
RESEARCH INTERESTS

Adversarially robust distributed learning; Byzantine fault tolerance; data ownership verification and digital watermarking; communication-efficient learning; reproducible machine learning research.

RESEARCH EXPERIENCE

Research Intern, Byzantine-Resilient Distributed Learning

Apr–Oct 2026

CMAP, École Polytechnique, France | ATLAS chair

Supervised by El-Mahdi El-Mhamdi, with Peva Blanchard and Sébastien Rouault.

- Co-developed **Krum**, an open-source Python/PyTorch library for evaluating distributed learning under Byzantine attacks, released on PyPI under the MIT licence.
- Implemented gradient aggregation rules, a zero-copy model wrapper, neural network architectures and centralised training simulations.
- Reproduced key experimental behaviours from NeurIPS 2017, ICML 2018 and ICML 2023 protocols, with documented adaptations, including a reduced-scale decentralised MoNNA case study.
- Wrote component tests, tutorials and reference documentation, and configured continuous integration and software release workflows.
- Compared related research libraries and contributed to the companion manuscript describing Krum and its experimental methodology.

EDUCATION

Incoming PhD Researcher

Starting Nov 2026

CMAP, École Polytechnique, France | ATLAS chair

Research topic: trade-offs between adversarial robustness, data ownership verification and efficient learning. Initial project on the Byzantine fault tolerance of signSGD.

Supervisor: El-Mahdi El-Mhamdi. Co-directors: Katia Meziani and Vladimir Kostic. Co-advisors: Peva Blanchard and Sébastien Rouault.

Master's in Statistical and Financial Engineering (M2)

2025–2026

Université Paris Dauphine–PSL, France | Data Science track

Selected coursework: learning theory, advanced machine learning, deep learning, reinforcement learning and natural language processing.

Master's thesis: *Byzantine-Resilient Aggregation for Distributed Learning: The Krum Library*.

Master's in Mathematics and Applications (M1)

2024–2025

Université Paris Dauphine–PSL, France | Statistics track

Selected coursework: statistical learning, generalised linear models, Monte Carlo methods, nonparametric statistics, time series and numerical optimisation.

BSc in Mathematics

2021–2024

Université Paris-Saclay, Orsay, France

MANUSCRIPT IN PREPARATION

Sébastien Rouault, **Arthur Danjou**, Mohamad-Ammar Said, Peva Blanchard and El-Mahdi El-Mhamdi.
Krum, the Library: Automated Byzantine Machine Learning Experiments on Python with Orchestration. 2026.
In preparation for the Machine Learning Open Source Software track of the *Journal of Machine Learning Research*. Code and documentation.

SELECTED RESEARCH & ACADEMIC PROJECTS

Krum: Byzantine-Resilient Distributed Learning **2026**

Co-developed a Python/PyTorch research framework combining robust aggregation, adversarial attacks, published-protocol simulations and reproducible experiment orchestration.

Byzantine-Robust Aggregation Reproduction **2026**

Implemented SignGuard, Multi-Krum and MoNNA, with ALIE and Fall of Empires attacks, from scratch in PyTorch. Documented implementation pitfalls that informed the design of Krum.

Generalisation Bounds for Two-Layer ReLU Networks **M2**

Studied Rademacher complexity bounds using symmetrisation and the positive homogeneity of ReLU networks in a learning theory coursework project.

Dropout Reduces Underfitting **M2**

Co-implemented a TensorFlow/Keras reproduction of Liu et al. (2023), comparing early, late, standard and no dropout through learning curves and ablation studies.

Monte Carlo Methods **M1**

Implemented inverse-transform sampling, acceptance-rejection sampling and stratification methods in R.

INDEPENDENT INFRASTRUCTURE PROJECT

ArtLab: Personal Homelab **2023–present**

Self-hosted infrastructure for DevOps, distributed systems and MLOps experimentation

- Operate Proxmox virtual machines and LXC containers alongside Docker services across multiple hosts. Version service configurations in Git and automate deployments through Dockhand.
- Manage NAS-backed storage and S3-compatible object storage, with infrastructure backups through Proxmox Backup Server and application backups using restic.
- Configure private Tailscale networking, TLS and single sign-on for service access; monitor resource usage and availability with Beszel and Uptime Kuma.

TECHNICAL SKILLS & LANGUAGES

Mathematics: Probability and statistics, optimisation, stochastic processes, numerical analysis, statistical learning theory.

Scientific computing & AI: Python, PyTorch, NumPy, pandas, scikit-learn, Matplotlib, Hugging Face.

Research software & infrastructure: L^AT_EX, Git, CI/CD, Docker, Linux, PostgreSQL, Redis, Proxmox, Cloudflare.

Web & developer tooling: TypeScript, Vue/Nuxt, Tailwind CSS, Gradio, Claude Code, Codex, OpenCode.

Languages: French (native); English (advanced).