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. Modifications that were actually made to the specifications are presented in Section 1. Ongoing works on further enhancements are described in Section 2.

1 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.
- Parameters providing a Decryption Failure Rate (DFR) higher than 2^{-128} have been discarded.

2 Ongoing work

Constant-time implementation. On February 22nd, Matthew Walters and Sujoy Sinha Roy announced the release of a constant-time BCH codes implementation (see PQC-forum). We are currently building upon their implementation [1] to provide a constant-time implementation of all HQC parameters. This implementation shall be made available before NIST second standardization conference, scheduled on August 22nd.

References

[1] Matthew Walters and Sujoy Sinha Roy. Constant-time bch error-correcting code. Cryptology ePrint Archive, Report 2019/155, 2019. https://eprint.iacr.org/2019/155.