# Raouf Kerkouche

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

## Research Interests

- Trustworthy Machine Learning
- Collaborative Learning

## Education and Postdoctoral Training

**CISPA Helmholtz Center for Information Security** — Sarrebruck, Germany
*Postdoctoral Researcher* — *2021 – Currently*

**Grenoble Alpes University** — Grenoble, France
*Ph.D. in Computer Science* — *2018 – 2021*

**Pierre and Marie-Curie University (Paris VI)** — Paris, France
*MSc in Network and Security, with Honors* — *2016 – 2017*

**Paris-Sud University (Paris XI)** — Orsay, France
*MSc in Computer Science, with Honors* — *2015 – 2016*

**University of Sciences and Technology Houari-Boumediene** — Algiers, Algeria
*BSc in Computer Science, with Honors* — *2012 – 2015*

## Publications

- ”Client-specific Property Inference against Secure Aggregation in Federated Learning”,
  **Raouf Kerkouche**, Gergely Ács, Mario Fritz. Preprint (paper under submission), [PDF].

- ”Fed-GLOSS-DP: Federated, Global Learning using Synthetic Sets with Record Level Differential Privacy”,
  Hui-Po Wang, Dingfan Chen, **Raouf Kerkouche**, Mario Fritz. Preprint (paper under submission), [PDF].

- ”Private Set Generation with Discriminative Information”,
  Dingfan Chen, **Raouf Kerkouche**, Mario Fritz. Proceedings of the 36th Conference on Neural Information Processing Systems (NeurIPS 2022), [PDF].

- ”Practical Challenges in Differentially-Private Federated Survival Analysis of Medical Data”,
  Shadi Rahimian, **Raouf Kerkouche**, Ina Kurth, Mario Fritz. Proceedings of the ACM Conference on Health, Inference and Learning (CHIL 2022), [PDF].

- ”Constrained Differentially Private Federated Learning for Low-bandwidth Devices”,
  **Raouf Kerkouche**, Gergely Ács, Claude Castelluccia and Pierre Genevès. Proceedings of the 37th Conference on Uncertainty in Artificial Intelligence (UAI 2021), [PDF].

- ”Compression Boosts Differentially Private Federated Learning”,
  **Raouf Kerkouche**, Gergely Ács, Claude Castelluccia and Pierre Genevès. Proceedings of the 6th IEEE European Symposium on Security and Privacy (IEEE EuroS&P 2021), [PDF].

- ”Privacy-Preserving and Bandwidth-Efficient Federated Learning: An Application to In-Hospital Mortality Prediction”,
  **Raouf Kerkouche**, Gergely Ács, Claude Castelluccia and Pierre Genevès. Proceedings of the ACM Conference on Health, Inference and Learning (CHIL 2021), [PDF].

- ”Federated Learning in Adversarial Settings”,
  **Raouf Kerkouche**, Gergely Ács, Claude Castelluccia. Preprint (2020), [PDF].

## Awards

- SaTML 2023 - Notable reviewer award

## Service

- **PC Member (Conferences):** AISTATS 2023, IEEE SaTML 2023
- **PC Member (Workshops):** AAAI PPAI 2022
- **Journals Reviewer:** ACM TOPS 2022, ECML PKDD 2022 (journal track)
- **External Reviewer:** IEEE EuroS&P 2021

## Invited Talks

- Data Science Law Forum 3.0: “Operationalizing Responsible AI”, Organized by Microsoft. On The Challenges of Practical Federated Learning, 2021.

## Referees

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

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

Dr. Gergely ÁCS
Assistant Professor
CrySyS Lab,
Budapest University of Technology
and Economics (BME)
✉ acs@crysys.hu