

Unit Name

Machine Learning and Data Science Unit

Collaborations

Professor Jiliang Tang, Mr. Pengfei He, Mr. Haoyu Han, Michigan State University, US, Trustworthy AI

Dr. Kenta Niwa (Distinguished Researcher), NTT Communication Science Laboratories, Kyoto, Japan, Hyperparameter Tuning-free Optimization

Professor Hidetoshi Shimodaira, Professor Hitoshi Kashima, Kyoto University Professor Yasuaki Hiraoka, Professor Shinichi Minato, Kyoto University, Kyoto Japan, Development of machine learning technology and its practical applications

Research Personnel

Mohammad Sabokrou, Staff Scientist

Yao-Hung Hubert Tsai, Visiting Researcher

Michiel De Hoon, Visiting Researcher

Benjamin Poignard, Visiting Researcher

Han Bao, Visiting Researcher

Clea Mehnica Laouar, PhD Student

Jose Renato Restom Viera, MBZUAI, Visiting Research Student

Pengfei He, Michigan State University, Visiting Research Student

Siqi Zeng, University of Illinois Urbana-Champaign, Visiting Research Student

Weiqiu You, University of Pennsylvania, Visiting Research Student

Yuki Takezawa, Kyoto University, Visiting Research Student

Ayoub Hamza Rhim, Ecole des Ponts Paris Tech, Research Intern

Daniel Yuxin Yang, ETH, Research Intern

Gabriele Pedroni, University Paris-Saclay, Research Intern

Guillaume Adrien Godefroy Henon-Just, University Paris-Saclay, Research Intern

Kenta Ozawa, Ecole Polytechnique, Research Intern

Pavlo Shkurovatskyi, University of Cambridge, Research Intern

Rahul Heinrich Steiger, ETH, Research Intern

Satoki Ishikawa, Tokyo Institute of Technology, Research Intern

Seyed Alireza Salehy Dehnavi, University of Tehran, Research Intern

Thibault de Surrel, Université Paris Dauphine, Guest Student

Scholarly Contributions and Creative Productions (by Faculty)

Conference Proceedings

1. Takezawa, Y.; Sato, R.; Bao, H.; Niwa, K.; Yamada, M.

- Polyak Research Intern Meets Parameter-Free Clipped Gradient Descent. In NeurIPS; 2024.
2. Sinha, A.; Zeng, S.; Yamada, M.; Zhao, H.
Learning Structured Representations with Hyperbolic Embeddings. In NeurIPS; 2024.
 3. Lin, Y.; He, P.; Xu, H.; Xing, Y.; Yamada, M.; Liu, H.; Tang, J.
Towards Understanding Jailbreak Attacks in LLMs: A Representation Space Analysis. In EMNLP; 2024.
 4. Pourkeshavarz, M.; Sabokrou, M.; Rasouli, A.
Adversarial Backdoor Attack by Naturalistic Data Poisoning on Trajectory Prediction in Autonomous Driving. In CVPR; 2024.
 5. Houry, G.; Bao, H.; Zhao, H.; Yamada, M.
Fast 1-Wasserstein Distance Approximations Using Greedy Strategies. In AISTATS; 2024.
 6. Han, H.; Liu, X.; Ma, L. i.; Torkamani, M.; Liu, H.; Tang, J.; Yamada, M.
Structural Fairness-Aware Active Learning for Graph Neural Networks. In ICLR; 2024.
 7. Naylor, P.; Di, C., Diego; Traviglia, A.; Yamada, M.; Fiorucci, M.
Implicit Neural Representation for Change Detection. In WACV; 2024.

Journal Article

1. He, P.; Xu, H.; Ren, J.; Cui, Y.; Zeng, S.; Xing, Y.; Tang, J.; Yamada, M.; Sabokrou, M.
Stealthy Backdoor Attack via Confidence-Driven Sampling. Transactions on Machine Learning Research 2024.
2. Yamada, M.; Takezawa, Y.; Houry, G.; Dusterwald, K. M.; Sulem, D.; Zhao, H.; Tsai, Y.-H. H.
An Empirical Study of Simplicial Representation Learning with Wasserstein Distance. Entropy 2024.

