

# Maksym Andriushchenko

## PERSONAL DATA

**Site:** <https://andriushchenko.me/>  
**Email:** [maksym@andriushchenko.me](mailto:maksym@andriushchenko.me)

**Scholar:** <https://scholar.google.com/citations?user=ZNtuJYoAAAAJ>  
**Github:** <https://github.com/max-andr/>

## EDUCATION

**École Polytechnique Fédérale de Lausanne (EPFL), Switzerland (Sep 2019 - now)**  
PhD student in Computer Science advised by Nicolas Flammarion

**Saarland University, Germany (Oct 2016 – Aug 2019)**  
Master's Degree in Computer Science advised by Matthias Hein from the University of Tübingen

**Dnipro National University of Railway Transport, Ukraine (Sep 2012 – June 2016)**  
Bachelor's Degree in Software Engineering — *with honors*

## 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 (ICML 2023) [[paper](#)]
- M. Andriushchenko**, N. Flammarion. Towards Understanding Sharpness-Aware Minimization (ICML 2022) [[paper](#)]
- M. Mosbach, **M. Andriushchenko**, D. Klakow. On the Stability of Fine-tuning BERT: Misconceptions, Explanations, and Strong Baselines (ICLR 2021) [[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 2020) [[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 2019**) [[paper](#)]
- M. Hein and **M. Andriushchenko**. Formal Guarantees on the Robustness of a Classifier Against Adversarial Manipulation (NeurIPS 2017) [[paper](#)]

## ACADEMIC SERVICE

- Reviewer**                    ICML'23, 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**    **ICML'23** “2nd ICML Workshop on New Frontiers in Adversarial ML”, **ICLR'23** “Workshop on Pitfalls of Limited Data and Computation for Trustworthy ML”, **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,** **Time:** July 2021 – October 2021  
 Media Intelligence Lab **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** **Time:** November 2015 – June 2016  
 (a part-time job in the largest Ukrainian bank) **Role:** Data Scientist working on predictive modeling, e-commerce personalization, text analysis.

**Cinemalist** **Time:** June 2013 – December 2014 (active time of development)  
 (a startup with 500 active users) **Role:** Co-founder of a movie recommendation website. Developed a personalized recommender system, website, and oversaw the general development of the project.

## STUDENT SUPERVISION

**Francesco d'Angelo** **PhD semester project (2023):** “Understanding the role of weight decay in deep learning”

**Théau Vannier** **MSc project (2023):** “Understanding the training instability of transformers”

**Joshua Freeman** **BSc project (2022, unofficial):** “Automatic recognition of unexploded ordnance using transfer learning”

**Jana Vuckovic** **MSc project (2022):** “Rethinking the relationship between sharpness and generalization”

**Mehrdad Saberi** **Summer internship (2021):** “Wasserstein adversarial training and perceptual robustness”

**Edoardo Debenedetti** **MSc project (2021):** “RobustBench: a standardized adversarial robustness benchmark” (published at NeurIPS'21 Datasets and Benchmarks Track)

**Klim Kireev** **PhD semester project (2020):** “On the effectiveness of adversarial training against common corruptions” (published at UAI'22)

**Etienne Bonvin** **MSc project (2020):** “Adversarial robustness of kernel methods”

**Oriol Barbany** **MSc project (2019):** “Affine-invariant robust training”

## 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.