

MOHAMED MALHOU

Meta FAIR & Sorbonne Université, CNRS, LIP6 ♦ Paris, France

mmalhou@meta.com ♦ [Google Scholar](#) ♦ [GitHub](#)

RESEARCH INTERESTS

Machine learning for mathematics and scientific discovery; AI-driven cryptanalysis of post-quantum cryptographic systems (lattice-based, code-based, multivariate); transformer architectures for symbolic reasoning; reinforcement learning.

EDUCATION

Meta SuperIntelligence Labs

2023 – Present

Ph.D. in Computer Science (contract with Sorbonne Université)

Paris, France

Thesis: *ML for Solving Hard Mathematical Problems in PQ Cryptography*. Advisors: Kristin Lauter (Meta), Ludovic Perret (Sorbonne), François Charton (Meta).

ENS Paris-Saclay (Cachan)

2021 – 2022

M2 MVA (Mathématiques, Vision, Apprentissage)

Cachan, France

Coursework: Reinforcement Learning, Convex Optimization, Random Matrix Theory, Sequential Learning, 3D Computer Vision.

École Polytechnique

2018 – 2022

Ingénieur Polytechnicien, Applied Mathematics & Statistics

Palaiseau, France

Coursework: Statistical Modeling, Advanced Algorithms, Advanced Machine Learning, Operations Research.

Lycée d'Excellence de Benguerir (LYDEX)

2016 – 2018

Classes Préparatoires MPSI–MP*

Benguerir, Morocco

RESEARCH EXPERIENCE

Meta AI (FAIR / Meta Superintelligence Labs)

2024 – Present

PhD Student (CIFRE)

Paris, France

- **Formal Math** working on theorem proving in **Lean** with agent self-play and HyperTree Proof Search (HTPS).
- Designing an **MCTS + reinforcement learning** framework that formulates hard mathematical problems as MDPs and learns to solve them through self-play, inspired by AlphaZero.
- Designed **HATSolver**, a Hierarchical Attention Transformer that learns to compute Gröbner bases for solving multivariate polynomial systems.
- Introduced the first application of deep learning to **code-based cryptanalysis**: DeepDistinguisher outperforms classical attacks on Goppa and QC-MDPC codes (ClassicMcEliece, BIKE).
- Developed a novel statistical attack separating “cool” and “cruel” bits of LWE secrets, recovering secrets in dimensions up to $n=1024$.

Meta AI (FAIR)

2022

Research Scientist Intern

Paris, France

- Developed **Salsa Picante**, an enhanced ML attack on LWE with sparse binary secrets; introduced a novel preprocessing step and cross-attention recovery mechanism, scaling to $n=350$.
- Paper accepted at **ACM CCS 2023 (A*)**.

Pathway

2023

R&D Engineer – LLMs

Paris, France

- Created the open-source **LLM App** framework (59.9k GitHub stars) and core contributor to the **Pathway** real-time data processing engine.

PUBLICATIONS ([GOOGLE SCHOLAR](#))

**Equal contribution.* †*Senior author.*

[P5] M. Malhou, L. Perret, K. Lauter. *HATSolver: Learning Gröbner Bases with Hierarchical Attention Transformers*. **ICLR 2026(A*)** (Oral – top 1.8%). [\[arXiv\]](#)

[P4] M. Malhou, L. Perret, K. Lauter. *AI for Code-based Cryptography*. **SAC 2025** (Selected Areas in Cryptography), pp. 489–518. [\[ePrint\]](#)

[P3] E. Wenger*, E. Saxena*, M. Malhou*, E. Thieu, K. Lauter. *Benchmarking Attacks on Learning with Errors*. **IEEE S&P 2025** Oakland (A*), pp. 279–297. [\[ePrint\]](#)

[P2] N. Nolte*, M. Malhou*, E. Wenger*, S. Stevens, C. Li, F. Charton†, K. Lauter†. *The Cool and the Cruel: Separating Hard Parts of LWE Secrets*. **AfricaCrypt 2024**, pp. 428–453. [\[ePrint\]](#)

[P1] C.Y. Li*, J. Sotáková*, E. Wenger, M. Malhou, E. Garcelon, F. Charton†, K. Lauter†. *Salsa Picante: A Machine Learning Attack on LWE with Binary Secrets*. **ACM CCS 2023**, Copenhagen. (A*) [\[ePrint\]](#)

PREPRINTS

[P6] M. Malhou, L. Perret, K. Lauter. *Discovering Lattice Reduction Strategies via Self-Play* (Submitted to NEURIPS 26). [\[arXiv\]](#)

SELECTED PROJECTS

Deep Reinforcement Learning

Implemented and benchmarked RL algorithms (DQN, PPO, A2C, SAC) across continuous and discrete control tasks. Studied reward shaping, curriculum learning, and sim-to-real transfer. Coursework project at ENS Paris-Saclay (MVA).

Multilingual Word Embeddings – Research Project, supervised by François Yvon

Proposed improvements to cross-lingual word embedding alignment via Procrustes and optimal transport in the supervised setting.

TECHNICAL SKILLS

Languages	Python, C++, Java, C#, Bash/Linux scripting
ML & DL	PyTorch, Transformers (Hugging Face), Reinforcement Learning (Stable-Baselines3), Scikit-learn
Research	Lattice reduction (BKZ/fplll/flatter), SageMath, SLURM, distributed training, L ^A T _E X