From: BIDOUX Loic <loic.bidoux@worldline.com>
Sent: Friday, December 14, 2018 11:05 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: RQC

Dear all,

We have conducted a study on the resistance of RQC to timing attacks which is available at
http://pqc-rqc.org/doc/rqc-constantTime.pdf

Abstract: This paper studies the resistance of the code-based encryption scheme RQC to timing attacks. We describe two choosen ciphertext timing attacks that relies on a correlation between the weight of the error to be decoded and the running time of Gabidulin code's decoding. These attacks are of theoretical interest as they outperform the best known algorithm to solve the rank syndrome decoding problem in term of complexity. Nevertheless, they are quite impracticable in real situations as they require a huge number of requests to a timing oracle. We also provide a constant-time algorithm for the decoding of Gabidulin codes that prevent these attacks without any performance cost for honest users.

An additional implementation including the aforementioned algorithm will be added later. This implementation should be seen as the first step of an effort to provide a constant time version of RQC.

Sincerely,
The RQC team