Ulrich Aïvodji

✉ ulrich.aivodji@etsmtl.ca • aivodji.github.io

Professional Experiences

École de Technologie Supérieure — **Montreal, Canada**
Assistant Professor — *Sept. 2021 – Present*
- Software and Information Technology Engineering Department

Université du Québec à Montréal — **Montreal, Canada**
Postdoctoral researcher — *March 2018–August 2021*
- Advisor : Sébastien Gambs
- Privacy, Interpretability, and Fairness in Machine Learning

Université du Québec à Montréal — **Montreal, Canada**
Visiting researcher — *July–August 2016*
- Advisors : Sébastien Gambs, Jean-Marc Robert
- Secure multi-party computation for linear programming

Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS-CNRS) — **Toulouse, France**
Research Intern — *March–August 2014*
- Distributed and privacy-preserving algorithms for route synchronization
- Using a secure multiparty computation protocol (private set intersection) and multimodal routing algorithms.
- Main programming languages and tech stacks : C++, Python, SWIG.

Dial Technologies — **Casablanca, Morocco**
Software Engineering Intern — *July–August 2013*
- Design and implementation of a Backend as a Service (BaaS) for mobile applications
- Optimized web services consumption using asynchronous networking and data caching.
- Main programming languages and tech stacks : PHP, Java, Android

Multi Information Technologies — **Marrakesh, Morocco**
Software Engineering Intern — *June–August 2012*
- Design and implementation of an Enterprise Resource Planning (ERP) software. Initiation to mobile development for Symbian OS.

Comtel Technologies — **Cotonou, Benin**
Software Engineering Intern — *June–July 2010*
- Initiation to Network Administration

Research Interests

— Machine learning : explainability, fairness, interpretability, privacy, security
— Data privacy : privacy-enhancing technologies, location-based services
— Optimization : combinatorial optimization, transportation

Education

Université Paul Sabatier — **Toulouse, France**
Ph.D. in Computer Science — *2014–2018*
- Dissertation : Privacy-enhancing technologies for ridesharing
- Advisors : Marie-José Huguet, Marc-Olivier Killijian
- Rapporteurs : Josep Domingo-Ferrer, Dominique Feillet
- Committee members : Cyril Briand, Françoise Fessant, Bertrand Le Cun, Benjamin Nguyen

Ecole Nationale des Sciences Appliquées — **Khouribga, Morocco**
Engineer's degree in Software Engineering — *2009–2014*

Awards

Travel Award: 36th International Conference on Machine Learning — *2019*
Travel Award: 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks — *2018*
Ph.D. Scholarship: École Doctorale MITT ($68,000$ euros) — *2014-2017*
Visiting scholar grant: Université Fédérale Toulouse Midi-Pyrénées — *2016*
AMCI Scholarship: Agence Marocaine de Coopération Internationale ($45,000$ dirhams) — *2009-2014*
Medal for exceptional academic achievements: Université Hassan 1^{er} — *2014*
Innov'IT (2nd place): AUSIM Maroc ($40,000$ dirhams) — *2013*
Startup Weekend (1st place): Startup Weekend Casablanca — *2013*
Medal for exceptional academic achievements: Université Hassan 1^{er} — *2013*

Publications

Journals and Conference proceedings

Local Data Debiasing for Fairness Based on Generative Adversarial Training. *Ulrich Aïvodji, François Bidet, Sébastien Gambs, Rosin C. Ngueveu, and Alain Tapp.* Algorithms, 14 (3), 87, 2021

Learning-based Incast Performance Inference in Software-Defined Data Centers. *Kokouvi Benoit Nougnanke, Yann Labit, Marc Bruyere, Simone Ferlin, and Ulrich Aïvodji.* Proceedings of the 24th Conference on Innovation in Clouds, Internet and Networks (ICIN), Virtual conference, 2021. **Best Paper Award**

Privacy in trajectory micro-data publishing : a survey. *Marco Fiore, Panagiota Katsikouli, Elli Zavou, Mathieu Cunche, Françoise Fessant, Dominique Le Hello, Ulrich Aïvodji, Baptiste Olivier, Tony Quertier, and Razvan Stanica.* Transactions on Data Privacy 13 (2), 91 - 149, 2020

