Meisam Mohammady

Contact Information

Department of Computer Science
Iowa State University
https://www.cs.iastate.edu/people/meisam-mohammady/

Address: 232 Atanasoff-
-Hall, 2434 Osborn Dr
Ames, IA 50011
E-Mail:meisam@iastate.edu

Research Interests

Differential Privacy, Secure Federated Learning, Anonymity, Computational Learning Theory, Secure Multiparty Computation, Fairness

---

Education

Ph.D., Information Systems Engineering Concordia University, Montréal, Canada
Dissertation: *Novel Approaches to Preserving Utility in Privacy Enhanced Technologies* — Winner of the Distinguished Doctoral Dissertation Prize in Natural Science and Engineering
Advisors: Prof. Lingyu Wang, Prof. Yuan Hong

M.Sc., Electrical & Computer Engineering Polytechnique Montréal, Canada
Thesis: *Differentially Private Event Stream Filtering for Traffic Estimation*
Advisor: Prof. Jerome Le Ny

B.Sc., Electrical & Computer Engineering Sharif University of Technology, Iran
Thesis: *Backstepping Control of Four-Wheel Mobile Robots*
Advisor: Prof. Mehrzad Namvar

Professional Experience

Assistant Professor Oct. 2022 – Present
Department of Computer Science, Iowa State University, Ames, IA, USA

Research Scientist Oct. 2020 – Oct. 2022
Data61, CSIRO, Sydney, Australia

Research Funding

G.1. *NSF CISE PDaSP Track 2: Holistic Privacy-Preserving Collaborative Data Sharing for Intelligent Transportation*, NSF #2452747, co-PI (ISU PI), $1.2M total ($250K ISU share), Oct 2025–Oct 2028.
Lead PI: Yuan Hong (UConn); Co-PIs: Xuegang Ban (UW), Binghui Wang (IIT).

REFEREED PUBLICATIONS

[1] Qin Yang, Nicholas Stout, **Meisam Mohammady (Corresponding author)**, Han Wang, Ayesha Samreen, Christopher J Quinn, Yan Yan, Ashish Kundu, Yuan Hong. *PLRV-O: Advancing Differentially Private Deep Learning via Privacy Loss Random Variable Optimization.* **In Proceedings of the 2025 ACM Conference on Computer and Communications Security (CCS '25).** *Acceptance rate: TBD.*

[2] Thirasara Ariyarathna, Salil Kanhere, Hye-Young (Helen) Paik, **Meisam Mohammady**. *FedSIG: Privacy-Preserving Federated Recommendation via Synthetic Interaction Generation.* In Proceedings of the 28th International Symposium on Research in Attacks, Intrusions and Defenses (RAID '25). *Acceptance rate: TBD.*

[3] M.A.P. Chamikara, Seung Ick Jang, Ian Oppermann, Dongxi Liu, Musotto Roberto, Sushmita Ruj, Arindam Pal, **Meisam Mohammady**, Seyit Camtepe, Sylvia Young,

Chris Dorrian, Nasir David. *Towards Usability of Data with Privacy: A Unified Framework for Privacy-Preserving Data Sharing with High Utility.* In Proceedings of the 20th ACM Asia Conference on Computer and Communications Security (ASIACCS '25). *Acceptance rate: TBD.*

[4] Shuya Feng, **Meisam Mohammady**, Hanbin Hong, Shenao Yan, Ashish Kundu, Binghui Wang, Yuan Hong. *Harmonizing Differential Privacy Mechanisms for Federated Learning: Boosting Accuracy and Convergence.* In Proceedings of the Fifteenth ACM Conference on Data and Application Security and Privacy (CODASPY '25). *Acceptance rate: TBD.*

[5] Gnanakumar Thedchanamoorthy, Michael Bewong, **Meisam Mohammady**, Tanveer Zia, Md Zahidul Islam. *UD-LDP: A Technique for Optimally Catalyzing User Driven Local Differential Privacy.* Future Generation Computer Systems (FGCS'25). *Impact Factor: 7.187.*

[6] Mengyuan Zhang, Yosr Jarraya, Makan Pourzandi, **Meisam Mohammady**, Shangyu Xie, Yuan Hong, Lingyu Wang, Mourad Debbabi. *Utility Optimized Differential Privacy System.* U.S. Patent No. 12321478.

[7] Shuya Feng*, **Meisam Mohammady***, Han Wang, Xiaochen Li, Zhan Qin, Yuan Hong. *DPI: Ensuring Strict Differential Privacy for Infinite Data Streaming.* The 45th IEEE Symposium on Security and Privacy (S&P' 24). *Acceptance rate: 202/1389* $\sim$ 14.5%. *Equal Contribution (Co-First Authors).

[8] Gnanakumar Thedchanamoorthy, Michael Bewong, **Meisam Mohammady**, Tanveer Zia, Md Zahidul Islam. *FUD-LDP: Fully User Driven Local Differential Privacy.* In Proceedings of the International Conference on Web Information Systems Engineering (WISE'24). *Acceptance rate: TBD.*

[9] Thirasara Ariyarathna, **Meisam Mohammady**, Hye-Young (Helen) Paik, Salil S. Kanhere. *VLIA: Navigating Shadows with Proximity for Highly Accurate Visited Location Inference Attack against Federated Recommendation Models.* The 19th ACM ASIA Conference on Computer and Communications Security (ASIACCS'24). *Acceptance rate: 55/284* $\sim$ 19%.

