Maksym Andriushchenko

PERSONAL DATA

Site: https://andriushchenko.me/	**Scholar:** https://scholar.google.com/citations?user=ZNtuJYoAAAAJ
Email: maksym@andriushchenko.me	**Github:** https://github.com/max-andr/

EDUCATION

École Polytechnique Fédérale de Lausanne (EPFL), Switzerland Sep 2019 - now	**PhD student in Computer Science** **Group**: Theory of Machine Learning headed by Nicolas Flammarion **Research focus**: adversarial robustness and understanding generalization in deep learning.
Saarland University, Germany Oct 2016 – Aug 2019	**Master's Degree in Computer Science** **GPA**: **1.1** (1.0 is the best grade, 5.0 is the worst grade) **Thesis**: Provable Adversarial Defenses for Boosting (completed at the **University of Tübingen**, supervised by Matthias Hein).
Dnipro National University of Railway Transport, Ukraine Sep 2012 – June 2016	**Bachelor's Degree in Software Engineering** — *with honors* **GPA**: **96.5** (100 is the best grade, 60 is the worst grade) **Thesis**: A question-answering system based on knowledge from Wikipedia

AWARDS

Scholarships and Grants	**Google PhD fellowship 2022-2025 ($80k per year)** **Open Philanthropy AI PhD Fellowship 2022-2024 ($10k per year for travel/equipment)** **Google Research Collab 2022-2023 ($80k for one year + $20k in cloud compute)** EDIC PhD fellowship from EPFL for the first year DAAD MSc scholarship for 2 years to study at Saarland University
Awards	ICLR'21 Security & Safety in ML Systems Workshop: **Best Paper Honorable Mention Prize** Swiss Machine Learning Day: **best paper award** for "*Provably Robust Boosted Decision Stumps and Trees against Adversarial Attacks*" (also published at NeurIPS'19)
Travel grants	NeurIPS'19, NeurIPS'17, ICML'19 Workshop on Uncertainty & Robustness in Deep Learning, ICML'18 student volunteer grant, Machine Learning Summer School 2015 at Kyoto University

SELECTED PUBLICATIONS

M. Andriushchenko, A. Varre, L. Pillaud-Vivien, N. Flammarion. SGD with large step sizes learns sparse features (arXiv, 2022) [paper]

M. Andriushchenko, N. Flammarion. Towards Understanding Sharpness-Aware Minimization (ICML'22) [paper]

M. Andriushchenko, X. Li, G. Oxholm, T. Gittings, T. Bui, N. Flammarion, J. Collomosse ARIA: Adversarially Robust Image Attribution (CVPR'22 Workshop on Media Forensics) [paper]

F. Croce*, **M. Andriushchenko***, V. Sehwag*, N. Flammarion, M. Chiang, P. Mittal, M. Hein. RobustBench: a standardized adversarial robustness benchmark (NeurIPS'21 Datasets and Benchmarks Track, **Best Paper Honorable Mention Prize** at ICLR'21 Workshop on Security and Safety in Machine Learning Systems) [paper]

M. Mosbach, **M. Andriushchenko**, D. Klakow. On the Stability of Fine-tuning BERT: Misconceptions, Explanations, and Strong Baselines (ICLR'21) [paper]

M. Andriushchenko, N. Flammarion. Understanding and Improving Fast Adversarial training (NeurIPS'20) [paper]

M. Andriushchenko*, F. Croce*, N. Flammarion, M. Hein. Square Attack: a query-efficient black-box adversarial attack via random search (ECCV'20) [paper]

M. Andriushchenko, M. Hein. Provably Robust Boosted Decision Stumps and Trees against Adversarial Attacks (NeurIPS'19) [paper]

M. Hein, **M. Andriushchenko**, J. Bitterwolf. Why ReLU networks yield high-confidence predictions far away from the training data and how to mitigate the problem (**oral at CVPR'19**) [paper]

M. Hein and **M. Andriushchenko**. Formal Guarantees on the Robustness of a Classifier Against Adversarial Manipulation (NeurIPS'17) [paper]

ACADEMIC SERVICE

Reviewer	NeurIPS'22 (**top reviewer**), ICML'22, NeurIPS'21, ICML'21, CVPR'21, ICLR'21 (**outstanding reviewer**), NeurIPS'20 (**top 10% reviewers**)
Program committee in workshops	**NeurIPS'22** "Workshop on Distribution Shifts", **NeurIPS'22** "ML Safety Workshop", **ICML'22** "New Frontiers in Adversarial Machine Learning", **ICML'22** "Principles of Distribution Shift", **NeurIPS'21**: "Distribution Shifts: Connecting Methods and Applications", **ICML'21** "Uncertainty and Robustness in Deep Learning", **CVPR'21** "Adversarial ML in Real-World Computer Vision Systems", **ICLR'21** "Robust and Reliable ML in the Real World", "Security and Safety in ML Systems", **ICML'20** "Uncertainty and Robustness in Deep Learning", **CVPR'20** "Adversarial ML in Computer Vision", **ICLR'20** "Towards Trustworthy ML" (**best reviewer award**)
Participant	Robust AI 4-day workshop organized by AirBus AI Research and TNO (January 2021)
Volunteer	National coordinator for Switzerland at #ScienceForUkraine Coordinator for Switzerland and admission officer at the Ukrainian Global University AI and STEM workshop at a summer camp for displaced Ukrainian children in Romania

WORK EXPERIENCE

Adobe Research, Media Intelligence Lab	**Time**: July 2021 – October 2021 **Role**: Research Intern supervised by John Collomosse. Developed adversarially robust image provenance models which are being patented and operationalized for Content Authenticity Initiative. Contributed to a data augmentation library beacon_aug.
PrivatBank (a part-time job in the largest Ukrainian bank)	**Time:** November 2015 – June 2016 **Role:** Data Scientist working on predictive modeling, e-commerce personalization, text analysis.
Cinemalist (a startup with 500 active users)	**Time**: June 2013 – December 2014 (active time of development) **Role**: Co-founder of a movie recommendation website. Developed a personalized recommender system, website, and oversaw the general development of the project.

STUDENT SUPERVISION

Jana Vuckovic	**MSc Project (2022)**: "Exploring the connection between sharpness and out-of-distribution performance"
Mehrdad Saberi	**Summer internship (2021):** "Wasserstein adversarial training and perceptual adversarial robustness"
Edoardo Debenedetti	**MSc project (2021)**: "RobustBench: a standardized adversarial robustness benchmark". This work led to a publication at NeurIPS'21 Datasets and Benchmarks Track.
Etienne Bonvin	**MSc project (2020)**: "Adversarial robustness of kernel methods"

TEACHING EXPERIENCE

EPFL	**Probability & Statistics 2021, 2022** (by E. Abbé), **Machine Learning 2020, 2021, 2022** (by M. Jaggi, N. Flammarion), **Advanced Algorithms 2020** (by M. Kapralov)
MPI for Informatics	**Machine Learning 2018-2019** (lecturer: B. Schiele)
Saarland University	**Neural Networks: Implementation and Application 2017** (lecturer: D. Klakow)

PERSONAL

Long-distance running (personal best half-marathon: 1 hour 30 min), trail running, orienteering, history books.