On the Hardness of Learning With Physical Rounding and Noise from Learning With Error

Emeline Repel*[1]

[1]Equipe AMACC - Laboratoire GREYC - UMR6072 – Groupe de Recherche en Informatique, Image et Instrumentation de Caen – France

Résumé

In the context of quantum computing, cryptographic primitives are about to change to ensure security against quantum adversaries. To handle this problem, the National Institute of Standards and Technology (NIST) began a standardization campaign for post-quantum cryptosystems. From that, new primitives are arising, and particularly lattices problems computationally hard to solve like the Learning With Error (LWE) problem (Regev05). The decisional LWE problem asks to distinguish a sample (A, As + e (mod q)) from the uniform (A, b) where A and s are uniforms over Zq and e is a gaussian error.
The search version of this problem asks to find s. However, in the precipitation of the standardization

process, some aspects of cryptanalysis are not well studied. Especially,

physical attacks (using electric consumption, magnetic field, ...), namely Side Channels Analysis, permits to recover additional information on the secret. To handle this problem, masking with random computation seems to be a good alternative, but at what cost ? To optimize the masking of post-quantum lattice-based schemes, we need to ensure the security of the underlying primitive in knowledge of additional information on the secret coming from sides channels analysis. To do it so, we study the most realistic model of information obtained with sides channels Analysis such as the noisy Hamming Weight. So then, the adversary obtains the Hamming weight of the element implied in the current operation. We present a new variant Noisy Hamming Weight LWE (NHW-LWE) consisting in an LWE sample with additional material such as the noisy Hamming weight of As: (A, As + e (mod q), HW(As)+η), and prove its hardness under the LWE assumption. Finally, we conclude on the hardness of the Learning With Physical Rounding and Noise (LWPRN) which gives (A, HW(As) + η) using the previous security reduction.
Collaboration avec Clément Hoffmann, Adeline Roux-Langlois et François-Xavier Standaert

*Intervenant