From: Moody, Dustin (Fed)
To: Peralta, Rene (Fed)
Subject: RE: memory requirements statement in PQC submissions
Date: Monday, October 16, 2017 7:45:00 AM

I've been mostly focusing on the sizes of inputs and outputs. It'd be nice if they addressed how much memory the algorithm used, but I haven't seen many which do that. But since our CFP says the sizes of inputs and outputs, I think that's what we should be checking for.

Hope that helps

Dustin

From: Peralta, Rene (Fed)
Sent: Friday, October 13, 2017 6:15 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: memory requirements statement in PQC submissions

Hi Dustin,

I've been assuming that "memory requirements" means how much computer memory the algorithms use. But I just noticed this

Memory estimate. The size of all inputs and outputs (e.g., keys, ciphertexts, signatures)

in the submission checklist. I am confused. If a submitter only specifies sizes of inputs (not including randomness) and outputs, has he/she satisfied the requirement?

Rene.