MARCO ROMANELLI, Ph.D.

+1 (347) 930-2338 marcoromane@gmail.com https://github.com/marcoromanelli-github

Ph.D. graduate with 4 years of experience in research and programming offering a strong foundation in Computer Science with a concentration in Machine Learning and Information Theory applied to Security and Privacy. Experienced in object-oriented programming: developing, testing and debugging code.

EDUCATION

Ph.D. in Computer Science *October 2020*
Inria-Saclay, Paris, France
University of Paris-Saclay and École Polytechnique, Paris, France
Joint Ph.D. with Università di Siena, Siena, Italy.

M.S. in Computer Engineering *April 2017*
Computer and Automation Engineering
Department of Information Engineering and Mathematics, Università di Siena, Siena, Italy
110/110 (cum laude).

B.S. in Computer Engineering *April 2014*
Computer and Automation Engineering
Department of Information Engineering and Mathematics, Università di Siena, Siena, Italy
110/110 (cum laude).

EXPERIENCE

Research Associate, NYU Tandon School of Engineering September 2022 - Present

- Investigate Selective Classification and Rejection Option.
- Apply of OOD detection to hardware design.
- Formalize the problem of detecting undesired behaviors in AI (bakcdoors, OOD, misclassifications).

Postdoctoral Fellow, CentraleSupélec and Université Paris-Saclay November 2020 - August 2022

- Investigated the relationship between the out-of-distribution-detection (ODD) problem and the misclassification detection problem.
- Investigated new membership inference attacks in the context of standalone and collaborative Federated Learning.

Ph.D. Candidate, Inria-Saclay and École Polytechnique October 2017 - October 2020

- Reviewed methods to provide privacy via noise injection, mainly Differential Privacy and its derivations.
- Conducted research studies on how Machine Learning can improve Privacy meeting Utility and Quality of Service requirements.
- Investigated the way in which Machine Learning can provide Black Box noise functions that can scale to big data, and only add noise where needed.
- Adopted privacy/utility loss functions from the field of Information Theory to design privacy oriented loss functions for Artificial Neural Networks (ANN), including applications of Generative Adversarial Networks (GANs) paradigm.
- Designed, developed and maintained code repository to support result reproducibility.
- Presented at MILA and UQÀM in Montreal (CA) as visitor student, August-September 2019.
- Received the UFI/UIF Vinci 2018 grant.

Intern at Inria-Saclay June 2017 - October 2017

- Contributed new research topics which combine notions from the fields of Artificial Intelligence and Machine Learning with those of Privacy and Security such like the connection between Information Leakage and Feature Selection.
- Analyzed techniques for Feature Selection in classification problems with a focus on Statistical Filter Methods for their intrinsic link to Information Theory, specifically Mutual Information and Information Entropy.
- Investigated the usage of Entropy, specifically Shannon Entropy and Rényi min-entropy, as metrics for selecting features, with a focus on how they influence the structures of the resulting Decision Trees.

- Designed and structured an experimental pipeline to compare different selection metrics utilizing Python as programming language, the scikit-learn python library (Data analysis and Support Vector Machines), the TensorFlow and Keras libraries (Artificial Neural Networks).
- Presented on statistics oriented techniques for Feature Selection specifically Lasso and InfoGain.

Data Scientist, GlaxoSmithKline plc. September 2016 - April 2017

- Worked with Exploratory Data Analysis Team as graduate intern student.
- Contributed expertise on the engineering and design of databases, and created an internal SQL database for storing protein experiment data.
- Developed R code to manage connections and queries to the internal database wrapping SQL CRUD operations.
- Contributed statistical analysis and code deployment for the STRAIN package and its corresponding publication.
- Continue to collaborate on existing projects focused on the usage of Machine Learning techniques, in particular Support Vector Machines (SVM), for Reverse Vaccinology (ML4RV) and new antigens prediction.

