

MIKKO A. HEIKKILÄ

mixheikk@proton.me ♦ mixheikk.github.io

EDUCATION

- University of Helsinki** 2023
Doctor of Philosophy
PhD thesis title: Differentially private and distributed Bayesian learning
- University of Helsinki** 2016
MSc Computational statistics
Minor in Mathematics & Computer science
- University of Helsinki** 2015
BSc Statistics
Minor in Mathematics & Computer science
- University of Helsinki** 2013
MA Folklore studies
Minor in Sociology & Finnish literature studies

RESEARCH EXPERIENCE

- University of Helsinki** 2024 -
Postdoctoral researcher *Helsinki, Finland*
· Trustworthy machine learning (e.g. differential privacy, fairness, robustness), federated learning, Bayesian learning.
- Telefónica Research** 2023 - 24
Associate researcher *Barcelona, Spain*
· Trustworthy machine learning (with differential privacy, algorithmic fairness, adversarial robustness) and learning from distributed data (federated learning).
- University of Helsinki** 2017 - 2023
Doctoral candidate *Helsinki, Finland*
· Privacy-preserving (differentially private) machine learning, distributed learning (federated learning), and Bayesian learning.
- University of Helsinki** June 2016-2017
Research assistant *Helsinki, Finland*
· Probabilistic graphical models and differential privacy.
- Tutkimustoimisto Kide Oy** January-December 2015
Data analyst *Helsinki, Finland*
· Statistical analysis and visualisation.
- IFO Institute** February-March 2014
Undergraduate intern *Munich, Germany*

- Assisting in statistical research by running statistical analysis and doing visualisations.

PUBLICATIONS

Tobaben, Alrawajfeh, Klasson, **Heikkilä**, Solin & Honkela: Differential privacy in continual learning: Which labels to update? On ArXiv, 2025.

Zhao, Rehn, **Heikkilä**, Tajeddine & Honkela: *Mitigating disparate impact of differentially private learning through bounded adaptive clipping*. On ArXiv, 2025.

Jimenez G., Solans, **Heikkilä**, Vitaletti, Kourtellis, Anagnostopoulos & Chatzigiannakis: *Non-IID data in federated learning: A survey with taxonomy, metrics, methods, frameworks and future directions*. On ArXiv, 2025.

Heikkilä: *On using secure aggregation in differentially private federated learning with multiple local steps*. In TMLR 2025.

Shah, Solans, **Heikkilä**, Raj & Kourtellis: *Speech robust bench: A robustness benchmark for speech recognition*. In ICLR 2025.

Corbucci, **Heikkilä**, Solans, Monreale & Kourtellis: *PUFFLE: Balancing privacy, utility, and fairness in federated learning*. In ECAI, 2024.

Heikkilä, Ashman, Swaroop, Turner & Honkela: *Differentially private partitioned variational inference*. In TMLR, 2023.

Koskela, **Heikkilä**, & Honkela: *Numerical accounting in the shuffle model of differential privacy*. In TMLR (Featured Certification), 2023.

Heikkilä, Koskela, Shimizu, Kaski, & Honkela: *Differentially private cross-silo federated learning*. On ArXiv, 2020.

Heikkilä, Jälkö, Dikmen & Honkela: *Differentially private Markov chain Monte Carlo*. In NeurIPS 2019 (Spotlight).

Niinimäki, **Heikkilä**, Honkela & Kaski: *Representation transfer for differentially private drug sensitivity prediction*. In ISMB 2019.

Heikkilä, Lagerspetz, Kaski, Shimizu, Tarkoma & Honkela: *Differentially private Bayesian learning on distributed data*. In NIPS 2017.

GRANTS

Nokia Scholarship	2017, 2020
-------------------	------------

TEACHING EXPERIENCE

Seminar on AI Security and Safety	Spring 2025 Teaching Assistant
Statistics for Data Science	Autumn 2022 Teaching Assistant
Computational Statistics	Autumn 2021 & Spring 2022 Teaching Assistant
Computational Statistics II	Autumn 2017 & 2018 Main lecturer (project course)
Bachelor student seminar	Spring 2020 Supervisor (CS department)
Trustworthy Machine Learning	Autumn 2020 Teaching Assistant

SERVICE

Peer-reviewer

NeurIPS, ICML, ICLR (Highlighted reviewer), AISTATS, UAI, TMLR, JMLR

TECHNICAL STRENGTHS

Programming languages Python, R, Matlab, Java (more used ones, currently mostly Python)

LANGUAGES

Finnish	Native
English	Near-native
Spanish	Good
Swedish	Basic