Arnaud Grivet Sébert

+33 6 17 75 53 50
arnaud.grivetsebert@gmail.com

EDUCATION

CEA-LIST — **Saclay, France**
PhD student — *2020 – 2023*
- **Title:** Combining differential privacy and homomorphic encryption for privacy-preserving collaborative machine learning
- **Advisors:** Renaud Sirdey and Cédric Gouy-Pailler
- **Publications:** [1, 2, 3, 4]

Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) — **Rio de Janeiro, Brazil**
Double degree with Ecole Centrale de Paris — *2015 - 2016*
- Computer science (AI, logic, programming)

Ecole Centrale de Paris — **Châtenay-Malabry, France**
Diplôme d'ingénieur (master level) — *2012 - 2014*

Université Paris-Sud (Paris XI) — **Orsay, France**
Bachelor in mathematics — *2012 - 2013*

Lycée privé Sainte Geneviève — **Versailles, France**
*"Classe préparatoire" MPSI-MP** — *2010 - 2012*
- Intensive courses (mostly mathematics and physics) to prepare to entrance exams to French engineering schools

EXPERIENCE

LIX, Ecole Polytechnique — **Palaiseau, France**
Post-doctoral researcher — *2024 – now*
- **Context**: Partnership between Ecole Polytechnique and Crédit agricole (French bank)
- Privacy-preserving machine learning: privacy and quantization, privacy for large language models
- **Advisors**: Catuscia Palamidessi and Sonia Vanier

LIP6, Sorbonne Université — **Paris, France**
Research engineer — *March 2019 – September 2019*
- **Context**: French National Research Agency (ANR) project COCORICO-CODEC (Computation, Communication, Rationality, and Incentives in Collective and Cooperative Decision) on computational social choice
- Preference and ranking aggregation: theoretical studies and implementation of voting rules
- **Publications**: [5, 6]

CEA-LIST — **Saclay, France**
Research engineer — *March 2017 - November 2018*
- **Context**: European project C-BORD (effective Container inspection at BORDer control points) whose aim was to detect illicit substances in containers transiting in ports and customs
- Explainable material classification from imprecise chemical data via fuzzy rules
- **Publications**: [7, 8]

Tecgraf institute, PUC-Rio — **Rio de Janeiro, Brazil**
Software developer intern — *October 2015 - June 2016*
- Development of a software for the visualization of oil reservoirs

TEACHING

Télécom SudParis — **Evry, France**
Teacher — *December 2021*
- Designed and taught a 3h course about attacks and defenses on data privacy in deep learning

INSTN — **Saclay, France**
Teacher — *December 2020 and December 2021*
- Designed and taught a 1h30 course about attacks and defenses on data privacy in deep learning

CentraleSupélec — **Gif-sur-Yvette, France**
Student project supervisor — *October 2017 - June 2018*
- Supervised a team of four first-year students on a project proposed as a CEA researcher on material classification using genetic algorithms

PUBLICATIONS

[1] A. Grivet Sébert, M. Zuber, O. Stan, R. Sirdey, and C. Gouy-Pailler, "A probabilistic design for practical homomorphic majority voting with intrinsic differential privacy," in *Proceedings of the 11th Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC)*, pp. 47–58, 2023.

[2] A. Grivet Sébert, R. Sirdey, O. Stan, and C. Gouy-Pailler, "Combining homomorphic encryption and diferential privacy in federated learning," in *Annual Conference on Privacy, Security and Trust (PST)*, 2023.

[3] A. Madi, O. Stan, A. Mayoue, A. Grivet-Sébert, C. Gouy-Pailler, and R. Sirdey, "A secure federated learning framework using homomorphic encryption and verifiable computing," in *Reconciling Data Analytics, Automation, Privacy, and Security: A Big Data Challenge (RDAAPS)*, pp. 1–8, IEEE, 2021.

[4] A. Grivet Sébert, R. Pinot, M. Zuber, C. Gouy-Pailler, and R. Sirdey, "Speed: Secure, private, and efficient deep learning," *European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD) journal track, Machine Learning Springer journal*, vol. 110, no. 4, pp. 675–694, 2021.

[5] A. Grivet Sébert, N. Maudet, P. Perny, and P. Viappiani, "Preference aggregation in the generalised unavailable candidate model," in *International Conference on Algorithmic Decision Theory (ADT 2021)*, pp. 35–50, Springer, 2021.

[6] A. Grivet Sébert, N. Maudet, P. Perny, and P. Viappiani, "Rank aggregation by dissatisfaction minimisation in the unavailable candidate model," in *20th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, 2021.

[7] A. Grivet-Sébert and J.-P. Poli, "Fuzzy rule learning for material classification from imprecise data," in *Information Processing and Management of Uncertainty in Knowledge-Based Systems (IPMU)*, 2018.

[8] A. Grivet-Sébert and J.-P. Poli, "Material classification from imprecise chemical composition: Probabilistic vs possibilistic approach," in *IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, 2018.

LANGUAGES

- **French**: native
- **English, Portuguese**: fluent
- **Spanish**: intermediary

INTERESTS AND HOBBIES

Environmental issues, linguistics, rock climbing