Java Developer, RedEvo Games April 2014 - September 2014

- Contributed to the development of an online strategic card game.
- Deployed code for front-end/back-end application to manage card creation and deletion, and update on a remote server.
- Debugged existing code to correct errors.
- Assisted with front-end client graphic interface using java.awt and java.swing.
- Helped develop back-end server side application handling of front-end/back-end communications via Java Web Services.

TEACHING

EL-GY-9163 - Machine Learning for Cyber-security, New York University, Academic Year 2023-2024.
CSE101 - Computer Programming, École Polytechnique, Academic Year 2018-2019.
CSE103 - Introduction to Algorithms, École Polytechnique, Academic Year 2017-2018.
INF442 - Algorithms for Big Data Analysis, École Polytechnique, Academic Year 2017-2018.

PROGRAMMING SKILLS

Programming Languages: C, C++, Python, Java, R, Bash, SQL, CUDA, Arduino, HTML, PHP.
Frameworks and Libraries: PyTorch, TensorFlow, SciKit, Caret.
Deployment: Git, SVN, Jupyter Notebooks.
Client-Server Technology: RESTful Web Services (RWS), Apache Tomcat.
Document Preparation Systems: LaTeX, Markdown.
Operative Systems: MacOS, Linux (Ubuntu Desktop, Ubuntu Server Edition, Arch Linux), CentOS, Windows.

PUBLICATIONS

Disparate Impact on Group Accuracy of Linearization for Private Inference. [Code] [Paper]
Saswat Das*, Marco Romanelli*, Ferdinando Fioretto
The Forty-first International Conference on Machine Learning - ICML 2024.
* stands for equal contribution.

Beyond the Norms: Detecting Prediction Errors in Regression Models. [Code] [Paper]
Andres Altieri, Marco Romanelli, Georg Pichler, Florence Alberge, Pablo Piantanida
The Forty-first International Conference on Machine Learning - ICML 2024, ***spotlight paper****.*

A Data-Driven Measure of Relative Uncertainty for Misclassification Detection. [Code] [Paper]
Eduardo Dadalto*, Marco Romanelli*, Georg Pichler*, Pablo Piantanida
The Twelfth International Conference on Learning Representations - ICLR 2024.
* stands for equal contribution.

Optimal Zero-Shot Detector for Multi-Armed Attacks. [Paper]
Federica Granese*, Marco Romanelli*, Pablo Piantanida
The 27th International Conference on Artificial Intelligence and Statistics (AISTATS 2024).
* stands for equal contribution.

On the (In)feasibility of ML Backdoor Detection. [Paper]
Georg Pichler, Marco Romanelli, Divya Prakash Manivannan, Prashanth Krishnamurthy, Farshad Khorrami, Siddharth Garg
The 27th International Conference on Artificial Intelligence and Statistics (AISTATS 2024).

Retrieval-Guided Reinforcement Learning for Boolean Circuit Minimization. [Code] [Paper]
Animesh Basak Chowdhury, Marco Romanelli, Benjamin Tan, Ramesh Karri, Siddharth Garg
The Twelfth International Conference on Learning Representations - ICLR 2024.

A Data-Driven Measure of Relative Uncertainty for Misclassification Detection - WS version. [Code] [Paper]
Eduardo Dadalto*, Marco Romanelli*, Georg Pichler*, Pablo Piantanida
NeurIPS 2023 Workshop on Mathematics of Modern Machine Learning.
* stands for equal contribution.

On the Limitation of Backdoor Detection Methods. [Paper]
Georg Pichler, Marco Romanelli, Divya Prakash Manivannan, Prashanth Krishnamurthy, Farshad Khorrami, Siddharth Garg
NeurIPS 2023 Workshop on Backdoors in Deep Learning.

A Minimax Approach Against Multi-Armed Adversarial Attacks Detection. [Paper]
Federica Granese*, Marco Romanelli*, Siddharth Garg, Pablo Piantanida
Submitted.
* stands for equal contribution.

A Halfspace-Mass Depth-Based Method for Adversarial Attack Detection. [Code] [Paper]
Marine Picot, Federica Granese, Guillaume Staerman, Marco Romanelli, Francisco Messina, Pablo Piantanida and Pierre Colombo
Trans. Mach. Learn. Res. 2023.

