Secured and optimized HW/SW Implementation of Agile Post-Quantum Cryptography based on lattices and codes

Description

Post-quantum cryptography is booming. This is due to quantum computer advances and to the NIST's initiative aiming at defining the first standards of post-quantum primitives by 2024. This new cryptography involves a scientific and industrial transition of the now wide cybersecurity ecosystem. Cryptographic primitives are at the heart of products for securing data and communications. They are designed to optimize a security-cost-performance ratio and must be revisited in this hybrid (combining pre- and post-quantum) and agile (proposing different post-quantum schemes) transition.

This PhD focuses on the acceleration and the security against physical attacks of post-quantum Key Encapsulation Mechanisms (KEM) based on lattices and error-correcting codes. It aims at taking advantage of existing mutualizations while respecting the resilience to physical attacks. The analysis of the HW/SW frontier will be of paramount importance and the identification of innovative architectures (based on Near-Memory Computing, for example) is not excluded. The implementation will be on SoC-FPGA.

The PhD will take place at the CEA Grenoble and will be supervised by the National Agency for Information Systems Security (ANSSI) and the CEA. It benefits from a strong dynamic around this subject, which will offer to the candidate a complete vision of the scientific, technological and industrial challenges of the general Cybersecurity domain.