

# ALEXANDRE ARAUJO

162 rue de la Croix Nivert – 75 015 – Paris

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

*Last update: July 15, 2020*

## EDUCATION

---

### PSL Research University, Université Paris-Dauphine

*Ph.D. Candidate in Computer Science (Expected graduation: Dec. 2020)*

- Subject: Building Compact and Secure Deep Neural Networks
- Advisors: Pr. Jamal Atif, Pr. Yann Chevaleyre and Dr. Benjamin Negrevergne

**Paris, France**

*2017 – Present*

### SKEMA Business School

*Master in Economics and Project Management*

**Lille, France**

*2013 – 2016*

### Université de Versailles

*Mathematics - Physics*

**Versailles, France**

*2008 – 2010*

## PUBLICATIONS

---

### Fast & Accurate Method for Bounding the Singular Values of Convolutional Layers with Application to Lipschitz Regularization

*Alexandre Araujo, Benjamin Negrevergne, Yann Chevaleyre and Jamal Atif*  
preprint (2020)

### Robust Neural Networks using Randomized Adversarial Training

*Alexandre Araujo, Laurent Meunier, Rafael Pinot, and Benjamin Negrevergne*  
preprint (2020)

### 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)*

### 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) (2020)

### Training 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

---

### Master Data Science – Ecole Polytechnique

*Data Science & Machine Learning Project*

**Paris, France**

*2016 – 2020*

### Master IASD – PSL Research University, Université Paris-Dauphine

*Data Mining & Machine Learning*

**Paris, France**

*2019*

### Master ID – PSL Research University, Université Paris-Dauphine

*Data Mining & Machine Learning*

**Paris, France**

*2019*

## SUPERVISED INTERNSHIPS

---

**Alexandre Verine:** Master student, Summer 2019

A dive into Adversarial Attacks in the latent space with Invertible Networks

## INDUSTRY EXPERIENCE

---

**Wavestone**

*Data Scientist*

**Paris, France**

*2015 – 2017*

**Amazon**

*Data Engineer Intern*

**Luxembourg**

*dec. 2014 – may 2015*

## INVITED TALKS

---

**Limits of AI, BPI Conference**

*June 2019*

**International Cybersecurity Forum**

*January 2020*

## 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

**Deep Learning Frameworks :** TensorFlow, PyTorch

**ML Libraries:** XGBoost, LightGBM, Scikit-Learn

**Data Science Framework :** OpenCV, SciPy, NumPy, Pandas