eShard

Post Quantum Cryptography Side Channel Attacks

Internship

KYBER, DILITHIUM, FALCON and SPHINCS+ are the future standards for public key cryptography to enter the Post-Quantum Cryptography era. Due to uncertainty related to Quantum Computing progress, there is a strong push to introduce these new algorithms and fasten the transition. From the theoretical standpoint, these new algorithms will achieve a sustainable security for years, but in the day-to-day, the biggest threat is coming from practical attacks like side-channel or faults. One of the tough challenges coming is the assessment of side-channel resistance. Within NIST recommendations, side-channel resistance is part of the picture, and first elements have already been studied c.f.: Side-Channel Analysis of Lattice-based PQC Candidates for instance, but we are only at the beginning of the story. From pure software to full hardware implementations, there is a need for validation by security experts. In this context, the industry is coming with solutions.

The purpose of this internship is to implement and explore selected side-channel analyses on NIST's chosen key encapsulation mechanism (KEM) algorithm Kyber, to initiate the side-channel resistance assessment. Integrated into a team of IC Security experts, the student will contribute to a dedicated Post Quantum Side Channel analysis module expected by the IC Security community.

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 **IC Security** 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).

Your day-to-day would be:

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

- Collect and summarize principal publications regarding Lattice based cryptography
- Document the state of the art of physical attacks, already described on Kyber (a good starting point is [Survey] on SCA and Fault Attack).
- Produce PoC (Proof of Concept) of side channel attack and fault attack on Kyber.

You're perfect for us, if...

- You are preparing a **master** or **engineering degree** and are in your last year of study
- You have developed a particular interest in:
  - Python
  - Public 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

References 📜

[Survey] P. Ravi, A. Chattopadhyay, A Baksi, Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results. eprint 2022-737