Hamming Quasi-Cyclic (HQC)

Modifications between 1st and 2nd rounds

HQC team

Abstract

This document summarizes the changes made to HQC submission for the second round.

Second round: Differences with 1st round

- Jurjen Bos (from Worldline) joined the HQC team as a developer.
- Problems with parity: As previously announced few months ago, the 2 and 3-DQCSD problems with parity distributions have been introduced to counter distinguisher from parity.
- Minor scheme modification : due to the specific use of tensor product codes (BCH and repetition), the length of the code is not required to be a prime. Specifically, the tensor product code has length $n_1 n_2$ with n_1 (resp. n_2) the length of the BCH (resp. repetition) code. In order to avoid algebraic attacks using polynomial factorization, we chose primitive primes n immediately greater than $n_1 n_2$. This results in extra bits, that are truncated where useless. The proof has been modified accordingly.
- The reference implementation now relies on NTL.
- We added an optimized implementation written in C that uses AVX2 instructions and takes advantages of the low Hamming weight of the vectors in HQC.
- We added a constant time implementation of the decoding of BCH codes.
- Parameters providing a Decryption Failure Rate (DFR) higher than 2^{-128} have been discarded.