CURRICULUM VITAE

Raouf Kerkouche

+33-758-069-385 ✉ raouf.kerkouche@cispa.de Website LinkedIn Google Scholar

Address: 13 Place du Forum, 57000 Metz, France.

*I am a **Dual Algerian-French citizen**.*

1) Professional history

Education and Postdoctoral Training

01/09/2021 – Now
Postdoctoral Researcher
CISPA Helmholtz Center for Information Security, Saarbrücken, Germany.
Research on trustworthy machine learning with a focus on Privacy & Security
Advisor: Mario Fritz.

01/01/2018 – 30/06/2021
Ph.D. in Computer Science
Inria Centre at Grenoble Alpes University, Grenoble, France.
Thesis: "Differentially Private Federated Learning for Bandwidth and Energy Constrained Environments"
Advisor: Claude Castelluccia and Pierre Genevès.
Thesis committee (07/07/2021): Massih-Reza Amini, Emiliano De Cristofaro, Reza Shokri, Aurélien Bellet, Marc Tommasi, Claude Castelluccia, and Pierre Genevès.

01/09/2015 – 01/09/2017
M.Sc. in Computer Science
Pierre and Marie-Curie University, Paris VI, France.
Paris-Sud University, Paris XI, France.
M.Sc. awarded in September 2017.

01/09/2012 – 30/06/2015
B.Sc. in Computer Science
University of Sciences and Technology Houari-Boumediene, Algiers, Algeria.
B.Sc. awarded in August. 2015.

Previous professional experiences

Start	End	Institution	Position and status
01/10/2017	31/12/2017	Inria Center of the University of Grenoble Alpes	Research Engineer
01/03/2017	31/08/2017	IMT Atlantique	Intern
01/05/2016	31/07/2016	CentraleSupélec	Intern

Number of years of professional research experience after the PhD: 3 years, 2 months (as of September 1st, 2021)

2) Supervision of students and early-stage researchers

2023-2024
- **Doctorate Student:** Tejumade Afonja.
- **Affiliation:** CISPA - Helmholtz Center for Information Security.
- **Main Supervisor** / **Percentage** Mario Fritz – 50%.
- **My Role** / **Percentage:** Co-supervisor – 50%.
- **Subject:** Tejumade is currently engaged in the development of synthetic tabular data generation methods that prioritize privacy. Our ongoing project leverages the capabilities of advanced large language models for this purpose. We are innovating new approaches to ensure data generation is conducted privately, employing differential privacy techniques. Simultaneously, we are focusing on optimizing the balance between privacy and utility in this process.

2023-2024
- **Doctorate Student:** Hui-Po Wang.
- **Affiliation:** CISPA - Helmholtz Center for Information Security.
- **Main Supervisor** / **Percentage** Mario Fritz – 50%.
- **My Role** / **Percentage:** Co-supervisor – 50%.
- **Subject:** We are supervising Hui Po Wang's research on federated architectures, which emphasize bandwidth efficiency, privacy, and adaptability in real-world scenarios with heterogeneous, non-independent and identically distributed (non-IID) data across clients. Our innovative approach, focused on bandwidth efficiency and privacy, deviates from the traditional method where clients send global model updates after local training. Instead, we use synthetic data to more effectively approximate the global loss, a technique that proves particularly advantageous in non-IID settings.

2022-2024
- **Doctorate Student:** Shadi Rahimian.
- **Affiliation:** CISPA - Helmholtz Center for Information Security.
- **Main Supervisor** / **Percentage** Mario Fritz – 50%.
- **My Role** / **Percentage:** Co-supervisor – 50%.
- **Subject:** Survival analysis, also known as time-to-event analysis, is focused on modeling and predicting the duration until the occurrence of a significant event within a given population or individual. This method is particularly relevant in medical settings, where it is used to estimate critical events such as death, metastasis, or other significant health changes. Shadi is at the forefront of enhancing this field by developing methodologies for the release of estimators through the application of differential privacy. These advanced techniques are crucial in accurately identifying and understanding survival patterns within patient cohorts, thereby enriching survival analysis with robust and privacy-preserving insights.

