Jaewoo Lee

Department of Computer Science
University of Georgia
620 Boyd Graduate Studies Research Center
Athens, GA 30602

Phone: (706) 542-8241
Email: jaewoo.lee@uga.edu
Homepage: http://cobweb.cs.uga.edu/~jwlee

Research Interests

Data privacy, Machine learning, optimization algorithms, and Cybersecurity

Education

Pennsylvania State Univeristy — University Park, PA

- Postdoctoral research associate — 2014-2016

Purdue University — West Lafayette, IN

- Ph.D. in Computer Science, 2014
- Advisor: Professor Chris Clifton
- Dissertation: Achieving Practical Differential Privacy

Yonsei University — Seoul, Korea

- M.S. in Computer Science, 2008
- Thesis: Efficiently Tracing Clusters over High-dimensional Data Streams

Yonsei University — Seoul, Korea

- B.E. in Computer Science, 2006

Research & Professional Experience

Aug. 2023 — Present	**University of Georgia** *Associate Professor*
Nov. 2018 — Present	**Institute of Cybersecurity and Privacy at UGA** *Member*
Feb. 2017 — Present	**Artificial Intelligence Institute at UGA** *Faculty affiliate*
Aug. 2016 — Present	**Georgia Informatics Institute at UGA** *Member*
Aug. 2016 — Jul. 2023	**University of Georgia** *Assistant Professor*
Sep. 2014 — Jul. 2016	**Penn State University**

	Postdoctoral Research Associate
Sep. 2013 — Jan. 2014	**NEC Laboratories America, Inc.** *Research Intern*
Sep. 2009 — Jul. 2014	**Indiana Center for Database Systems at Purdue** *Research Assistant & Teaching Assistant*
Mar. 2010 — Aug. 2011	**Rosen Center for Advanced Computing at Purdue** *Graduate Student Programmer*
Sep. 2008 — Aug. 2009	**Software Application Research Institute at Yonsei** *Researcher*
Sep. 2006 — Aug. 2008	**Database Laboratory at Yonsei** *Research Assistant & Teaching Assistant*
Mar. 2002 — Feb. 2005	**Gallup Research Korea** *Programmer*

Grants Received

External Grants

- CAREER: Robust Adaptive Optimization Algorithms for Differentially Private Learning, National Science Foundation, Amount: $529,560 (USD), 2020/3/9 - 2025/2/28, Principal Investigator
- Differentially Private Synthetic Data Generation, Samsung SDS, Amount: $50,000 (USD), 2020/11/1 - 2021/07/31, Principal Investigator
- Innovation Corps (i-Corps), NSF: Deep ground penentrating radar, $3,000 for travel, Co-Investigator

Internal Grants

- Faculty Research Grants, University of Georgia: Differentially Private Deep sum-product network, $9,829, 7/1/2017 - 6/30/2018, Principal Investigator
- Secure and Privacy-Sensitive Data Science for Enabling Resilient Communities, Office of the Vice President for Research in partnership with the Office of the Provost PRE-SEED, University of Georgia, $5,500, 2020, Co-Investigator
- Addiction Prevention, Office of the Vice President for Research in partnership with the Office of the Provost PRE-SEED, University of Georgia, $3,000, 2019, Co-Investigator

Publications

- Soham Sajekar, Sanika Katekar, and **Jaewoo Lee**. Diffusion Augmented Flows: Combining Normalizing Flows and Diffusion Models for Accurate Latent Space Mapping. In *Future of Information and Communication Conference (FICC) 2024*, FICC, 2024

