Appealing: Incentivizing Honesty in Strategic Classification Problems.
    K. Jin, **X. Zhang** and M. Liu

21. Differentially Private Real-Time Release of Sequential Data.
    X. Zhang, M. Khalili and M. Liu
    (* indicates equal contribution)

TEACHING

Instructor, The Ohio State University
○ CSE 5539: Fairness in Machine Learning   *Fall 2021*

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

PROPOSAL WRITING

National Training Program of Innovation and Entrepreneurship   Beihang University
○ **Award number:** 201310006007   *2013 - 2014*
○ **Project:** *Intelligent Guidance System Based on Image Recognition and 3D Reconstruction*
  (Awarded 18,600 CNY by the Chinese Ministry of Education)

ACADEMIC SERVICES

Journal and Conference Reviewer
○ International Conference on Machine Learning (ICML)   *2021*
○ AAAI Conference on Artificial Intelligence (AAAI)   *2021*
○ International Conference on Learning Representations (ICLR)   *2021*
○ IEEE Access   *2021*
○ Conference on Decision and Game Theory for Security (GameSec)   *2021*
○ IEEE Transaction on Information Forensics and Security (TIFS)   *2020*
○ Conference on Neural Information Processing Systems (NeurIPS)   *2020, 2021*
○ IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)   *2019*
○ Conference on Decision and Control (CDC)   *2019, 2020*

Session Chair/Leader
○ **Session:** Fairness and bias in ML and NLP session   *07/2020*
  Women in Machine Learning (WiML) Un-Workshop, ICML
○ **Session:** People, AI, and Fairness, Physics and Machine Learning   *02/2020*
  Information Theory and Applications (ITA) Workshop, UCSD

Workshop Organizer
○ Workshop on Socially Responsible Machine Learning,   *07/2021*
  International Conference on Machine Learning (ICML)

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

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*

SKILLS   PYTHON, PYTORCH, TENSORFLOW, MATLAB, C/C++, HTML, CCS

REFERENCES   Available upon request.