FY 2025 Annual Report

Unit Name

Machine Learning and Data Science Unit

Associate Professor Makoto Yamada

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

Benjamin Poignard, Visiting Researcher

Yao-Hung Hubert Tsai, Visiting Researcher

Michiel De Hoon, Visiting Researcher

Xiaobing Sheng, Visiting Researcher

Han Bao, Visiting Researcher

Kaichuang Yang, Research Intern

Eiji Miyamoto, PhD Student

Clea Mehnia Laouar, PhD Student

Keyu Wang, Research Intern

Gabriele Pedroni, Research Intern

Selim Jerad, Research Intern

Remi Surat, Research Intern

Mouhssine Rifaki, Research Intern

Mohammed Yassine Habibi, Research Intern

Yi-Hsiang Chiao, Research Intern

Vedant Janardanbhai Dave, Research Intern

Antoine Gilson, Research Intern

Felix Theo Anael Chavelli, Visiting Research Student

Pengfei He, Visiting Research Student

Klea Ziu, Visiting Research Student

Kenta Ozawa, Visiting Research Student

Yuki Takezawa, Visiting Research Student

Scholarly Contributions and Creative Productions (by Faculty)

Conference Proceedings

1. Ishikawa, S.; Yamada, M.; Bao, H.; Takezawa, Y.

   PhiNets: Brain-Inspired Non-Contrastive Learning Based on Temporal Prediction Hypothesis. In ICLR; 2025.
2. Zeng, S.; Du, S.; Yamada, M.; Zhao, H.

   Learning Structured Representations by Embedding Class Hierarchy with Fast Optimal Transport. In ICLR; 2025.
3. Dusterwald, K. M.; Hromadka, S.; Yamada, M.

   Fast Unsupervised Ground Metric Learning with Tree-Wasserstein Distance. In ICLR; 2025.
4. He, P.; Xu, H.; Xing, Y.; Liu, H.; Yamada, M.; Tang, J.

   Data Poisoning for In-Context Learning. In NAACL Findings; 2025.

Journal Article

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

   Necessary and Sufficient Watermark for Large Language Models. Transactions on Machine Learning Research 2025.
2. He, P.; Cui, Y.; Xu, H.; Liu, H.; Yamada, M.; Tang, J.; Xing, Y.

   Towards the Effect of Examples on In-Context Learning: A Theoretical Case Study. Stat 2025, 14, e70045.

Scholarly Contributions (by Unit Members)

Name of Unit Member	Type	Title	Outlet	Publisher	Year Pub
Mohammad Sabokrou	Book Chapter	Dimensionality reduction in deep learning through group actions	Dimensionality Reduction in Machine Learning	Morgan Kaufmann	2025
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
Mohammad Sabokrou	Conference Proceedings	Scanning Trojaned Models Using Out-of-Distribution Samples		NeurIPS	2024
Mohammad Sabokrou	Journal Article	A unified concept-based system for local, global, and misclassification explanations	Neurocomputing	Elseviour	2025
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	APML: Adaptive Probabilistic Matching Loss for Robust 3D Point Cloud Reconstruction	NeurIPS	Openreview	2025

Name of Unit Member	Type	Title	Outlet	Publisher	Year Pub
Mohammad Sabokrou	Poster Presentation at Conference	Adversarially Robust Anomaly Detection through Spurious Negative Pair Mitigation	Conference on Neural Information Processing Systems		2025
Mohammad Sabokrou	Poster Presentation at Conference	Mitigating Spurious Negative Pairs for Robust Industrial Anomaly Detection	ICLR2025	Openreview	2025
Mohammad Sabokrou	Poster Presentation at Conference	Adversarially Robust Anomaly Detection through Spurious Negative Pair Mitigation	ICLR2025	Openreview	2025
Mohammad Sabokrou	Poster Presentation at Conference	FrameShield: Adversarially Robust Video Anomaly Detection	NeurIPS2025	Openreview	2025

Honors, Awards & Fellowships

Term 2 2024 - Ongoing	IEICE TC-IBISML Research Award, IEICE TC-IBISML Research Award, 2024 [Fiscal Year: 2024-11-01]
Term 2 2020 - Ongoing	Outstanding SPC award, ACM International Conference on Web Search and Data Mining (WSDM 2020), 2020 [Fiscal Year: 2020-04-01]
Term 2 2019 - Ongoing	Outstanding SPC award, ACM International Conference on Web Search and Data Mining (WSDM 2019), 2019 [Fiscal Year: 2019-04-01]
Term 2 2016 - Ongoing	Best paper award, ACM International Conference on Web Search and Data Mining (WSDM 2016), 2016 [Fiscal Year: 2016-04-01]
Term 2 2014 - Ongoing	Yahoo Labs Excellence Award, 2014, 2014 [Fiscal Year: 2014-04-01]

External Service

Term 2 2024 - Ongoing	Area chair, ICML 2025 [Fiscal Year: 2025-02-01]

Other Institutional Service

Term 1 2025 - Term 1 2025	Mathematics Event 'the Okinawa Math Festival'　おきなわ数学まつり, (Yamada - Machine Learning and Data Science Unit) [Fiscal Year: 2026-10-11]
Term 3 2025 - Term 3 2025	Let’s Explore the Latest AI Research! One-Day Hands-On Event　最新 AI 研究に触れてみよう！1 日体験イベント, (Yamada - Machine Learning and Data Science Unit) [Fiscal Year: 2025-08-08]

Workshops and Seminars [Organized and Hosted by Faculty/Units]

Speaker Name(s)	Title	Location	Co-Organizers	Date
Keynote Speakers: Prof. Nicolò Cesa-Bianchi (Università degli Studi di Milano / Politecnico di Milano, Italy), Prof. Kaoru Ota(Tohoku University / Muroran Institute of Technology), Prof. Yu-Chiang Frank Wang (National Taiwan University / NVIDIA), Dr. Leander Thiele (Kavli IPMU)	The 28th Information-Based Induction Science Workshop (IBIS2025)	Naha Cultural Arts Theater NAHArt	RIKEN AIP	2025-11-12
Prof. Lenka Zdeborová, EPFL	MLDS Unit Seminar 2025-7	Seminar Room C210 (& Zoom)		2025-10-20

Speaker Name(s)	Title	Location	Co-Organizers	Date
Ms. Haru Negami	MLDS Unit Seminar 2025-6	Seminar Room C210, OIST		2025-10-15
Dr. Aurélien Corroyer-Dulmont	MLDS Unit Seminar 2025-5	Seminar Room C210		2025-10-01
Mr. Rémi Surat, Ms. Klea Ziu	MLDS Unit Seminar 2025-4	Seminar Room D23, Lab 5, OIST		2025-09-16
Dr. Ziyin Liu	MLDS Unit Seminar 2025-3	Seminar Room C210, OIST		2025-07-15
Dr. Gregory Schwartzman	MLDS Unit Seminar 2025-2	Seminar Room C210, OIST		2025-07-11
Mr. Niklas Muennighoff	MLDS Unit Seminar 2025-1	Online		2025-05-13
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