- Juyeon Seo, **Jaewoo Lee**, Juhyun Lee, and Hyunsuk Ko. Deep compression network for enhancing numerical reconstruction quality of full-complex holograms. *Opt. Express*, 31(15):24573–24597, Jul 2023
- Yongrok Kim, Won Shin, **Jaewoo Lee**, Kwan-Jung Oh, and Hyunsuk Ko. Performance analysis of versatile video coding for encoding phase-only hologram videos. *Opt. Express*, 31(23):38854–38877, Nov 2023
- Michael Chassé, Louis Mullie, Philippe Després, Vincent Ferretti, Jessica Kissinger, **Jaewoo Lee**, Wenzhan Song, Peter Zinterhof, Christian Wachinger, and Bjoern Eskofier. Federated Learning and Analysis for Collaborative Research in Healthcare at a National and International Scale, December 2023. Published Online
- **Jaewoo Lee**. MBAG: A Scalable Mini-Block Adaptive Gradient Method for Deep Neural Networks. In *2022 IEEE International Conference on Big Data (Big Data)*, 2022
- **Jaewoo Lee**, Minjung Kim, Yonghyun Jeong, and Youngmin Ro. Differentially Private Normalizing Flows for Synthetic Tabular Data Generation. In *Proceedings of the AAAI Conference on Artificial Intelligence*, AAAI, 2022
- Shivani Arbat, Vinod Jayakumar, **Jaewoo Lee**, Wei Wang, and In Kee Kim. Wasserstein Adversarial Transformer for Cloud Workload Prediction. In *Proceedings of the 34th Annual Conference on Innovative Applications of Artificial Intelligence*, IAAI, 2022
- Seung Woo Kwak, Jeongyoun Ahn, **Jaewoo Lee**, and Cheolwoo Park. Differentially Private Goodness-of-Fit Tests for Continuous Variables. *Econometrics and Statistics*, 2021
- Sen He, Tianyi Liu, Palden Lama, **Jaewoo Lee**, In Kee Kim, and Wei Wang. Performance Testing for Cloud Computing with Dependent Data Bootstrapping. In *The 36th IEEE/ACM International Conference on Automated Software Engineering*, 2021
- Amanda Giordano, Lindsay Lundeen, Kelly Wester, **Jaewoo Lee**, Samuel Vickers, Michael Schmit, and In Kee Kim. Nonsuicidal self-injury on Instagram: Examining hashtag trends. *International Journal for the Advancement of Counselling*, 2021
- **Jaewoo Lee** and Daniel Kifer. Scaling up Differentially Private Deep Learning with Fast Per-example Gradient Clipping. *Proceedings on Privacy Enhancing Technologies*, 2021(1), 2021
- Chen Chen and **Jaewoo Lee**. Stochastic Adaptive Line Search for Differentially Private Optimization. In *IEEE International Conference on Big Data (Big Data)*, 2020 (**Acceptance rate for regular papers: 15.5%**)
- Daniele Ucci, Roberto Perdisci, **Jaewoo Lee**, and Mustaque Ahamad. Towards a Practical Differentially Private Collaborative Phone Blacklisting System. In *Proceedings of the 36th Annual Computer Security Applications Conference*, ACSAC '20, New York, NY, USA, 2020. Association for Computing Machinery

- Chen Chen and **Jaewoo Lee**. Renyi Differentially Private ADMM for Non-Smooth Regularized Optimization. In *Proceedings of the 10th ACM Conference on Data and Application Security and Privacy*, CODASPY, 2020
- Vinodh K. Jayakumar, **Jaewoo Lee**, In Kee Kim, and Wei Wang. A Self-Optimized Generic Workload Prediction Framework for Cloud Computing. In *Proceedings of the 34th IEEE International Parallel and Distributed Processing Symposium*, IPDPS, 2020
- Jaewoo Lee and Daniel Kifer. Differentially private deep learning with direct feedback alignment. *CoRR*, abs/2010.03701, 2020
- Lei Xian, Samuel D. Vickers, Amanda L. Giordano, **Jaewoo Lee**, In Kee Kim, and Lakshmish Ramaswamy. #Selfharm on Instagram: Quantitative Analysis and Classification of Non-Suicidal Self-Injury. In *Proceedings of 2019 IEEE International Conference on Cognitive Machine Intelligence*, CogMI, 2019
- Chen Chen, **Jaewoo Lee**, and Daniel Kifer. Renyi Differentially Private ERM for Smooth Objectives. In *Proceedings of the 22nd International Conference on Artificial Intelligence and Statistics*, **AISTATS**, 2019 (**Oral presentation**)
- Yue Wang, Daniel Kifer, and **Jaewoo Lee**. Differentially Private Confidence Intervals for Empirical Risk Minimization. *Journal of Privacy and Confidentiality*, 9(1), 2019
- Yue Wang, Daniel Kifer, **Jaewoo Lee**, and Vishesh Karwa. Statistical Approximating Distributions Under Differential Privacy. *Journal of Privacy and Confidentiality*, 8(1), 2018
- **Jaewoo Lee** and Daniel Kifer. Concentrated Differentially Private Gradient Descent with Adaptive per-Iteration Privacy Budget. In *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, **KDD**, 2018 (**Acceptance rate: 10.8 %**)
- **Jaewoo Lee**. Differentially Private Variance Reduced Gradient. In *Proceedings of the International Conference on New Trends in Computing Sciences*, ICTCS, 2017
- **Jaewoo Lee** and Daniel Kifer. Postprocessing for Iterative Differentially Private Algorithms. In *ICML 2016 Workshop on Theory and Practice of Differential Privacy*, ICML, 2016 (poster)
- Yue Wang, **Jaewoo Lee**, and Daniel Kifer. Differentially Private Hypothesis Testing, Revisited. *ArXiv e-prints*, November 2015
- **Jaewoo Lee**, Yue Wang, and Daniel Kifer. Maximum Likelihood Postprocessing for Differential Privacy under Consistency Constraints. In *Proceedings of the 21st ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, **KDD**, 2015 (**Acceptance rate: 19.4 %**)
- **Jaewoo Lee** and Chris Clifton. Top-k Frequent Itemsets via Differentially Private FP-trees. In *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, **KDD**, 2014 (**Acceptance rate: 14.6 %**)

