Masking Kyber Compression

Laurent Imbert*[1]

[1]Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier – Centre National de la Recherche Scientifique, Université de Montpellier – France

Résumé

In July 2022, NIST has completed the third round of the Post-Quantum Cryptography (PQC) standardization process. A total of four proposals have been selected for standardization, among which Kyber is the only algorithm in the public-key encryption/key encapsulation mechanism (KEM) category. Kyber security is based on the hardness of solving the learning-with-errors (LWE) problem over module lattices. Over the past years, securing the implementations of Kyber against side-channel attacks has been a very hot topic. A generic approach to thwart high-order attacks consists in masking the secret data using secret sharing schemes. In this talk, I will present a novel approach for masking one of Kyber's internal component, namely the compression and decompression functions.

*Intervenant