2022-2023
- **Doctorate Student:** Dingfan Chen.
- **Affiliation:** CISPA - Helmholtz Center for Information Security.
- **Main Supervisor** / **Percentage** Mario Fritz – 50%.
- **My Role** / **Percentage:** Co-supervisor – 50%.
- **Subject:** Generating synthetic data under differential privacy protocols ensures theoretical protection for the privacy of user data. This assurance is likely to encourage user participation in creating these datasets. Such synthetic data proves invaluable for tasks like training models and extracting vital insights, including statistical analysis of the original data. However, a major challenge emerges due to the degradation in data quality, a consequence of the noise inherent in differential privacy techniques. In collaboration with Dingfan Chen, we have endeavored not only to devise innovative solutions to this issue but also to spotlight the limitations inherent in current generative methods. These methods often prioritize one aspect – typically the utility for downstream tasks – while neglecting crucial statistical or specific characteristics of the original, private data.

3) Responsibilities

Program Committee (Conferences)

2025
- 28th International Conference on Artificial Intelligence and Statistics (AISTATS)
- 3rd IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)

2024
- 31th ACM Conference on Computer and Communications Security (CCS)
- 27th International Conference on Artificial Intelligence and Statistics (AISTATS)
- 2nd IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)

2023
- 26th International Conference on Artificial Intelligence and Statistics (AISTATS)
- 1st IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)

Program Committee (Workshops)

2023
- 16th ACM Workshop on Artificial Intelligence and Security (AISec)
- Algorithmic Fairness through the Lens of Time (AFT)

2022
- Algorithmic Fairness through the Lens of Causality and Privacy (AFCP)
- 3rd AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI)

Journals Reviewer

2023
- Transactions on Machine Learning Research (TMLR)
- Nature Medicine (NM)

2022
- ACM Transactions on Privacy and Security (TOPS)
- European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD)

External Reviewer

2025 - 13th International Conference on Learning Representations (ICLR)
2023 - 6th IEEE European Symposium on Security and Privacy (EuroS&P)

Organized Competitions

2025 - Inference Attacks Against Document VQA (SaTML 2025 Competition).
Description: As part of the European Lighthouse on Secure and Safe AI (ELSA) project, I am contributing to the organization of this competition, which will be launched on October 15, 2024. The competition challenges participants to develop inference attacks aimed at extracting sensitive information from Document Visual Question Answering (DocVQA) models, which are particularly vulnerable to privacy breaches. In collaboration with my team, I have been involved in writing the competition proposal, setting attack baselines, and designing the competition framework. The goal is to explore real-world privacy risks and assess the robustness of differential privacy in multimodal models.

2023 - Privacy Preserving Federated Learning Document VQA (NeurIPS 2023 Competition).
Description: As part of the European Lighthouse on Secure and Safe AI (ELSA) project, I played an active role in establishing the first privacy attack challenge focused on multi-modal models for the DocVQA task. Initially, I participated in preliminary discussions about the necessity and potential impact of organizing such a challenge. Subsequently, I contributed to the development of the challenge platform. This included preparing the base model, creating its privacy-enhanced version, and conducting a privacy analysis on the latter. Our challenge proposal was submitted to NeurIPS, one of the premier conferences in the field of artificial intelligence, where it was accepted. Following the submission, I was involved in evaluating the participants' submissions.

4) Mobility

2023
- **Visiting Postdoc at The Computer Vision Center (CVC).**
- **City/Country:** Barcelona, Spain
- **Type:** Different laboratory
- **Duration:** 1 week
- **Research:** Privacy-Aware Document Visual Question Answering
- **Laboratory:** The Vision and Language research group.
- **Hosted by:** Dimosthenis Karatzas
- **Funding:** ELSA.

2018
- **Visiting Ph.D. Student at Inria centre Lille (Inria).**
- **City/Country:** Lille, France
- **Type:** Different laboratory
- **Duration:** 2 weeks
- **Research:** Private Collaborative Learning
- **Laboratory:** Magnet
- **Hosted by:** Marc Tommasi and Aurélien Bellet
- **Funding:** Cross Disciplinary Project (CDP) - IDEX.

5) Teaching

2023-2024
- **Teaching Assistant and Lecturer on Machine Learning in Cybersecurity**
- **Institution / Program:** Saarland University and Leibniz University, Master degree.
- **Duration / Language:** 80 hours, English
- **Content:** Machine Learning (ML) for improving security, Attacks on ML, Defenses for ML, ML and Privacy, Security of Large Language Models.

