From: Moody, Dustin (Fed)
To: Liu, Yi-Kai (Fed); Perlner, Ray A. (Fed)
Subject: Re: IDF text
Date: Thursday, March 31, 2022 10:52:28 AM

Yi-Kai,

Yes - we have to wait until there is something publicly available. You could go in and write it and comment it out I guess.

Dustin

From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Sent: Thursday, March 31, 2022 10:29 AM
To: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: IDF text

Sounds good, let me know if/when I should make these changes. (I guess it's best if we can cite a publicly available version of the IDF/Matzov paper.)

--Yi-Kai

_____
From: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Sent: Thursday, March 31, 2022 9:51 AM
To: Moody, Dustin (Fed); Liu, Yi-Kai (Fed)
Subject: RE: IDF text

Yi-Kai's proposed edits seem reasonable to me. BTW, while I was poking around on overleaf, I took the liberty of adding a couple newer references on enumeration in appendix C. Hopefully this was not a grievous sin.

Ray

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, March 31, 2022 8:45 AM
To: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: Re: IDF text

Fine by me.

Ray, thoughts?

_____
From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov<mailto:yi-kai.liu@nist.gov>>
Sent: Wednesday, March 30, 2022 8:48 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov<mailto:dustin.moody@nist.gov>>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov<mailto:ray.perlner@nist.gov>>
Subject: Re: IDF text

Hi guys,

Maybe we could do this:

In section 3.2.3, where we mention primal/dual attacks on SIS/LWE problems, we cite a list of papers... we can cite the IDF/Matzov paper there (without going into details).

In the section on Kyber, under "significant events," we can say that recent results like IDF/Matzov might affect the estimates of security strength (without going into details).

What do you think? I don't want to say very much about the paper, because it will probably take some time to understand it properly.

--Yi-Kai

From: Moody, Dustin (Fed) <dustin.moody@nist.gov<mailto:dustin.moody@nist.gov>>
Sent: Wednesday, March 30, 2022 9:18 AM
To: Perlner, Ray A. (Fed); Liu, Yi-Kai (Fed)
Subject: IDF text

Ray and Yi-Kai,

Can we get whatever possible text we might want to add in response to the IDF/Matzov paper figured out now? That way if it is published we can just immediately insert the text. Yesterday we discussed including a sentence or two in Section 3, and probably also in the Significant Events part of Kyber.

Thanks,

Dustin