[10] Thirasara Ariyarathna, **Meisam Mohammady**, Hye-Young (Helen) Paik, Salil S. Kanhere. *DeepSneak: User GPS Trajectory Reconstruction from Federated Route Recommendation Models.* ACM Transactions on Intelligent Systems and Technology (ACM TIST'24). *Impact Factor: 10.489.*

[11] Kane Walter, **Meisam Mohammady**, Surya Nepal, Salil S. Kanhere. *Mitigating Distributed Backdoor Attack in Federated Learning Through Mode Connectivity.* The 19th ACM ASIA Conference on Computer and Communications Security (ASIACCS'24). *Acceptance rate: 55/284* $\sim$ 19%.

[12] G. Thedchanamoorthy, M. Bewong, **M. Mohammady**, T. A. Zia, M. Z. Islam. *Optimization of UD-LDP with Statistical Prior Knowledge.* The 22nd International Conference on Pervasive Computing and Communications (PerCom 2024). *Acceptance rate: TBD.*

[13] Kane Walter, **Meisam Mohammady**, Surya Nepal, Salil S. Kanhere. *Optimally Mitigating Backdoor Attacks in Federated Learning.* IEEE Transactions on Dependable and Secure Computing (TDSC'23). *Impact Factor: 7.3.*

[14] **Meisam Mohammady**, Reza Arablouei. *Efficient Privacy-Preserved Processing of Multimodal Data for Vehicular Traffic Analysis.* The 2023 Symposium on Vehicles Security and Privacy (VehicleSec'23). *Acceptance rate: TBD.*

[15] **Meisam Mohammady**, Momen Oqaily, Lingyu Wang, Yuan Hong, Habib Louafi, Makan Pourzandi, Mourad Debbabi. *A Multi-view Approach to Preserve Both Privacy and Utility in Network Trace Anonymization.* ACM Transactions on Privacy and Security (TOPS), 2020. *Impact Factor: 3.2.*

[16] Shangyu Xie, **Meisam Mohammady**, Han Wang, Yuan Hong, Lingyu Wang, Jaideep Vaidya. *Generalizing Prefix-Preserving Data Outsourcing: Ensuring both Privacy and Utility.* IEEE Transactions on Knowledge and Data Engineering (TKDE), 2020. *Impact Factor: 8.881.*

[17] **Meisam Mohammady**, Shangyu Xie, Yuan Hong, Mengyuan Zhang, Lingyu Wang, Makan Pourzandi, Mourad Debbabi. *R^2DP: A Universal and Automated Approach to Optimizing the Randomization Mechanisms of Differential Privacy.* ACM CCS'20. *Acceptance rate: 11%.*

[18] Momen Oqaily, Yosr Jarraya, **Meisam Mohammady**, Suryadipta Majumdar, Lingyu Wang, Makan Pourzandi, Mourad Debbabi. *SegGuard: Protecting Audit Data Using Segmentation-based Anonymization for Multi-tenant Cloud Auditing.* IEEE TDSC, 2019. *Impact Factor: 6.864.*

[19] Bingyu Liu, Shangyu Xie, Han Wang, Yuan Hong, Xuegang Ban, **Meisam Mohammady**. *VTDP: Privately Sanitizing Fine-grained Vehicle Trajectory Data with Boosted Utility.* IEEE TDSC, 2019. *Impact Factor: 6.864.*

[20] Suryadipta Majumdar, Azadeh Tabiban, **Meisam Mohammady**, Alaa Oqaily, Yosr Jarraya, Makan Pourzandi, Lingyu Wang, Mourad Debbabi. *Proactivizer: Transforming Existing Verification Tools into Efficient Solutions for Runtime Security Enforcement.* In Proceedings of ESORICS'19. *Acceptance rate: 19.5%.*

[21] Suryadipta Majumdar, Azadeh Tabiban, **Meisam Mohammady**, Alaa Oqaily, Yosr Jarraya, Makan Pourzandi, Lingyu Wang, Mourad Debbabi. *Multi-Level Proactive Security Auditing for Clouds.* In Proceedings of the 2019 IEEE DSC.

[22] **Meisam Mohammady**, Lingyu Wang, Yuan Hong, Habib Louafi, Makan Pourzandi, Mourad Debbabi. *Preserving Both Privacy and Utility in Network Trace Anonymization.* In Proceedings of ACM CCS'18. *Acceptance rate: 16.5%.*

[23] Jerome Le Ny, **Meisam Mohammady**. *Differentially Private MIMO Filtering for Event Streams.* IEEE Transactions on Automatic Control, 2018. *Impact Factor: 5.625.*

[24] Jerome Le Ny, **Meisam Mohammady**. *Differentially Private MIMO Filtering for Event Streams and Spatio-temporal Monitoring.* In Proceedings of CDC'14. *H-index: 118.*

Patents

[1] **Meisam Mohammady**, Han Wang, Yuan Hong, Mengyuan Zhang, Suryaipta Majumdar, Lingyu Wang, Makan Pourzandi and Mourad Debbabi. *Dpod: differentially private outsourcing of anomaly detection.* US Patent App. 18/005,761, 2023.