MEAD: A Multi-Armed Approach for Evaluation of Adversarial Examples Detectors. [Code] [Paper]
Federica Granese, Marine Picot, Marco Romanelli, Francisco Messina and Pablo Piantanida
Proceedings of the 2022 European Conference on Machine Learning and Data Mining (ECML-PKDD).

DOCTOR: A Simple Method for Detecting Misclassification Errors. [Code] [Paper]
Federica Granese*, Marco Romanelli*, Daniele Gorla, Catuscia Palamidessi and Pablo Piantanida
Proceedings of the 35th Conference on Neural Information Processing Systems (NeurIPS 2021), ***spotlight paper****.*
* stands for equal contribution.

Perfectly Accurate Membership Inference by a Dishonest Central Server in Federated Learning. [Code] [Paper]
Georg Pichler, Marco Romanelli, Leonardo Rey Vega and Pablo Piantanida
IEEE Transactions on Dependable and Secure Computing, 2023.

Estimating g-Leakage via Machine Learning. [Code] [Paper]
Marco Romanelli, Konstantinos Chatzikokolakis, Catuscia Palamidessi and Pablo Piantanida
Proceedings of the 27th ACM SIGSAC Conference on Computer and Communications Security (CCS 2020).

Estimating g-Leakage via Machine Learning (Extended abstract).
Marco Romanelli, Konstantinos Chatzikokolakis, Catuscia Palamidessi and Pablo Piantanida
Montreal AI Symposium (MAIS) 2020.

Optimal Obfuscation Mechanisms via Machine Learning. [Code] [Paper]
Marco Romanelli, Catuscia Palamidessi and Konstantinos Chatzikokolakis
Proceedings of the 33rd *IEEE Computer Security Foundations Symposium (CSF 2020).*

Modern Applications of Game-Theoretic Principles (Invited Paper). [Paper]
Catuscia Palamidessi, Marco Romanelli
Proceedings of the 31st LIPICS International Conference on Concurrency Theory, (CONCUR 2020).

Derivation of Constraints from Machine Learning Models and Applications to Security and Privacy. [Paper]
Moreno Falaschi, Catuscia Palamidessi and Marco Romanelli
Proceedings of Recent Developments in the Design and Implementation of Programming Languages 2020.

Generating Optimal Privacy-Protection Mechanisms via Machine Learning (Extended abstract).
Marco Romanelli, Catuscia Palamidessi and Konstantinos Chatzikokolakis
Privacy Preserving Machine Learning Workshop (PPML) co-located with 26th ACM SIGSAC Conference on Computer and Communications Security (CCS 2019).

Feature selection in machine learning: Rényi min-entropy vs Shannon entropy. [Code] [Paper]
Catuscia Palamidessi and Marco Romanelli
Proceedings of the 8th *International Association for Pattern Recognition TC3 Workshop on Artificial Neural Networks in Pattern Recognition, (ANNPR 2018).*

STRAIN: an R package for multi-locus sequence typing from whole genome sequencing data. [Paper]
Mattia Dalsass, Margherita Bodini, Christophe Lambert, Marie-Cecile Mortier, Marco Romanelli, Duccio Medini, Alessandro Muzzi and Alessandro Brozzi
BMC Bioinformatics.

AWARDS

- Received the 2021 UFI/UIF best Ph.D. thesis award.

PROFESSIONAL SERVICE

- **Program committee member**, *The Third AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI-22).* Fully virtual workshop - February 28th and March 1st, 2022.
- **Program committee member**, *The Second AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI-21).* Fully virtual workshop - February 8th and 9th, 2021.
- **Provided external or sub-reviews for**: IEEE Computer Security Foundations Symposium (CSF), Montreal AI Symposium (MAIS), Conference on Neural Information Processing Systems (NeurIPS), IEEE Transactions on Dependable And Secure Computing, IEEE Transactions on Information Forensics and Security, International Conference on Learning Representations (ICLR), Conference on Computer Vision and Pattern Recognition (CVPR).