6) Visibility

2024 - **Tutorials:** We are organizing a tutorial on Private, Collaborative Learning in Document Analysis which is hosted at the International Conference on Document Analysis and Recognition. (ICDAR)

2023 - **Awards:** Notable reviewer award (SaTML)
- **Invited Talk:** Privacy-Preserving Collaborative Deep Learning. In: PreMeDICaL Inria-Inserm team.

2021 - **Invited Talk:** On The Challenges of Practical Federated Learning. In: Data Science Law Forum 3.0. **Description:** Invited by Microsoft to contribute as a distinguished speaker at the Data Science & Law Forum 3.0, a prestigious event that has carved out a niche for fostering collective insights and advancing knowledge on the principles of responsible AI since 2018. The 2021 edition focused on the operational aspects of AI, emphasizing the practical implementation of artificial intelligence and advocating for the establishment of comprehensive guidelines to ensure AI systems are robust, trustworthy, and regulated. Engaged with an esteemed assembly of professionals from academia, civil society, policymaking, and legal sectors to enrich discussions on the future of AI governance.

7) Other relevant information

Participation in Research Projects

ELSA
- **Title:** European Lighthouse on Secure and Safe AI.
- **Partners:** 26 European institutions (e.g., CISPA, Inria, CVC, NVIDIA Switzerland, EPFL).
- **Role:** Project member.
- **Contributions:** I have been a member since the launch of this ambitious and immensely exciting project. I have contributed to numerous work packages by conducting research [2], organizing competitions, and writing deliverable reports. Additionally, I am consistently available to participate in the various events associated with this project.

PRO-GENE-GEN
- **Title:** Protecting Genetic Data with Synthetic Cohorts from Deep Generative Models.
- **Partners:** 2 academic institutions (CISPA and DZNE)
- **Role:** Project member.
- **Contributions:** When I joined CISPA, the project was already underway. I contributed scientifically by collaborating with Dingfan Chen on developing methods for generating private synthetic data. This collaboration resulted in the publication of several research papers at prestigious international conferences, such as NeurIPS (CORE: A*) and PETS (CORE: A).

LOKI
- **Title:** Integrated Early Warning System for Local Recognition, Prevention, and Control for Epidemic Outbreaks.
- **Partners:** 6 academic institutions (CISPA, HZI, AÖGW, FZJ, DLR and UFZ)
- **Role:** Project member.
- **Contributions:** The goal of this project is to establish a platform for pandemic management over the short, medium, and long term. Consequently, the platform will oversee the entire process, from the generation of data at the hospital level to its transmission to a system. This system will either train predictive models that can be reused in the future or perform direct analysis on the data. I have been part of this project from the beginning, focusing on evaluating the privacy risks associated with handling such highly sensitive medical data. Following this evaluation, I proposed practical solutions that come with theoretical guarantees, detailing how this data can be securely shared on the platform without compromising privacy.

TFDA
- **Title:** Trustworthy Federated Data Analytics.
- **Partners:** 2 academic institutions (CISPA and DKFZ)
- **Role:** Project member.
- **Contributions:** This project had already begun when I arrived at CISPA. The work of Shadi Rahimian, who worked under my supervision on this project, resulted in two research papers, one published and the other under submission.

8) Complete list of contributions

1. Publication policy

My publication strategy emphasizes submitting to top-tier international conferences that hold an A or A* ranking. Given my research focus in the intersecting fields of privacy, security, and machine learning, I am open to contributing to either specialized conferences in artificial intelligence or those dedicated to security and privacy.

2. Publications

Conference proceedings are the main publication venue in Computer Science.

2.1 International journals

- Dingfan Chen, **Raouf Kerkouche**, & Mario Fritz. A Unified View of Differentially Private Deep Generative Modeling. *Accepted at TMLR (Survey Certification)*, 2024.

2.2 Reviewed international conferences

- Rubèn Pérez Tito, Khanh Nguyen, Marlon Tobaben, **Raouf Kerkouche**, Mohamed Ali Souibgui, Kangsoo Jung, Lei Kang, Ernest Valveny, Antti Honkela, Mario Fritz and Dimosthenis Karatzas. "Privacy-Aware Document Visual Question Answering.". Proceedings of the 18th International Conference on Document Analysis and Recognition (ICDAR 2024).

- Hui-Po Wang, Dingfan Chen, **Raouf Kerkouche** and Mario Fritz. "FedLAP-DP: Federated Learning by Sharing Differentially Private Loss Approximations.". Proceedings of the 24th Privacy Enhancing Technologies Symposium (PETS 2024).

