From: Moody, Dustin (Fed)
To: Kerman, Sara J. (Fed)
Subject: RE: One addition to an FAQ question
Date: Thursday, December 15, 2016 10:37:00 AM

Thanks!

From: Kerman, Sara J. (Fed)
Sent: Thursday, December 15, 2016 10:37 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: One addition to an FAQ question

Added that paragraph to the answer. (It's actually Q5 now, because we kept three questions from the original FAQs).

Sara

From: Moody, Dustin (Fed)
Sent: Thursday, December 15, 2016 10:01 AM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: One addition to an FAQ question

Sara,

One more late addition. We got a question on our pqc-forum that is prompting us to add to the FAQ.

On the 2nd question "Will NIST consider platforms other than the "NIST PQC Reference Platform" when evaluating submissions?" can you add another paragraph to the answer? The new paragraph should read:

The reference platform should be treated as a single core machine. If an algorithm can make particular use of multiple cores or vector instructions, submitters are encouraged to provide additional implementations for these platforms.

Thanks,

Dustin

(So the 2nd question will now be):

Q: Will NIST consider platforms other than the "NIST PQC Reference Platform" when evaluating submissions?

A: The reference platform was defined in order to provide a common and ubiquitous platform to verify the execution of the code provided in the submissions. NIST will include performance metrics from a variety of platforms in our evaluation, including: 64-bit "desktop/server class," 32-bit "mobile class," microcontrollers (32-, 16-, and where possible, 8-bit), as well as hardware platforms (e.g., FPGA). Submitters are encouraged to provide additional implementations for these platforms if possible.

The reference platform should be treated as a single core machine. If an algorithm can make particular use of multiple cores or vector instructions, submitters are encouraged to provide additional implementations for these platforms.