From: gaborit <gaborit@unilim.fr>
Sent: Tuesday, April 03, 2018 3:01 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: RankSign

Dear NIST organizers,

We have been aware very recently of an attack on our RankSign proposal by T. Debris-Alazard and JP Tillich, we checked that the attack worked, and broke our proposed parameters. The authors confirmed to use that the attack will soon be available on eprint.

We guess it is possible to find some reparation, but such reparation would need to modify the scheme, hence we think it is better to withdraw our RankSign proposal. What we do by this mail.

Notice that the attack is very specific to the structure of RankSign and does not impact at all all our other proposals in rank metric.

best,

the RankSign team