

# Sina Sajadmanesh

📍 Zurich, Switzerland   ✉ sina.sajadmanesh@gmail.com   🌐 sajadmanesh.com   in sajadmanesh   📷 sisaman

## Education

Swiss Federal Institute of Technology (EPFL), PhD in Electrical Engineering	May 2019 – Aug 2023
Sharif University of Technology, MSc in Information Technology Engineering	Sept 2014 – Sept 2016
University of Isfahan, BSc in Computer Software Engineering	Sept 2009 – Feb 2014

## Experience

Sony AI, AI Engineer – Zurich, Switzerland   Oct 2023 – present

- Working on privacy-preserving vision foundation models
- Implemented easy-to-use APIs for vision foundation model inference and deployment
- Developed a comprehensive multi-task learning framework based on OpenMMLab libraries and PyTorch, supporting various vision tasks, new model architectures, and mixed-precision and distributed training
- Implemented an end-to-end open-world classification pipeline using MMClassification, HuggingFace transformers, and CLIP
- Improved model training and inference speed by optimizing the data pipeline, using mixed-precision training, and leveraging distributed training on multiple GPUs

Idiap Research Institute, Research Assistant – Martigny, Switzerland   May 2019 – Aug 2023

- Worked as a doctoral researcher on differentially private machine learning with graph neural networks
- **3 published papers** in top-tier conferences (CCS, USENIX Security, and NDSS) with **185+ citations**
- **7 invited talks** at top universities and research institutions, including Imperial College, UIC, and Twitter
- **6 open-source projects** with **110+ stars** on GitHub
- **1 short course** taught on "Trustworthy Machine Learning" at Artificial Intelligence Doctoral Academy 📄
- **Finalist** in CSAW Applied Research Competition 📄 for the best paper award in computer security in Europe

The Alan Turing Institute, Visiting Collaborator – London, UK   Mar 2023 – Mar 2023

- Co-organized a workshop on "Privacy and Fairness in AI for Health" 📄 with 60+ attendees

Brave Software, Research Intern – Remote   Mar 2022 – May 2022

- Developed a novel privacy-preserving **federated learning** framework for **neural bandit models** under client heterogeneity using PyTorch, Flower, Dask, and Tensorflow-Lite

Sharif University of Technology, Research Assistant – Tehran, Iran   Nov 2014 – May 2019

- Worked on various research projects including privacy-preserving machine learning, web data science, and social and information network analysis.
- **4 published papers** in top-tier venues (WWW, TKDD, IoTJ, ASONAM) with **430+ citations**
- **5+ press releases** in top-tier media outlets, including MIT Technology Review 📄, France 24 📄, and The Independent 📄
- **2 open-source projects** with **20+ stars** on GitHub
- **1 semester course** taught on "Fundamentals of Programming with Python" at Sharif University of Technology

## Skills and Expertise

**Programming Languages:** Python, C++, Java, SQL, Shell,  $\LaTeX$

**Machine Learning and AI:** PyTorch, TensorFlow, HuggingFace, OpenMMLab, PyTorch-Lightning

**MLOps and DevOps:** Weights & Biases, Docker, GitHub, Dask, Neptune, Linux

**Privacy-Enhancing Technologies:** Flower, Opacus, Auto-DP

## Community and Professional Service

---

**Invited Speaker:** Imperial College London (2023, 2020), University of Illinois at Chicago (2022), L3S Research Center (2022), Graph Neural Networks User Group Meetup (2021), Twitter Machine Learning Seminar (2021)

**Organizing Committee:** Privacy and Fairness in AI for Health [🔗](#) (2023)

**Program Committee:** PPAI [🔗](#) (2024), WiseML [🔗](#) (2023), PAIR2Struct [🔗](#) (2022), DPML [🔗](#) (2021)

**Reviewer:** NeurIPS [🔗](#) (2024), IMWUT [🔗](#) (2024), TDSC [🔗](#) (2023), LoG [🔗](#) (2023, 2022), AISTATS [🔗](#) (2023), AIJ [🔗](#) (2022), TBD [🔗](#) (2021), TIST [🔗](#) (2020), SNAM [🔗](#) (2020), WWWJ [🔗](#) (2018)

## Publications

---

<b>ProGAP: Progressive Graph Neural Networks with Differential Privacy Guarantees</b> <a href="#">🔗</a>	Mar 2024
Sina Sajadmanesh, Daniel Gatica-Perez	
ACM International Conference on Web Search and Data Mining (WSDM)	
<b>Privacy-Preserving Machine Learning on Graphs</b> <a href="#">🔗</a>	Aug 2023
Sina Sajadmanesh	
Doctoral Thesis - Swiss Federal Institute of Technology (EPFL)	
<b>GAP: Differentially Private Graph Neural Networks with Aggregation Perturbation</b> <a href="#">🔗</a>	Aug 2023
Sina Sajadmanesh, Ali Shahin Shamsabadi, Aurélien Bellet, et al.	
USENIX Security Symposium (USENIX Security)	
<b>Locally Private Graph Neural Networks</b> <a href="#">🔗</a>	Nov 2021
Sina Sajadmanesh, Daniel Gatica-Perez	
ACM Conference on Computer and Communications Security (CCS)	
<b>When Differential Privacy Meets Graph Neural Networks</b> <a href="#">🔗</a>	June 2020
Sina Sajadmanesh, Daniel Gatica-Perez	
Technical Report, ArXiv e-prints	
<b>A Hybrid Deep Learning Architecture for Privacy-Preserving Mobile Analytics</b> <a href="#">🔗</a>	May 2020
Seyed Ali Osia, Ali Shahin Shamsabadi, Sina Sajadmanesh, et al.	
IEEE Internet of Things Journal (IoTJ)	
<b>Continuous-Time Relationship Prediction in Dynamic Heterogeneous Information Networks</b> <a href="#">🔗</a>	Aug 2019
Sina Sajadmanesh, Sogol Bazargani, Jiawei Zhang, Hamid R. Rabiee	
ACM Transactions on Knowledge Discovery from Data (TKDD)	
<b>NPGLM: A Non-Parametric Method for Temporal Link Prediction</b> <a href="#">🔗</a>	June 2017
Sina Sajadmanesh, Jiawei Zhang, Hamid R. Rabiee	
Technical Report, ArXiv e-prints	
<b>Kissing Cuisines: Exploring Worldwide Culinary Habits on the Web</b> <a href="#">🔗</a>	Apr 2017
Sina Sajadmanesh, Sina Jafarzadeh, Seyed Ali Ossia, et al.	
International World Wide Web Conference Companion (WWW)	
<b>Predicting Anchor Links between Heterogeneous Social Networks</b> <a href="#">🔗</a>	Aug 2016
Sina Sajadmanesh, Hamid R. Rabiee, Ali Khodadadi	
International Conference on Advances in Social Networks Analysis and Mining (ASONAM)	