

# Public key Side Channel simulation

*Internship - Pessac*

---

## Introduction

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. This applies to all parts of objects: from chips in semiconductors to mobile applications.

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 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.

In the context of IC Security, the Public Key Cryptography (PKC) algorithms have taken an important role in many applications, and the **[side-channel]** community put the focus on the resistance of PKA implementations against side-channel attacks. Counter-measures such as randomization are deployed but are still challenged by specific attack techniques. In this context, development and validation of counter-measures on products require open devices, and material to acquire side-channel. To break the physical barrier, and pre-validate implementation of counter-measures, the simulation is a flexible and efficient vector. We want to go a step ahead in this direction to support efficiently Designers and Security Analysts.

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 2022.

The position is based in Pessac (Bordeaux).

# Job description

## Responsibilities

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

- Leverage the simulation tools of esDynamic to generate side-channel and fault campaigns.
- From execution of a reference PKC implementation executed with esDynamic Simulated Vulnerability Analysis (SVA) module to:
  - generate side-channel traces with parameters such as leakage source and model
  - generate faulty execution with parameters such as fault model
- A step further will be to implement the counter-measure and challenge it with side-channel or fault attacks.

## You are

You are preparing a master degree and are in your last year of study

- You have developed a particular interest in:
  - Python and C programming
  - Signal Processing
  - Public Key Cryptography
- You have some knowledge of side-channel, side-channel attacks, machine learning and deep learning and acquisition systems and instrumentation
- You are curious by nature, 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

## Your 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?

Send your resume and motivation letter to:

[career@eshard.com](mailto:career@eshard.com)

# Get in touch

---



[contact@eshard.com](mailto:contact@eshard.com)



[www.eshard.com](http://www.eshard.com)

## France

Bâtiment GIENAH  
11 avenue de Canteranne  
33600 PESSAC

7 rue Gaston de Flotte  
13012 Marseille

## Singapore

#04-01 Paya Lebar Quarter  
1 Paya Lebrar Link  
Singapore 408533

## Germany

Lebacher Str. 4  
66113 Saarbrücken  
Germany