Fairwashing : the risk of rationalization. *Ulrich Aïvodji, Hiromi Arai, Olivier Fortineau, Sébastien Gambs, Satoshi Hara, and Alain Tapp.* Proceedings of the 36th International Conference on Machine Learning (ICML), Long Beach, CA, 2019

SRide : a privacy-preserving ridesharing system. *Ulrich Aïvodji, Kévin Huguenin, Marie-José Huguet, and Marc-Olivier Killijian.* Proceedings of the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Stockholm, Sweden,2018

Meeting points in ridesharing : a privacy-preserving approach. *Ulrich Aïvodji, Sébastien Gambs, Marie-José Huguet, and Marc-Olivier Killijian.* Transportation Research Part C : Emerging Technologies, 72, 239-253, 2016

Book chapters

Les enjeux éhiques de l'apprentissage machine. *Ulrich Aïvodji and Sébastien Gambs.* 13 défis de la cybersécurité. Gildas Avoine and Marc-Olivier Killijian (Dir.), CNRS Éditions 2020.

Workshops

GAMIN : an adversarial approach to black-box model inversion. *Ulrich Aïvodji, Sébastien Gambs, and Timon Ther.* AAAI Workshop on Privacy-Preserving Artificial Intelligence, New York, 2020

IOTFLA : a secured and privacy-preserving smart home architecture implementing federated learning. *Ulrich Aïvodji, Sébastien Gambs, and Alexandre Martin.* IEEE Workshop on the Internet of Safe Things, San Francisco, CA, 2019

Privacy-preserving carpooling. *Ulrich Aïvodji, Sébastien Gambs, Marie-José Huguet, and Marc-Olivier Killijian.* 6th International Workshop on Freight Transportation and Logistics, Ajaccio, France, 2015

Pre-prints

Characterizing the risk of fairwashing. *Ulrich Aïvodji, Hiromi Arai, Sébastien Gambs, and Satoshi Hara.* [arXiv:2106.07504]

Model extraction from counterfactual explanations. *Ulrich Aïvodji, Alexandre Bolot, and Sébastien Gambs.* [arXiv:2009.01884]

Hiccups on the road to accountable machine learning : the risk of ethics washing. *Ulrich Aïvodji, Hiromi Arai, Céline Castets-Renard, Sébastien Gambs, and Dominic Martin.*

Learning fair rule lists. *Ulrich Aïvodji, Julien Ferry, Sébastien Gambs, Marie-José Huguet, and Mohamed Siala.* [arXiv:1909.03977]

Teaching

École Nationale de l'Aviation Civile (19.5 hours)

Lecture: Computer Security *Fall 2017*

Institut National des Sciences Appliquées de Toulouse (123.5 hours)

Lab sessions: Algorithms, Complexity, Graph Theory, Database, Data Analysis, Unix *2015-2017*

Talks

Guest Lectures

Privacy and security risks in machine learning: INF8750, Université du Québec à Montréal *2021*

AI & Society: INM6000, Université du Québec à Montréal *2021*

Privacy and security risks in machine learning: IFT6758, Université de Montréal *2020*

Privacy and security risks in machine learning: INF8750, Université du Québec à Montréal *2020*

Privacy and Transparency in Machine Learning: IFT6758, Université de Montréal *2019*

Location privacy: INM6000, Université du Québec à Montréal *2018*

Invited Talk

Fairwashing and model extraction : Two challenges for XAI: Havard University, AI4LIFE research group *2021*