- Dingfan Chen, Marie Oestreich, Tejumade Afonja, **Raouf Kerkouche**, Matthias Becker, Mario Fritz. (2024). "Towards Biologically Plausible and Private Gene Expression Data Generation". Proceedings of the 24th Privacy Enhancing Technologies Symposium (PETS 2024).

- Dingfan Chen, **Raouf Kerkouche**, & Mario Fritz. Private set generation with discriminative information. Advances in Neural Information Processing Systems (NeurIPS 2022), 35, 14678-14690.

- Shadi Rahimian, **Raouf Kerkouche**, Ina Kurth, & Mario Fritz. Practical challenges in differentially-private federated survival analysis of medical data. In Conference on Health, Inference, and Learning (CHIL 2022). PMLR.

- **Raouf Kerkouche**, Gergely Ács, Claude Castelluccia, & Pierre Genevès. Constrained differentially private federated learning for low-bandwidth devices. In Uncertainty in Artificial Intelligence (UAI 2021). PMLR.

- **Raouf Kerkouche**, Gergely Ács, Claude Castelluccia, & Pierre Genevès, "Compression Boosts Differentially Private Federated Learning," in 2021 IEEE European Symposium on Security and Privacy (IEEE EuroS&P 2021).

- **Raouf Kerkouche**, Gergely Ács, Claude Castelluccia, & Pierre Genevès. 2021. Privacy-preserving and bandwidth-efficient federated learning: an application to in-hospital mortality prediction. In Proceedings of the Conference on Health, Inference, and Learning (CHIL 2021). Association for Computing Machinery, New York, NY, USA, 25–35.

- **Raouf Kerkouche**, Réda Alami, Raphaël Féraud, Nadège Varsier, & Patrick Maillé. (2018, June). Node-based optimization of LoRa transmissions with Multi-Armed Bandit algorithms. In 2018 25th International Conference on Telecommunications (ICT) (pp. 521-526). IEEE.

2.3 Reviewed international workshops

- Shadi Rahimian, **Raouf Kerkouche**, Ina Kurth and Mario Fritz. Private and Collaborative Kaplan-Meier Estimators. In Proceedings of the 23rd Workshop on Privacy in the Electronic Society (WPES '24).

- **Raouf Kerkouche**, Gergely Ács, & Mario Fritz. 2023. Client-specific Property Inference against Secure Aggregation in Federated Learning. In Proceedings of the 22nd Workshop on Privacy in the Electronic Society (WPES '23). Association for Computing Machinery, New York, NY, USA, 45–60.

2.4 Reviewed national workshops

- **Raouf Kerkouche** and Claude Castelluccia. "Privacy-Preserving Processing of Medical Data." Atelier sur la Protection de la Vie Privée (2018).

2.5 Research reports and publications under review

- **Raouf Kerkouche**, Gergely Ács and Claude Castelluccia. "Federated Learning in Adversarial Settings." ArXiv abs/2010.07808 (2020).

2.6 Ongoing Projects

- I am working on an unsupervised membership attack on multi-modal models in white-box and black-box settings.
- I am developing a new differentially private in-context learning approach for large language models (LLMs).
- I am designing a new type of privacy attack on new generative models, which can potentially be exploited to enhance the performance of both privacy and security attacks.

3. Socio-economic impact and transfer

Research Collaboration Whithin MELLODY Project

- **Description of transfer:** Knowledge transfer (research collaboration). During my doctoral studies, I collaborated with one of the Principal Investigators involved in the European Melloddy project. This project focused on developing a federated learning platform for various pharmaceutical companies, facilitating drug discovery for different diseases. A major concern in the pharmaceutical industry is the protection of proprietary information, particularly regarding the molecules they research. This confidentiality is vital, as it directly influences their business model. In response to these challenges, I proposed a solution that was published in the proceedings of the Uncertainty in Artificial Intelligence (UAI) conference. This solution, implemented in the Melloddy platform, demonstrated promising results. It effectively balanced utility and privacy, guided by the principles of differential privacy..
- **Modalities of the transfer:** We had weekly meetings with Gergely Acs and after submitting our paper to UAI. I provided the code to Gergely Acs to evaluate the solution using real data from various pharmaceutical companies that were involved in the project.
- **Personal contribution:** My proposed solution for federated learning significantly enhances bandwidth efficiency in both communication directions — from server to client and vice versa — achieving up to a 99% improvement. Moreover, it offers robust theoretical guarantees of privacy through the implementation of differential privacy. This is accomplished while maintaining a remarkably high level of utility.;
- **Benefits and impact of the transfer:**This study has showcased the feasibility of collaboratively learning an accurate model while ensuring differential privacy. Additionally, the remarkable reduction of bandwidth usage enhances its practicality. The findings of our research have been published in the proceedings of the Conference on Uncertainty in Artificial Intelligence (UAI).

