From: Kerman, Sara J. (Fed)
To: Moody, Dustin (Fed)
Subject: RE: DAGS-5 Entropy
Date: Tuesday, February 13, 2018 12:30:47 PM

Especially Daniel ☺

From: Kerman, Sara J. (Fed)
Sent: Tuesday, February 13, 2018 12:29 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: DAGS-5 Entropy

These people needed to be using the proper subject line…..

From: Moody, Dustin (Fed)
Sent: Tuesday, February 13, 2018 12:19 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: FW: DAGS-5 Entropy

This should probably be an official comment as well.

From: Smith-Tone, Daniel (Fed)
Sent: Tuesday, January 09, 2018 12:20 PM
To: pqc-comments <pqc-comments@nist.gov>
Cc: pqc-forum@list.nist.gov
Subject: DAGS-5 Entropy

Dear community,

I was asked to comment on DAGS since there seem to be no comments on this issue yet.

The parameters and performance data in the submission files for DAGS-5 are invalid because it is incapable of establishing shared keys of length at least 256-bits as required by our CFP--- at least not keys with 256-bits of entropy. The issue is that the shared seed for generating the keys has only 192 significant bits.

We communicated with the submitters on this issue before our acceptance decision and we agree that it is an easy issue to correct. One would assume that they have updated this aspect of the scheme on their project's website.

Please note--- along with my apologies--- this was not the only scheme I noticed that did not meet the implicit entropy requirements for KEMs, but I can't remember what other schemes suffered from this same oversight. I will try to check as my schedule allows, but as a warning, we may find similar (and hopefully easily correctable) errors in other submissions. The good news is that this is something that should be easy to fix in general; the bad news is that it invalidates data that we could really use.

Cheers,
Daniel Smith-Tone