Fairwashing and model extraction : Two challenges for XAI: UTC, CID research group *2021*
Fairwashing and model extraction : Two challenges for XAI: INRIA Lille, MAGNET research group *2021*
Fairwashing and model extraction : Two challenges for XAI: Carrefour DEEL #4, Montreal (Canada) *2021*
Learning Fair Rule Lists: RE·WORK Responsible AI Summit 2019, Montreal (Canada) *2019*
Fairwashing : the risk of rationalization: Université du Québec à Montréal, Montreal (Canada) *2019*
Fairwashing : the risk of rationalization: SÉSÀM 2019, Montreal (Canada) *2019*
Transparency and privacy in the era of big-data: Toulouse Data Science Meetup, Toulouse (France) *2017*
Privacy Enhancing Technologies for ridesharing: Université du Québec à Montréal, Montreal (Canada) *2016*
Privacy-preserving two-points synchronization for ridesharing: IRISA, Rennes (France) *2015*

Academic Services

Program committee

ICML Workshop on Algorithmic Recourse: *2021*

Reviewer

Conference on Neural Information Processing Systems (NeurIPS): *2021*
International Conference on Machine Learning (ICML): *2021*
IEEE Transactions on Knowledge and Data Engineering: *2020*
IEEE Transactions on Computers: *2020*
IEEE Transactions on Mobile Computing: *2020*
Privacy Enhancing Technologies Symposium (PETS): *2020*
IEEE Software: *2019*
Network Management: *2018*

Review assistance

IJCAI-ECAI: *2018*

Software Skills

Programming: Python, C++, Java, C#, Scala, R, Julia
Machine learning & Optimization: Scikit-learn, Pytorch, Tensorflow, Flux, Or-tools, CPLEX, JuMP

Open source projects and popular science

Volunteering

Mentor at UpstartED: coaching college students on privacy-preserving ML projects *Since Feb. 2020*

Software

Co-author of FairCORELS: open-source library for learning fair rule lists *2019*
Co-author of LaundryML: open-source library for adversarial explainable AI *2019*

Popular Science

Fête de la science: Demo of a privacy-preserving ride-sharing system developed during my Ph.D. *2016*
Ma thèse en 180 secondes: Scientific vulgarization challenge of presenting Ph.D. research in 180 seconds *2015*
Open Source Days: Co-design the website of the event. Demo of an AIML-based chatbot *2012*

Projects

DEEL(Dependable & Explainable Learning) **Montreal, Canada**
CRIAQ *August 2020 – Present*
— DEEL is an international collaboration project (with among others IRT Saint Exupéry, IVADO, CRIAQ and ANITI) for the development of artificial intelligence in critical systems.
— It focuses on *dependability*, *explainability*, *certifiability* and *privacy* challenges in critical systems that embedded predictive models.
— Role : Contributor on the privacy and explainability research axes.

Privacy and Ethics in machine learning **Montréal, Canada**
Privacy Commissioner of Canada *April 2020 – Present*
— This project aims to understand the tensions and convergences between privacy and ethical issues such as equity, explainability, interpretability, security and accountability in the responsible development of artificial intelligence.
— Role : Co-PI for UQAM.

ADAGE(Anonymous mobile traffic DAta GEneration) **Toulouse, France**
Orange *Sept. 2017 – Mars. 2018*

— Development of privacy-preserving techniques for call detail records analysis
— Role : Contributor on the analysis of state of the art techniques

PlayMob **Toulouse, France**
LAAS-CNRS *Oct. 2014 – Jan. 2018*
— Development of a web platform to promote results on various problems of route calculations and shared mobility.
— Role : Principal developer
— Technologies : C++, Python, Django, SWIG.

AMORES(Architecture for MObiquitous REsilient Systems) **Toulouse, France**
Agence Nationale de la Recherche (ANR) *Mars 2014 – Jan. 2016*
— Development of privacy-preserving location-based services
— Role : Developer of privacy-preserving algorithms for route synchronization.

Hakifach **Khouribga, Morocco**
Personal project *Jan. 2013 – Jan. 2014*
— Development of *Hakifach* : a *How-To* web platform aiming to assist citizens in carrying out their administrative procedures.
— Hakifach present the different steps involved in each procedure through various channels : texts, images, audio, videos, and chatbot.
— Hakifach won the 2nd prize of the Innov'IT competition : a Moroccan national competition for innovation in information and communication technologies.
— Role : Principal co-developer
— Technologies : PHP, AIML.