Research Collaboration With Orange Labs – Lannion

- **Description of transfer:** Knowledge transfer (research collaboration). The expanding application of Low Power Wide Area Networks (LPWANs) is driven by their benefits in low cost, energy efficiency, and extended coverage. Despite the growing interest from industry and network operators, LPWANs encounter challenges in energy consumption, network coverage, and service quality. This paper focuses on enhancing LoRaWAN (Long Range Wide Area Network) performance, a prominent LPWAN technology. During my master's internship at IMT Atlantique, in collaboration with Orange Labs, we developed an innovative approach. Our solution enables nodes to use lightweight learning methods, specifically multi-armed bandit algorithms, for optimizing communication parameters such as spreading factor and emission power. Through comprehensive simulations, we demonstrate that these learning methods effectively balance energy use and packet loss, outperforming the Adaptive Data Rate (ADR) algorithm. The ADR algorithm typically adjusts spreading factors and transmission powers based on Signal to Interference and Noise Ratio (SINR) values. Our findings indicate a significant advancement in managing LPWANs' operational efficiencies.
- **Modalities of the transfer:** My internship was funded by Orange Labs. Biweekly meetings were held with my supervisor at IMT Atlantic, Patrick Maillé, and my supervisor at Orange Labs, Raphaël Féraud.
- **Personal contribution:** I developed and executed a range of multi-armed bandit algorithms, subsequently comparing their performance against the ADR (Adaptive Data Rate) algorithm. The outcomes from this comparative analysis distinctly demonstrate the superiority of my methodologies. Following these findings, I submitted a detailed research paper to the International Conference on Telecommunications (ICT) for peer review. Additionally, I collaborated with Orange Labs, providing them with the code for practical application and real-world testing.
- **Benefits and impact of the transfer:** I pioneered the application of machine learning techniques, particularly multi-armed bandit algorithms, in optimizing Low Power Wide Area Network (LPWAN) technologies. This innovative approach was detailed in my research publication [1]. Additionally, my work has had practical implications, as it's been implemented in experimental networks overseen by Orange, demonstrating its effectiveness in real-world scenarios.

9) Referees

Claude Castelluccia
Research Director, Inria
Founding-member of the
Privatics Group,
INRIA Rhone-Alpes
✉ claude.castelluccia@inria.fr

Mario Fritz
Faculty CISPA Helmholtz Center
for Information Security
Professor at Saarland University
✉ fritz@cispa.de

Antti Honkela
Professor at the University of Helsinki,
Coordinating Professor of Research Programme in Privacy-preserving and Secure AI,
Finnish Center for Artificial Intelligence (FCAI)
✉ antti.honkela@helsinki.fi

Dimosthenis Karatzas
Professor at the Universitat Autónoma de Barcelona
Associate director of the Computer Vision Centre
Co-Director of the ELLIS Unit Barcelona
✉ dimos@cvc.uab.es

Pierre Genevès
Research Director, CNRS
Leader of the Tyrex research team,
INRIA Rhone-Alpes
✉ pierre.geneves@inria.fr

Mérouane Debbah
Director of the KU 6G Research,
Khalifa University
✉ merouane.debbah@ku.ac.ae

Gergely Ács
Associate Professor,
CrySyS Lab, Budapest University
of Technology and Economics
✉ acs@crysys.hu

Bibliography

[1] Raouf Kerkouche, Reda Alami, Raphaël Féraud, Nadege Varsier, and Patrick Maillé. Node-based optimization of lora transmissions with multi-armed bandit algorithms. In *2018 25th International Conference on Telecommunications (ICT)*, pages 521–526, 2018.

[2] Rubèn Tito, Khanh Nguyen, Marlon Tobaben, Raouf Kerkouche, Mohamed Ali Souibgui, Kangsoo Jung, Lei Kang, Ernest Valveny, Antti Honkela, Mario Fritz, et al. Privacy-aware document visual question answering. *arXiv preprint arXiv:2312.10108*, 2023.