From: Chen, Lily (Fed)
To: Alperin-Sheriff, Jacob (Fed); Moody, Dustin (Fed)
Cc: internal-pqc
Subject: RE: Regarding the FAP_KC Submission
Date: Wednesday, December 20, 2017 9:49:40 AM

Jacob and the team,

We have done an amazing job to look into 82 packages in such a short period of time. It is very wise to look into some "No" submissions one more time in case we have missed something. Not complete and/or not proper shall be a major reason to be categorized to "No".

Thanks all for the job well done!

Lily

From: Alperin-Sheriff, Jacob (Fed)
Sent: Wednesday, December 20, 2017 9:32 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Regarding the FAP_KC Submission

(It was definitely worth looking at again, I agree).

The closest thing I see to security level/strength estimates are that in some of the Section 6 (Analysis of Known Attacks) they give some concrete numbers of costs of attackjs.

However, Algorithm 3 (in Section 6.4, pgs 16-17) says "According to the formula, [formula] is a lower bound for the
search amounts in average case, taking l = tau = 23, which is equal to 2^90 + 2^88 whenever [some variables take on some values] respectively."

And Algorithm 5 (in Section 6.4.2, pg. 18) says "the probability of successfully choosing … the probability is 2^{-76} whenever [some variables take on some values, same variables and values as in Algorithm 3], respectively."

so it seems attacks significantly cheaper than Security Level 1 are already given by the authors themselves.

I will check the code too I guess, but I believe "complete and proper" precludes algorithms that the submitters themselves say don't meet our minimum security/etc. requirements, which is why we aren't allowing LEDAsig and why we kicked out PruneHorst

—Jacob Alperin-Sheriff