eShard

# Hardware Attack on Lightweight Crypto

## *Internship*

From the adoption of the Advanced Encryption Standard, the industry of secure IC devices has never stopped asking for an alternative to AES with less demanding implementation. Indeed, RFID, sensors, or some IoT devices and some applications like home automation, healthcare, smart city push requirements for constrained devices such that AES is considered as a not good enough trade off from the security, energy, cost and performance point of view. It took time for the community to establish guidelines, and in 2018 the NIST has established a list of requirements for a dedicated competition to define a Lightweight Cryptographic (LWC) Standard. Noticeably, the basic requirement is to provide Authenticated Encryption with Associated Data (AEAD), but a specific property for implementations raised or interest: implementations or the future standard must be "easy to protect against side channel attacks and fault attacks". Since March 2021, the list of ten finalists is known, and in late 2022 the winner(s) will be announced officially.

The purpose of the internship is to study side-channel and fault attacks applied to the winners, and initiate a series of notebooks starting with knowledge about the winner(s), the potential attack paths and build some attack Proof of Concepts on simulation.

COMPANY

eShard is a technology company specializing in the security of mobile or connected objects: electronic chips, mobile applications or any other communicating object for which there is both the storage of personal data and the exchange of information.

Our role is to provide our customers, designers or users of connected objects with the means to control cyber risk and to ensure that the objects integrate the right level of protection: understand the threat, carry out automatic checks, obtain the knowledge of attacks.

To do this, we have assembled a team of specialists, researchers who are experts in cryptography, IC security and security of mobile applications, and we offer our customers a range of tools and services: SaaS platform, software, technical training and security testing service.

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 2023.

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

eShard

## Your day-to-day would be:

Directly attached to the **Chief Scientist**, you will be in charge of the following missions:

- Create knowledge notebooks describing LWC winner(s).
- Create knowledge notebooks with attack paths related to embedded implementation of LWC winners.
- Develop Side-Channel or Fault injection attacks of winners as a Proof of Concept.

## You're perfect for us, if...

- You are preparing a master degree and are in your last year of study
- You have developed a particular interest in:
  - Python
  - Symmetric Key Cryptography
- You have some knowledge of 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