Thomas **Winninger**

Student in gap year

✉ thomas.winninger@telecom-sudparis.eu   ⌂ https://le-magicien-quantique.github.io   ○ Sckathach   in Thomas Winninger

Whoami?

Aka *the quantum warlock, the masked camel, the fanOfThermodynamics, the pipe and clouds engineer, the whale orchestra conductor*, or just **Sckathach**. I'm a french student at Télécom SudParis, and soon, a ML(4SEC) researcher!

Fond of mathematics and physics, I ended up at the Télécom SudParis engineering school where I focused on cyber security. As I quickly became interested in AI security, I decided to take a gap year to bring myself up to speed on the subject: AI security research, interpretability, tools, statistics; and since that's what I like best, I plan to continue with a master's degree and a thesis, most likely in the same field.

Education

Master of Science in Cybersecurity

Institut polytechnique de Paris (IPP)   2024 - 2026

Engineering Degree

Télécom SudParis   2022 - 2026

Telecommunications, network security and web applications, graph theory (application to AI and 6G). Computer theory and databases. Signal processing and probability.

Experience

Research internship in AI security

Thales   Jul - Dec 2024

- Implementations and improvements of state-of-the-art attacks on LLMs (ACG, I-GCG, TAP), and on LLM-based systems (RAG, agents).
- Development of tools to facilitate research in the field (integration of TransformerLens).
- Use of interpretability techniques (probes, steering vectors, SAE) to create a new attack class (publication at the end of January).

Cybersecurity training, cloud management, and more...

HackademINT   2023 - 2024

- Responsible for training (regular training on Tuesday evenings, and practical work on Thursday afternoons) and infrastructure (Docker, Kubernetes).
- Creation and organisation of the 404CTF 2023 & 2024.
- Created challenges in artificial intelligence (adversarial attacks, poisoning, backdoors) and quantum physics (QKD attack).

Skills

Languages	**Python**, **Ocaml**, Typst, TypeScript, Rust, Lua, C, Bash
Spoken Languages	**English**, **French**, Korean
Frameworks/ Other	**PyTorch**, PyG, Docker (Podman), Kubernetes, Qiskit, Sage, Archlinux :)

Other interests

Piano, guitar, creating & playing video games, reading, geopolitics, particle physics, sport, meditation, teaching.