PQ-TLS Chair Offer

Junior Research Leader

Side-Channel Attack for Post-Quantum Cryptography Applications

General information

Funding project: PEPR QUANTIQUE
Type of contract: Research Chair in Post-Quantum Cryptography
Contract period: 3+ years
Expected starting date: March 2024

Context

Cryptography is at the heart of many secure devices for ensuring confidentiality, integrity and authenticity of communications, programs and data. The security of the current asymmetric cryptography relies on problems that are easy to break with a quantum computer. In practice, the real threat of quantum computing is predicted to be operational in decades. However, through the National Institute of Standards and Technologies (NIST) impulsion, the community decided to move on a stronger cryptography, resilient to attacks from classical and quantum computers. This cryptography is called post-quantum cryptography (also called quantum-safe cryptography or quantum-resistant cryptography).

PQ-TLS is a 5-year research project driven by the French National Research Agency (ANR) and the France 2030 strategy under the frameworks of the Priority Research Programs and Equipments (PEPR). PQ-TLS aims at developing innovative and efficient hardware implementations of post-quantum cryptography resistant to physical attacks. Indeed, side channel attacks (computation time,energy consumption, electromagnetic radiation) and attacks by perturbation (fault injection) are important threats for embedded devices in scenarios where the attacker can be very close to the device (connected objects, smartphones, transportation, etc.).

Mission description

Side-Channel Attacks are important research topic nowadays and the security of post-quantum embedded implementations is a competitive research area. More and more papers have been published since 2015 and now that Kyber, Dilithium, Falcon and other schemes are standardized, it is highly important to know how to implement them securely. Usually masking is a well-known technique, but it is often costly to use this technique, which incurs a $O(d^3)$ multiplicative factor, where d is the masking order. There are a lot of research issues to tackle in this new research field. We are looking for young researcher interested in doing research in the security of post-quantum implementations.

Localisation

The job localisation will be determined by the candidate's employer, and the best team fitted to the subject.

Offer requirements

The candidate must have at least 2 years of experience after their PhD and have research experience in hardware security and post-quantum cryptography. In particular, it will be important to have strong knowledge in masking scheme and security proof of masking.
To already be employed by one of the following institutions: Rennes University, CNRS, Inria, CEA, Limoges Université, Rouen Normandie University, Bordeaux University, Jean Monnet Saint-Etienne University, Versailles Saint-Quentin University, ENS Lyon, Bretagne Occidentale University.

How to apply

Please send your application to pierre-alain.fouque@univ-rennes1.fr and marilou.gaborel@irisa.fr.

Required documents:

- Detailed CV with list of publications
- Two letters of recommendation
- Short research statement (1 page max)

Application Process

- Your application is reviewed by our committee
- Your application is accepted: it will be reviewed by the pilots and the ANR
- They accept you application: Oral presentation in front of the committee, and recruitment if approved.