From: Cooper, David A. (Fed)
To: Apon, Daniel C. (Fed); Peralta, Rene C. (Fed)
Subject: Re: Coordination meeting
Date: Wednesday, October 27, 2021 11:38:43 AM

Hi Daniel, Rene,

My guess is that the most recent presentation on Dilithium and Falcon was by Quynh in December 2020: https://nistgov.sharepoint.com/:p:/r/sites/PQC/Shared%20Documents/round%203%20presentations/12_3_2020%20version_Dillithium%20and%20Falcon%27s%20Round%203%20changes.pptx?d=w0bb3f3e4b2f144f5a18e380dde65ac92&csf=1&web=1&e=BiuKot.

As a starting point for our presentation, however, we should look at the three documents for the upcoming Kyber, Saber, NTRU (KSN) presentation in https://nistgov.sharepoint.com/:f:/r/sites/PQC/Shared%20Documents/End%20of%20Round%203?csf=1&web=1&e=akKjSc.

On 10/27/21 10:52 AM, Apon, Daniel C. (Fed) wrote:

> - present both algorithms
> - size and speed (and RAM/ROM usage?)
> - security arguments (NTRU / MLWE / hash-and-sign / Fiat-Shamir) ?
> - tightness in QROM?
> - any attacks? partial attacks?
> - implementation issues
> - use-cases (arguments for one or the other in different situations)
> - patents? (none?)
> - will the on-ramp give something better? or just 'different'?
> - variants of Falcon? (Zalcon, etc.? Do we know what their performance, etc, is like?)

From: Apon, Daniel C. (Fed)
Sent: Tuesday, October 26, 2021 11:30 AM
To: Peralta, Rene C. (Fed) <rene.peralta@nist.gov>; Cooper, David A. (Fed) <david.cooper@nist.gov>
Subject: Coordination meeting
When: Wednesday, October 27, 2021 10:00 AM-11:00 AM.
Where:

To join the video meeting, click this link (b) (6)

Otherwise, to join by phone, dial (b) (6) enter this PIN: (b) (6)
To view more phone numbers, click this link (b) (6) =5