Decoding Problem in the Sublinear Regime and Calibration of HQC

Valerian Hatey*[1]

[1]ETIS UMR 8051 – CY Cergy-Paris Université, ENSEA, CNRS – France

Résumé

HQC is a code-based encryption scheme where the private key is made of two sparse vectors in a quasi-cyclic structure, enabling the legitimate party to transform the ciphertext into a codeword corrupted by a small number of errors that can be efficiently decoded. Currently, there are no known attacks that exploit the underlying quasi-cyclic structure except for the DOOM framework. Consequently, the security of HQC relies on the difficulty of the DOOM Problem for random linear codes.
Problem DOOM(n, k, t, N). Given a parity-check matrix H of size (n–k) × n over F, a collection of syndromes s, ..., s_N in F^(n–k), and an integer t between 0 and n, find an error vector e in F^n and an index j in {1, ..., N} such that:

H · e = s, and

the Hamming weight of e is exactly t

The decoding problem (and its DOOM variant) is widely believed to remain computationally hard, even against quantum adversaries. In HQC, the parameter t is particularly small: it is sublinear in n. More precisely, the scheme uses k = n/2, t approximately equal to sqrt(k), and N = k. Since HQC is currently undergoing standardisation, it is crucial to study the decoding problem in the sublinear regime and, in particular, to investigate the non-asymptotic complexity of the various decoding algorithms for the parameters of HQC in order to properly calibrate the scheme.

In this presentation, we start from the HQC parameters and first review the complexity of known attacks, relying in particular on the work of Esser and Bellini. We then present various advanced decoding techniques that we consider relevant in the sublinear regime.

In particular, dual attacks have been only scarcely studied in the sublinear regime. We therefore propose several variants of dual attacks that are better suited to the sublinear regime, drawing inspiration from the current state-of-the-art techniques.

*Intervenant

Furthermore, lattice-inspired sieving algorithms are relatively new in the code-based setting and appear to be particularly relevant in the sublinear regime. We therefore also propose several variants and improvements of existing sieving algorithms.

In addition, we observe that, for the HQC parameters, Gaussian elimination dominates the complexity of Information Set Decoding algorithms. We therefore propose an attack that combines Stern's algorithm with an efficient factorisation of the Gaussian elimination, based on a technique from Jiseung Kim and Changmin Lee.

We then evaluate these different attacks on the HQC parameters and discuss the results obtained.
In collaboration with: Kevin Carrier, Jean-Pierre Tillich and Laura Luzzi