NinjaLab
12 rue Boussairolles
34000 Montpellier
France
https://ninjalab.io

Montpellier, December 4, 2024

Side-Channel Attacks on Post-Quantum Cryptography and Hybridation

Internship – 6 months from February 2025 – Montpellier, France

1 Presentation of NinjaLab

NinjaLab is a French company based in Montpellier, specialized in cryptology and embedded systems security.

NinjaLab was founded in 2017 by two internationally recognized researchers in cryptology and embedded systems security, with more than 20 years of experience as security experts for top high-tech companies and cybersecurity governmental agencies among the most famous in the world.

We propose different kind of services:

- Side-channel and fault attacks penetration tests on cryptographic devices (smartcard, microcontroller, SoC, FPGA, IoT, Smartphone, . . .)
- Consulting for custom / turnkey side-channel and fault attacks platforms and tools
- Technical support for Common Criteria, EMVCo and CSPN certification

Our headquarters are based in Montpellier downtown, and are equipped with our own side-channel and fault attacks platforms, and our own security evaluation tools.

For specific needs, a convention allows us to use the clean room (CTM) and the high performance computing center (MESO-LR) of the University of Montpellier.

We are also active academic researchers in the fields of cryptology and embedded systems security, members of IACR *(International Association of Cryptology Research)*, and often members of top conference / journal program committees (CHES, CASCADE, FDTC, Communications in Cryptology, . . .).

Finally NinjaLab hit few times the spotlight in the side-channel community for having found vulnerabilities and developed cryptanalytic exploits allowing full secret key extraction on several commercial secure devices like the Ledger Nano S, the Google Titan Security Key and Yubikeys.

2 Context

The new cryptographic primitive standards (hopefully) resistant to a quantum computer have been selected, the research community is actively working on implementing them. A central issue is the robustness of these implementations against side-channel attacks, a type of hardware attacks which consists

in observing the time, the power consumption or the electromagnetic activity of the circuit running a cryptographic operation in order to extract the secret.

The new PQC standards show very strong sensitivity to side-channel attacks, many new directions of attack have been proposed in the past few years. This new area of research is still emerging and many crucial questions are remaining open, among them: (1) Is there a better way to access to and exploit a *plaintext checking oracle* in practice[1]? (2) What hybridation[2] has to offer in terms of side-channel attacks.

3 Objectives

- (Re-)implement ML-KEM, the key-encapsulation standard, in Python. This will be used to generate simulations (synthetic side-channel traces).
- Implement a specific subset of the state-of-the-art side-channel attacks on ML-KEM (validation on simulations).
- Study new attack methods.
- Study the hybridization schemes in the light of side-channel attacks.

4 Skills Required

- Being in last year of master in sciences or engineering school in computer science / cybersecurity / cryptology / mathematics
- Strong background in number theory
- Good knowledge in cryptology
- Correct level in programming (Python, C, ...)
- Correct level in English
- Basics in side-channel attacks
- Most important: being motivated to learn / being curious / having the hacker mindset

5 Conditions

- Salary of 1700€ gross (approximately1500€ net)
- Lunch tickets (10€ per working day)
- Exciting scientific environment with offices in downtown Montpellier (the sunniest city in France, 10km away from the Mediterranean Sea)
- Depending on the internship outcomes, a PhD student position will be open (most probably in collaboration with the LIRMM - *Laboratory of Computer Science, Robotics and Microelectronics of the university of Montpellier*)

6 Apply

Apply by sending an email to apply@ninjalab.io, with the title of the internship, your resume and a motivation letter.

[1] see *e.g.* COSADE'22 paper from Azouaoui *et al.*, the understanding of this article is **not** mandatory to apply to the internship.

[2] In the transition toward PQC, there will be a time period where PQC and classical cryptography will be used together, this is called *hybridation*, see *e.g.* ANSSI point-of-view.