- Rajesh Kalyanam, Lan Zhao, Carol X. Song, Yuet Ling Wong, **Jaewoo Lee**, and Nelson B. Villoria. iData: A Community Geospatial Data Sharing Environment to Support Data-driven Science. In *Proceedings of the Conference on Extreme Science and Engineering Discovery Environment: Gateway to Discovery*, XSEDE, 2013
- **Jaewoo Lee** and Chris Clifton. Differential identifiability. In *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining*, **KDD**, 2012 (**Acceptance rate: 17.6 %**)
- **Jaewoo Lee** and Chris Clifton. How much is enough? Choosing ϵ for Differential Privacy. In *Information Security*, volume 7001 of *LNCS*, pages 325–340. Springer Berlin / Heidelberg, 2011
- Hazem Elmeleegy, Ahmed Elmagarmid, and **Jaewoo Lee**. Leveraging Query Logs for Schema Mapping Generation in U-MAP. In *Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data*, **SIGMOD**, 2011
- Hazem Elmeleegy, **Jaewoo Lee**, El Kindi Rezig, Mourad Ouzzani, and Ahmed Elmagarmid. U-MAP: A System for Usage-based Schema Matching and Mapping. In *Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data*, **SIGMOD**, 2011 (demo)
- **Jae Woo Lee**, Nam Hun Park, and Won Suk Lee. Efficiently Tracing Clusters over High-dimensional On-line Data Streams. ***Data Knowledge & Engineering***, 68(3):362–379, March 2009
- **Jae Woo Lee** and Won Suk Lee. A Coarse-grain Grid-based Subspace Clustering Method for Online Multi-dimensional Data Streams. In *Proceedings of the 17th ACM Conference on Information and Knowledge Management*, **CIKM**, 2008

Presentations & Posters

Taming Large-scale Generative Models for Differential Privacy, Google Techtalk, Nov. 2023 (Virtual)

Privacy Concerns in an AI-driven World: challenges and solutions, Changbal Tech summit 2023, Seattle, WA

MBAG: MBAG: A Scalable Mini-Block Adaptive Gradient Method for Deep Neural Networks, IEEE BigDATA 2022, Osaka, Japan

Robust and Adaptive Optimization with Differential Privacy, Argonne National Research Laboratory 2022, Lemont, IL (Virtual)

Towards Practical Differentially Private Learning, Gwangju Institute of Science & Technology, South Korea, 2022 (Virtual)

Privacy-Preserving Machine Learning in Theory and Practice, Korea Internet & Security Agency (KISA), 2022

Differentially Private Normalizing Flows for Synthetic Tabular Data Generation, AAAI 2022 (Virtual)

Scaling up Differentially Private Deep Learning with Fast Per-example Gradient Clipping, PETS 2021 (Virtual)

Differentially Private Empirical Risk Minimization, Samsung SDS, 2020 (Virtual)

#SelfHarm on Instagram: Analysis and Classification of Non-Suicidal Self-Injury, CogMI 2019, Los Angeles, CA

Rényi Diferentially Private ERM for Smooth Objectives, AISTATS 2019, Naha, Japan

Concentrated Differentially Private Gradient Descent with Adaptive per-Iteration Privacy Budget, KDD 2018, London, UK

Differentially Private Variance Reduced Gradient, ICTCS, Amman, Jordan, 2017

Post-processing for Iterative Differentially Private Algorithms, TPDP ICML 2016 Workshop

