eShard

Exploring side-channel attacks on ML-DSA

Internship

ML-DSA is a digital signature algorithm, standardized by the US' NIST in the FIPS 204 document [1]. It is recommended as a general purpose signature algorithm for the post-quantum transition. While its mathematical security is considered sound, the physical security (including side-channel analysis and fault-injection attacks) of its implementations requires additional scrutiny. Multiple works have started the assessment of physical vulnerabilities of the algorithm [2]. Nevertheless, additional work is needed to ensure resilience for ML-DSA-enabled embedded systems.

In this context, we propose a research internship exploring side-channel attacks on ML-DSA on either microcontroller or FPGA implementations.

[1] NIST, "FIPS 204 Module-Lattice-Based Digital Signature Standard," doi: 10.6028/NIST.FIPS.204

[2] Ravi et al., "Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results,", doi: 10.1145/3603170

COMPANY

eShard is a technology company focused on securing embedded devices and connected objects, ranging from electronic chips to mobile apps, where confidential data storage and secure information exchange are critical.

We empower designers, developers, and users of connected technologies to effectively manage cyber risks and maintain robust protection by analyzing security threats, conducting automated verifications, and assessing emerging attack vectors.

Driven by an expert team of researchers in cryptography, integrated circuit security, and mobile application protection, we deliver a comprehensive suite of solutions: Security testing platforms, specialized software, technical training, and security evaluation services.

As part of the development of our activity, we are recruiting an intern in our **Security Expert** team to work on this topic for a period of 6 months remunerated.

🗓️ **Desired start date:** February 2027.

📍 The position is based in **Pessac** (Bordeaux).

eShard

Your day-to-day would be:

You will be in charge of the following missions:

- Understand the ML-DSA algorithm and its implementations
- Perform a state of the art of the most relevant side-channel attacks
- Implement existing attacks, with the possibility of side-channel analyses and fault-injection attacks
- Redact write-ups of attacks in the form of notebooks, blogposts, with the possibility of peer-reviewed scientific publications

You're perfect for us, if...

- You are preparing a **master's degree** and are in your last year of study.
- You have developed a particular interest in:
  - Python
  - Embedded C
  - RTL (Verilog/VHDL)
- Previous experience on cryptography and/or physical security is a plus, including side-channel, signal processing and statistics.
- You are hacker minded, responsive and have the spirit of initiative.
- You demonstrate autonomy in your assignments.
- You demonstrate good interpersonal skills that will allow you to work as a team effectively.
- You have a good writing level in English.

Benefits

- Support from professionals in a cutting-edge and booming business sector.
- Dynamic work environment within a young and friendly team.
- High-performance work equipment.
- Flexible working hours.
- Space dedicated to talent development.
- Mutual health insurance with good medical and dental coverage.
- "Tickets restaurant" covered up to 50%.
- Annual events, snacks and drinks.

Interested?

Contact us by sending your resume to

intern@eshard.com