From: Moody, Dustin (Fed)
To: Apon, Daniel C. (Fed); Perlner, Ray A. (Fed)
Subject: Re: What do you think about sending the Kyber team a short email
Date: Tuesday, June 2, 2020 12:51:40 PM

Let's wait a day and see if they respond on the forum. They may present some arguments.

If they don't, then we can ask them to respond.

Either way, we can write them and mention your idea of a possible tradeoff and ask them what they think and any other questions we have.

Dustin

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Tuesday, June 2, 2020 12:37 PM
To: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: What do you think about sending the Kyber team a short email

Yes, I think it's worth doing for all 4..

I need to write stuff for the 2nd Round report first, but at some point, perhaps it is worthwhile to craft an email to all 4 of them

---

From: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Sent: Tuesday, June 2, 2020 12:36 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: What do you think about sending the Kyber team a short email

Do you plan on sending emails to NTRU, Falcon and Dilithium as well?

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Tuesday, June 2, 2020 12:34 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: What do you think about sending the Kyber team a short email

Mentioning the CoreSVP vs DFR trade-off (RE: their noise rate at level 1 / 3)?

--Daniel