Scholarly Contributions (For Unit Members Only)

Name of Unit Member (Author-Presenter)	Type	Title	Outlet	Publisher	Year Pub
Mohammad Sabokrou	Conference Proceedings	Scanning Trojaned Models Using Out-of-Distribution Samples		NeurIPS	2024
Mohammad Sabokrou	Conference Proceedings	Adversarial Backdoor Attack by Naturalistic Data Poisoning on Trajectory Prediction in Autonomous Driving.		CVPR	2024
Mohammad Sabokrou	Conference Proceedings	Stealthy Backdoor Attack via Confidence-driven Sampling		Transactions on Machine Learning Research	2024
Mohammad Sabokrou	Conference Proceedings	Universal Novelty Detection through Adaptive Contrastive Learning		CVPR	2024
Yao-Hung Hubert Tsai	Journal Article	An Empirical Study of Simplicial Representation Learning with Wasserstein Distance		MDPI Entropy	2024
Mohammad Sabokrou	Poster Presentation at Conference	Adversarially Robust Anomaly Detection through Spurious Negative Pair Mitigation	Conference on Neural Information Processing Systems		2025

Honors, Awards & Fellowships

2024-11-01 - Ongoing IEICE TC-IBISML Research Award, IEICE TC-IBISML Research Award, 2024

External Service

2025-02-01 - Ongoing Area chair, ICML 2025

2024-09-01Area chair, ICLR 2025

2024Area chair, NeurIPS 2024

Other Institutional Service

2024-11-02

Okinawa Mathematics Cafe 沖縄数学カフェ, (Research Units)

Workshops and Seminars (Organized and Hosted by Faculty/Units)

Speaker Name(s)	Title	Location	Co-Organizers	Date
Prof. Pierre Alquier, Prof. Yuki Asano, Dr. Frank Nielsen, Prof. Asuka Takatsu, Prof. Marco Modelli, Dr. Aston Zhang, Prof. Yuki Arase, Prof. Krilamol Muadet, Prof. Hisashi Kashima, Prof. Asako Kanezaski, Prof. Sebastian Stich, Dr. Takuya Akiba, Prof. Kenji Doya, Prof. Makoto Yamada	OIST ML Workshop 2025	Auditorium, OIST	Research Center for Statistical Machine Learning	2025-03-03
Alireza Salehy, University of Tehran	MLDS Unit Seminar 2024-11	Seminar Room D23, Lab5		2024-10-23
Prof. Fumihiko Ishikawa(RIKEN-Institute of Science Tokyo)	MLDS Unit Seminar 2024-10	Seminar Room D23, Lab5, OIST		2024-10-22
Mr. Jose Restom, Dr. Mohammad Sabokrow	MLDS Unit Seminar 2024-9	Seminar Room D23, Lab5, OIST		2024-07-25
Ms. Weiqiu You, Mr. Xiaoyuan Zhang	MLDS Unit Seminar 2024-8	Seminar Room D23, Lab5, OIST		2024-07-18
Mr. Rahul Steiger, Mr. Thibault De Surrel	MLDS Unit Seminar 2024-7	Seminar Room C210, OIST		2024-07-11
Mr. Kazusato Oko, Mr. Yuki Takezawa	MLDS Unit Seminar 2024-6	Seminar Room C210, OISTC210		2024-07-09
Mr. Kenta Vert Ozawa, Ms. Cindy Zeng	MLDS Unit Seminar 2024-5	Seminar Room D23, Lab5, OIST		2024-06-27
Mr. Daniel Yuxin Yang, Mr. Guillaume Henon-Just	MLDS Unit Seminar 2024-4	Seminar Room D23, Lab5, OIST		2024-06-13
Dr. Makoto Yamada	MLDS Unit Seminar 2024-2	Seminar Room D23, Lab5, OISTLab		2024-06-06
Mr. Ayoub Rhim, Dr. Florian Yger	MLDS Unit Seminar 2024-3	Seminar Room D23, Lab5, OIST		2024-06-06
Dr. Gordon Wichern	MLDS Unit Seminar 2024-1	Seminar Room D23, Lab5, OIST		2024-04-26