

ALEXANDRE ARAUJO

162 rue de la Croix Nivert – 75 015 – Paris

☎ +33 6 74 75 22 75 • ✉ alexandre.araujo@dauphine.eu
🌐 alexandrearaujo.com

EDUCATION

PSL Research University **Paris, France**
Ph.D. in Computer Science (Thesis defended in June 2021) *2017 – 2021*
○ Subject: Building Compact and Robust Deep Neural Networks with Toeplitz Matrices
○ Advisors: Pr. Jamal Atif, Pr. Yann Chevaleyre and Dr. Benjamin Negrevergne

SKEMA Business School **Lille, France**
MS in Economics *2013 – 2016*

University of Versailles Saint-Quentin-en-Yvelines **Versailles, France**
DEUG in Mathematics (equivalent of 2 years of bachelor's degree) *2008 – 2010*

PUBLICATIONS

On Lipschitz Regularization of Convolutional Layers using Toeplitz Matrix Theory

Alexandre Araujo, Benjamin Negrevergne, Yann Chevaleyre and Jamal Atif

Thirty-Fifth AAAI Conference on Artificial Intelligence (2020)

Advocating for Multiple Defense Strategies against Adversarial Examples

Alexandre Araujo, Laurent Meunier, Rafael Pinot, and Benjamin Negrevergne

Workshop on Machine Learning for CyberSecurity (MLCS@ECML-PKDD) (2020)

Understanding and Training Deep Diagonal Circulant Neural Networks

Alexandre Araujo, Benjamin Negrevergne, Yann Chevaleyre and Jamal Atif

24th European Conference on Artificial Intelligence (ECAI 2020) (2019)

Theoretical Evidence for Adversarial Robustness through Randomization

Rafael Pinot, Laurent Meunier, Alexandre Araujo, Hisashi Kashima, Florian Yger, Cedric Gouy-Pailler and Jamal Atif

Advances in Neural Information Processing Systems 32 (2019)

Compact Deep Learning Models for Video Classification using Circulant Matrices

Alexandre Araujo, Benjamin Negrevergne, Yann Chevaleyre and Jamal Atif

The European Conference on Computer Vision (ECCV) Workshops (2018)

TEACHING

Executive Master – Université Paris Dauphine – PSL **Paris, France**
AI project & Machine Learning *2020, 2021*

Master IASD – Université Paris Dauphine-PSL **Paris, France**
Data Mining & Machine Learning *2019*

Master ID – Université Paris Dauphine-PSL **Paris, France**
Data Mining & Machine Learning *2019*

Master Data Science – École Polytechnique **Paris, France**
Data Science & Machine Learning *2016, 2017, 2018, 2019, 2020*

INDUSTRY EXPERIENCE

Wavestone **Paris, France**
Ph.D. Candidate – CIFRE contract *2017 – 2020*

- Participation in the research and development program
- Supervision of trainees on core machine learning issues (security, scalability, interpretability, etc.)
- Management of the partnership with Ecole Polytechnique

Wavestone **Paris, France**
Data Scientist *2015 – 2017*

- Mortgage Broker – Gathered 5 years of historic data and applied Machine Learning algorithms to predict if the mortgage application will be accepted. Deployed the model into production.
- Energy Company – Gathered 3 years of historic data with Hadoop to construct a dataset with 1 billion lines. Applied Machine Learning algorithms to predict if the customer is willing to leave for the competitor (churn).
- Railway Company – Gathered 20 years of historic data for dataset creation. Applied Machine Learning algorithms to predict train breakdown.

Amazon **Luxembourg**
Data Engineer Intern *dec. 2014 – may 2015*

- Coded SQL queries on Amazon Redshift that showcase transportation and financial statistics.
- Automated data pipelines to feed BI dashboards.

SUPERVISED INTERNSHIPS

Alexandre Verine: Master student, Summer 2019 (Now Ph.D. student)
A dive into Adversarial Attacks in the latent space with Invertible Networks

INVITED TALKS

INRIA/ENS Paris	<i>July 2021</i>
ENS Lyon	<i>July 2021</i>
INSIS – French National Center for Scientific Research	<i>January 2021</i>
PFIA – French AI conference	<i>June 2019, 2020, 2021</i>
International Cybersecurity Forum	<i>January 2020</i>
Limits of AI – BPI Conference	<i>June 2019</i>

SOFTWARE

Advertorch : Contributor of open-source library for adversarial robustness research with PyTorch
Circulant Youtube-8M: Author of open-source library for training efficient & compact Deep Learning model for video classification
Adversarial Robustness Through Randomization: Author of open-source library for training randomized neural networks to be robust against adversarial attacks

TECHNICAL SKILLS

Programming Languages : Python, C++, SQL
HPC Job Schedulers : Slurm, IBM Spectrum LSF
Deep Learning Frameworks : TensorFlow, PyTorch
ML Libraries: XGBoost, LightGBM, Scikit-Learn
Data Science Framework : OpenCV, SciPy, NumPy, Pandas