# 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: December 4, 2020*

## EDUCATION

**PSL Research University, Université Paris-Dauphine**                                          **Paris, France**
*Ph.D. Candidate in Computer Science (Expected defense: Feb. 2021)*                     *2017 – Present*
- Subject: Building Compact and Secure Deep Neural Networks
- Advisors: Pr. Jamal Atif, Pr. Yann Chevaleyre and Dr. Benjamin Negrevergne

**SKEMA Business School**                                                                                        **Lille, France**
*Master in Economics and Project Management*                                                        *2013 – 2016*

**Université de Versailles**                                                                              **Versailles, France**
*Mathematics - Physics*                                                                                           *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 (2021)

**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)

**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**                                                     **Paris, France**
*Data Sience & Machine Learning Project*                                                               *2016 – 2020*
**Master IASD – PSL Research University, Université Paris-Dauphine**                    **Paris, France**
*Data Mining & Machine Learning*                                                                                    *2019*
**Master ID – PSL Research University, Université Paris-Dauphine**                        **Paris, France**
*Data Mining & Machine Learning*                                                                                    *2019*

## Supervised Internships

**Alexandre Verine**: Master student, Summer 2019
A dive into Adversarial Attacks in the latent space with Invertible Networks

## Industry Experience

| | |
|---|---|
| **Wavestone** | **Paris, France** |
| *Ph.D. Candidate – CIFRE (Industrial Agreements for Training through Research)* | *2017 – 2020* |
| *Data Scientist* | *2015 – 2017* |
| **Amazon** | **Luxembourg** |
| *Data Engineer Intern* | *dec. 2014 – may 2015* |

## Invited Talks

| | |
|---|---|
| **INSIS – French National Center for Scientific Research** | *January 2021* |
| **PFIA – French AI conference** | *June 2020* |
| **International Cybersecurity Forum** | *January 2020* |
| **Limits of AI – BPI Conference** | *June 2019* |

## 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