Rank Quasi-Cyclic (RQC)

Modifications between first and second round

RQC Team

Abstract

RQC is a candidate to the NIST's competition for post-quantum cryptography standardization that have been selected for round 2. This document presents the modifications performed on RQC with respect to round 1 and describes ongoing works on RQC.

1 Modifications

- Two additional members have been added to the RQC proposal: Alain COUVREUR and Adrien HAUTEVILLE.
- RQC now uses ideal codes instead of quasi-cyclic codes.
- The parameters of the scheme have been updated so that the weight of the error, which is the most important parameter for the security, increases regularly with each level of security. In practice, it leads to a small increase of the parameters.
- The supporting documentation has been reorganized for clarification. Besides, additional details have been provided on Gabidulin codes, quantum speed-up on known attacks as well as resistance to timing attacks.
- The reference implementation have been updated: finite field arithmetic now relies on NTL in place of MPFQ and some improvements have been made on the implementation of Gabidulin codes.

2 Ongoing works

- We are working on a constant-time implementation of RQC based on the results described in the supporting documentation.
- We are working on an optimized implementation that no longer relies on the NTL library nor the MPFQ library and uses AVX2 instructions to speed-up finite field operations. This implementation shall be available before NIST second standardization conference, scheduled on August 22nd .