From: Moody, Dustin (Fed)
To: internal-pqc
Subject: Dan"s skeleton package
Date: Thursday, September 21, 2017 11:17:36 AM

Everyone,

Dan has submitted a "skeleton package" that he is suggesting can be a template for other submitters, and asked for a quick review from us. I've looked at it, and it looks good to me. Larry has also looked at the KAT files and thinks they look fine. Please let me know any comments you have today, as I'm going to reply by the end of the day on the forum.

Thanks,
Dustin

Comments so far:

- Dan could include the optional "Additional_Implementations" Directory
- This is not an official submission – if Dan and his coauthors would like it to be, they need to send it to pqc-submissions@nist.gov
- While the format looks good to us, this is not a guarantee that anybody using this template will have a "complete and proper" submission. That will depend on what the submitter fills in the template with.
- In the source code files for KAT generation, we had the number of times to run it hard coded in as 100. Dan has this set to a variable KATNUM. We will recommend submitters set KATNUM to 100, but submitters can change this value (with the restriction that KATNUM must be at least 10).