Improving analysis of privacy-enhanced data, University at Albany, 2016

Data mining with Differential Privacy, NEC Laboratories Inc., NJ, 2014

Top-k Frequent Itemsets via Differentially Private FP-trees, KDD conference, NYC, NY, 2014

Top-k Frequent Itemsets via Differentially Private FP-trees, CERIAS Symposium 2014

Privacy-preserving data mining with differential privacy, University of Notre Dame, IN, 2013

Differential identifiability, KDD Conference, Beijing, China, 2012

Differential identifiablity, CERIAS Symposium, IN, 2012

Choosing ϵ for differential privacy, CERIAS Symposium, IN, 2011

Conference Program Committees

Privacy Enhancing Technologies Symposium (PETs 2024), PC Member

AAAI Conference on Artificial Intelligence (AAAI 2022, 2023), PC Member

ACM SIGKDD 2022-2023, PC Member

Artificial Intelligence and Statistics (AISTATS 2021, 2024), PC Member

Annual Computer Security Applications Conference (ACSAC 2023), PC Member

ICML Workshop on Theory and Practice of Differential Privacy (TPDP 2022), PC Member

SIAM International Conference on Data Mining (SDM 2022), PC Member

IEEE Symposium on Computational Intelligence in Cyber Security (IEEE CICS) 2019, PC Member

IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom) 2018, PC Member

National Cybersecurity Summit 2018, 2019, 2021, PC member

Southern Data Science Conference (SDSC) 2018 - 2020, PC Member

Open Science in Big Data (OSBD) Workshop, IEEE BigData 2017, 2018, PC Member

Professional Activities

NSF Security and Trustworthy Computing (SaTC) Panel 2017, 2022

Reviewer for Journal of Privacy and Confidentiality 2021, 2022

Reviewer for Journal of Mathematical Programming 2021

Reviewer for Journal of Neurocomputing 2021

Reviewer for Ambient Intelligence and Humanized Computing 2021

Reviewer for American Journal of Data Mining and Knowledge Discovery 2020-2021

Reviewer for International Conference on Artificial Intelligence and Statistics (AISTATS) 2020

Reviewer for IEEE Transactions on Pattern Analysis and Machine Intelligence 2019

Reviewer for IEEE Transactions on Knowledge and Data Engineering (TKDE), 2015-2016, 2018-2019, 2022

Reviewer for ACM Transactions on Database Systems (TODS), 2016, 2017

Reviewer for ACM Transactions on Privacy and Security (TOPS), 2022

Reviewer for IEEE Transactions on Information Forensics and Security (TIFS), 2018-2020

Reviewer for IEEE Transactions on Mobile Computing, 2020

Reviewer for Elsevier Journal of Computers & Security, 2015

Reviewer for Elsevier Journal of Network and Computer Applications (JNCA), 2017, 2019

Reviewer for IEEE Transactions on Dependable and Secure Computing, 2014, 2019, 2020

Reviewer for IEEE Transactions on Service Computing, 2017, 2018

Reviewer for IEEE Internet of Things Journal, 2019

External reviewer for VLDB 2012

Courses Developed

- UGA CSCI 8960: Privacy-preserving Data Analysis
- UGA CSCI 4260/6260: Data security and privacy
- UGA CSCI 8950: Large-scale Optimization for Machine Learning

Courses Taught

University of Georgia — Athens, GA

- Instructor, CSCI 2610 Discrete Mathematics — 2021 Spring
- Instructor, CSCI 4260/8260: Data security and privacy — 2018 Fall, 2020 Fall
- Instructor, CSCI 3360: Data science I — 2017, 2018 Spring, 2019 Fall
- Instructor, CSCI 8960: Privacy-preserving data analysis — 2017 Fall, 2019 - 2022 Spring
- Instructor, CSCI 6900: Special topics - data privacy — 2016 Fall

Scholdarship & Awards

Faculty recognition for student career development, UGA Career Center	*2019 - 2021*
Research excellence award, CS Department at UGA	*2019*
KDD Madness, Honorable mention	*2012*
Graduate fellowship, Yonsei University	*2006 — 2007*
University designated scholarship, Yonsei University	*2000 — 2001*

Media Coverage

Digging deep for data: Informatics at UGA is more than a numbers game, UGA Today, 2018

Preserving privacy in an ocean of personal data, UGA Research, 2020

Privacy-preserving machine learning, one of the fastest-growing fields in AI, AI Times, 2021 (in Korean)