From: Tomas Fabsic <tomas.fabsic@gmail.com>
Sent: Wednesday, February 07, 2018 3:04 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: LEDApkc

Dear authors, dear all,

we have studied the vulnerability of LEDApkc against a reaction attack and would like to point to a new reaction attack which we think is relevant for this cryptosystem. The description of our attack is available at:

https://eprint.iacr.org/2018/140.pdf

Best regards,

Tomas Fabsic, Viliam Hromada, Pavol Zajac

From: marco.baldi.work@gmail.com on behalf of Marco Baldi <m.baldi@univpm.it>
Sent: Friday, February 09, 2018 1:02 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: LEDApkc

Dear Tomas, Viliam and Pavol,

thank you for pointing out this improved version of your previous statistical attack based on reactions.

We observe that the effectiveness of this attack has been verified under the following two assumptions:
i) n_0 = 2,
ii) artificially increased DFR through modified system parameters.

In this respect, we have the following comments.

1) According to our preliminary evaluations, the number of candidates for G increases approximately as 2^{n_0^2} p^{n_0^2}, thus the efficiency of this attack against the LEDApkc instances with n_0 > 2 cannot be claimed (and we believe is questionable).
2) Assumption ii) ignores the fact that the number of decryptions to reconstruct the matrix Q depends also on the rate of change of the DFR as a function of the number of errors t near the working point of the code on the said curve. Therefore, the conclusions drawn by artificially changing the working point of the code cannot be easily generalized to the parameter sets in the LEDApkc proposal.

Based on the above considerations, we believe that the arguments provided in your paper are not sufficient to prove that this attack affects the LEDApkc instances with n_0 = 2 at their DFR working point.
Concerning LEDApkc instances with higher n_0, there is no evidence of the efficiency of this attack even under the assumption of an artificially increased DFR.

In any case, please take into account that DFR^{−1} can be considered as a lower bound on the number of safe encryptions/decryptions for any LEDApkc keypair, independently of reaction attacks and their future evolution.

Best regards,
-- The LEDApkc team