[2] Mengyuan Zhang, Yosr Jarraya, Makan Pourzandi, **Meisam Mohammady**, XIE Shangyu, Yuan Hong, Lingyu Wang, Mourad Debbabi. *Utility optimized differential privacy system.* US Patent App. 17/610,795, 2022.

[3] **Meisam Mohammady**, Yosr Jarraya, Lingyu Wang, Mourad Debbabi and Makan Pourzandi. *Partition-based prefix preserving anonymization approach for network traces containing ip addresses.* US Patent 11,316,831, 2022.

Supervision

Current Students

[1] Gnanakumar Thedchanamoorthy (PhD, Co-advised)

[2] Nicholas Stout (PhD)

[3] Ayesha Samreen (PhD)

[4] Qin Yang (PhD, Co-advised)

Former Students

[1] Thirasara Ariyaratna (PhD)

[2] Kane Walter (PhD)

[3] Md. Rayhanul Islam (PhD)

[4] Daniel A. Asante (PhD)

[5] Mehedi Hassan (PhD)

[6] Hrishi Masurkar (BS)

[7] Fardeen Shaikh (MSc)

[8] Paige Rolling (BS)

Invited Talks

[1] "Preserving Both Privacy and Utility in Network Trace Anonymization", Université du Québec à Montréal (UQAM), Montréal, Canada, November 22, 2019

[2] "R^{2}DP: A Universal Approach to Optimizing the Randomization Mechanisms of Differential Privacy for Utility Metrics with No Known Optimal Distributions", Université du Québec à Montréal (UQAM), Montréal, Canada, November 22, 2019

[3] "DP-IDS: Differentially Private Intrusion Detection System ", Security, Privacy and Forensics (SPF) seminars, Montréal, Canada, May 10, 2019

[4] "R^{2}DP: A Universal Approach to Optimizing the Randomization Mechanisms of Differential Privacy for Utility Metrics with No Known Optimal Distributions", The CSIRO, Data61 Reading seminar, Sydney, Australia, November 22, 2020

[5] Novel Approaches to Preserving Utility in Privacy Enhancing Technologies, Discovery Partners Institute (DPI) R&D Seminar, Chicago, IL, USA, September 9, 2021

Demonstrations

[1] "Preserving Both Privacy and Utility in Network Trace Anonymization", *Ericsson Research Canada*, Montréal, Canada, May 2018

[2] "R^{2}DP: A Universal and Automated Approach to Optimizing the Randomization Mechanisms of Differential Privacy for Utility Metrics with No Known Optimal Distributions", *Ericsson Research Canada*, Montréal, Canada, October 2019

[3] "DPOAD: Differentially Private Outsourcing of Anomaly Detection with Optimal Sensitivity Learning", *Ericsson Research Canada*, Canada, October 2020

Awards

[1] Our data privacy tool *Personal Information Factor (PIF)* were awarded merit winner in the Technology Platform Solution category at the *iAwards*, the Australia's longest running innovation recognition program 2022

[2] Winner of the Best PhD Dissertation Awards (among all engineering and national science majors), Concordia University 2020

Professional Activities

Program Committee Member

- ACM Conference on Computer and Communications Security (CCS'23, '24, '25, '26)
- Privacy Enhancing Technologies Symposium / PoPETs (PoPETs'21, '22, '24, '25)
- IEEE Conference on Secure and Trustworthy Machine Learning (SaTML'25, '26)
- AAAI Conference on Artificial Intelligence (AAAI'22)
- IEEE Transactions on Dependable and Secure Computing (TDSC'19–'21)

Publicity Chair

- Privacy Enhancing Technologies Symposium (PETS'21–'22)
- CRC Security Automation and Orchestration Seminar Series (2021)

Journal Reviewer

- IEEE Transactions on Information Forensics and Security (TIFS)
- IEEE Transactions on Automatic Control
- Information Systems Research (ISR), INFORMS
- IEEE Transactions on Parallel and Distributed Systems (TPDS)
- Journal of Computer Security (JCS)

Conference Reviewer

- IEEE INFOCOM, IEEE ICDE, IEEE ICDCS, ESORICS, ACNS

Professional Memberships

- Association for Computing Machinery (ACM)
- Institute of Electrical and Electronics Engineers (IEEE)

Teaching

COM S 3520: Introduction to Operating Systems Spring 2024, Fall 2025
COM S 4530: Privacy-Preserving Algorithms and Data Security Spring 2023, Fall 2023, Fall 2024

Reference

Dr. Yuan Hong, Associate Professor, School of Computing University of Connecticut
`yuan.hong@uconn.edu`

Dr. Lingyu Wang, Professor, School of Engineering, The University of British Columbia
`lingyu.wang@ubc.ca`