From: Moody, Dustin (Fed)
To: Alperin-Sheriff, Jacob (Fed)
Subject: Re: Found Another Submission Hidden Inside GeMSS (DualModeMS)
Date: Friday, December 8, 2017 4:10:56 PM

Yeah, lets leave doing more testing on it til after you do the rest. Looking at their pdf, it says KeyGen is horrendously slow (like over 10 minutes), while signing is like 2 seconds, and verifying like 2ms. Strange.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Friday, December 8, 2017 4:08:55 PM
To: Moody, Dustin (Fed)
Subject: Re: Found Another Submission Hidden Inside GeMSS (DualModeMS)

The probability of 1 verifying properly but the algorithm not working is actually quite small. I'm gonna get the rest of the submissions I haven't checked the final versions of done first.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Friday, December 8, 2017 at 4:07 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: Re: Found Another Submission Hidden Inside GeMSS (DualModeMS)

So, the 1st KAT verified? And it takes around 25 minutes to do one? I think maybe let's check a few more, and if they all seem to check out we can trust they work. We could include a note on what exactly we verified and why.

Why is their algorithm so slow?

From: Alperin-Sheriff, Jacob (Fed)
Sent: Friday, December 8, 2017 3:34:01 PM
To: Moody, Dustin (Fed)
Cc: internal-pqc
Subject: Re: Found Another Submission Hidden Inside GeMSS (DualModeMS)

Man, now I wish I hadn't found it.

It took 12.5 minutes to do a single one of the 100 desired KAT iterations (they only sent 10 for what's now obvious reasons), and that was with their
optimized version, which they did make different from the reference as they used a library we'd approved earlier as long as they integrated it into their submission [which they didn't do but I checked anyway]).

With the reference version, I gave up about 25 minutes in.

FWIW, the 1 KAT iteration did match the first iteration in their file.

I guess we can discuss on Monday what to send them. I definitely need to tell them that the library needs to be integrated into their submission, but do I mark it as KATs verified?

From: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Date: Friday, December 8, 2017 at 2:21 PM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Found Another Submission Hidden Inside GeMSS

Dustin and everyone,

The GeMSS submission actually contains a 2nd submission inside the .tar file Dustin uploaded (called DualModeMS) that we must have missed. I haven't checked it over yet but it was clearly in on time so I am adding it to the spreadsheet and creating a new directory for it.

—Jacob Alperin-Sheriff