www.raphaelolivier.github.io

Raphaël Olivier

5000 Forbes Avenue
Pittsburgh PA, USA 15213
✉ *rolivier@cs.cmu.edu*
raphaelolivier.github.io
Github: RaphaelOlivier

Education

2019–Ongoing **Carnegie Mellon University**,
Ph.D in Language Technologies, Language Technologies Institute
Thesis on security and robustness for Speech Recognition models, advised by prof. Bhiksha Raj

2017–2019 **Carnegie Mellon University**,
M.S. in Language Technologies, Language Technologies Institute

2014–2017 **École Polytechnique of Paris**,
Applied Mathematics and Computer Science, Ingénieur Polytechnicien Program

2012–2014 **Classes Preparatoirs**,
Math, Physics and Computer Science, Lycée Pasteur

- Two years of intensive training for nationwide entrance exams to French Grandes Écoles
- Ranked 1st/40 all two years
- Ranked 30th to 60th nationwide at 4 competitive entrance exams

Experience

June 2021–Aug 2021 **Applied Scientist Intern**, Amazon Alexa, Pittsburgh, PA
I worked on data poisoning attacks and defenses on Speech Recognition models

June 2020–Aug 2020 **Applied Scientist Intern**, Amazon Alexa, Pittsburgh, PA
I worked privacy and membership inference attacks and defenses on Speech Recognition models

Apr 2017–Aug 2017 **Research Intern**, AgroParisTech, Paris, France
Research project on Transfer Learning for time series using boosting methods, advised by prof. Antoine Cornuejols

June 2016–Aug 2016 **Data Scientist Intern**, DataScienTest, Paris, France
Participated in the creation of the DataScienTest platform that trains and evaluate data scientists online.

Projects

Jan 2021–Ongoing **Evaluating robustness beyond adversarial accuracy**, *Prof. Bhiksha Raj*

- Identify limits of the current methodology for evaluating robustness to adversarial attacks
- Design alternative robustness metrics to overcome those limits
- Papers in review at the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) and the AAAI Conference on Artificial Intelligence

Sep 2020–Nov 2021 **Sequential Randomized Smoothing for Adversarially Robust Speech Recognition[Code]**, *Prof. Bhiksha Raj*

- Combine Randomized Smoothing for adversarial robustness and Speech Processing performance mitigation strategies
- Released code for robust DeepSpeech2 and Transformer models
- Paper presented at the 2021 Conference on Empirical Methods in Natural Language Processing

Jan 2020–June 2021 **High-Frequency Smoothing for robust audio classification** , *Prof. Bhiksha Raj*

- Improve randomized smoothing to account for the distribution of adversarial perturbation in the high-frequency spectrum
- Paper presented at the 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)

Sep 2018–Dec 2018 **Movie-level Representation for Clip-level Movie Tasks**, *Self-motivated*

- Implement multimodal models for tasks on movie clips such as caption generation
- Apply Contextual embeddings from the entire movie to improve performance

Jan 2018 - Nov 2018 **Retrieval-based neural code generation [Code]**, *Prof. Graham Neubig*

- Implement the paper *A Syntactic Neural Model for General-Purpose Code Generation* by Pengcheng Yin and Graham Neubig
- Improve the results of this paper with sentence retrieval from the training set
- Paper presented at the 2018 Conference on Empirical Methods in Natural Language Processing

Apr 2017–Aug 2017 **Transfer Learning by Learning Projections from Target to Source**, *Prof. Antoine Cornuejols*

- Time series prediction with boosting of weak predictors
- Application to transfer learning contexts
- Paper presented at the 2020 Symposium on Intelligent Data Analysis

Skills

Languages	Python(A), C/C++(B), Java, SQL(B)
Frameworks	PyTorch, Tensorflow, DyNet
Utilities	Anaconda, Git, Jupyter Notebook, Alexa Skills. AWS Lambda

Courses

Machine Learning	Natural Language Processing, Deep Learning, Advanced Machine Learning, Multimodal Machine Learning, Neural Language Translation
Computer Science	Algorithms, Advanced Programming, Data Management, Computational Geometry
Math	Logic, Linear Algebra, Group and Field Algebra, Galois Theory, Number Theory, Analysis, Optimization, Differential Equations, Sequences and Series

Teaching

Sep 2018–May 2019 **Introduction to Deep Learning**, *Prof. Bhiksha Raj*, Teaching Asistant

- 200+ students course at Carnegie Mellon University
- Recitations, Homework design and grading, Office Hours, Project mentoring, Surrogate lectures