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

Montpellier, December 4, 2024

Side-Channel Attacks on Elliptic Curve Crypto.

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

In 2023 the ANSSI *(French governmental cybersecurity agency)* published on Github a hardware cryptographic accelerator called IPECC, dedicated to accelerate the *elliptic curve scalar multiplication*, the longest operation in Elliptic Curve Cryptography.

Furthermore, this accelerator implements several optional layers of countermeasures allowing to be protected 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.

3 Objectives

- Thanks to IPECC documentation, the intern will follow the tutorial to install IPECC on a FPGA board Xilinx Zynq Arty Z7.
- The intern will develop a Python script to communicate with the board for executing ECC cryptographic operations.
- The intern will perform side-channel attacks thanks to NinjaLab platforms and dedicated softwares on the unprotected version of IPECC.
- The intern will perform side-channel attacks on protected versions of IPECC by activating the different layers of countermeasures.
- Depending on the internship outcomes, the results could lead to the writing and submission of a research paper in an international conference, and/or to the publication of a public database of side-channel measurements for the side-channel research community (similarly to the ASCAD project).

4 Skills Required

- Being in last year of master in sciences or engineering school in computer science / cybersecurity / cryptology / electronics / microelectronics
- Correct level in programming (Python, C, . . .)
- Correct level in English
- Basics in cryptology (especially elliptic curve cryptography)
- Basics in side-channel attacks
- Basics in electronics / microelectronics is a plus
- 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.