From:	Miller, Carl A. (Fed)
To:	Moody, Dustin (Fed)
Subject:	Re: Security proof for Dilithium
Date:	Tuesday, August 31, 2021 10:42:47 AM

Ok.

-Carl

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Date: Tuesday, August 31, 2021 at 10:41 AM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Subject: Re: Security proof for Dilithium

Yep

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Tuesday, August 31, 2021 10:41 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Security proof for Dilithium

Ok. 10:00am?

-Carl

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Date: Tuesday, August 31, 2021 at 10:31 AM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Subject: Re: Security proof for Dilithium

Great - lets do the 14th.

Dustin

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Tuesday, August 31, 2021 10:30 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Security proof for Dilithium

Hi Dustin –

How about Sept. 14th or Sept. 21st? (We can go ahead and make "Security of Falcon and Dilithium in the QROM" the official title.)

-Carl

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Date: Monday, August 30, 2021 at 12:03 PM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Subject: Re: Security proof for Dilithium

Carl,

I appreciate your initiative. Yes, I think the direction you've outlined is great. Let me know when you want to do it.

Dustin

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Monday, August 30, 2021 12:00 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Security proof for Dilithium

("crypto group" à "postquantum crypto group")

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Date: Monday, August 30, 2021 at 11:59 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Security proof for Dilithium

Hi Dustin –

Following up on our discussion in early August:

I was thinking I could give a talk to the crypto group entitled "Security of Falcon and Dilithium in the QROM," or something like that. The main goal would be to see if we can enumerate all of the assumptions that underlie the security proofs of Falcon and Dilithium.

Partly this is a learning experience for me -- I'm choosing one aspect of the postquantum crypto project and seeing if I can get fully up to speed on it. But, I'd only want to do this if it's also going to benefit the postquantum crypto project overall. What do you think? (I'm open to doing the talk from a different angle.)

-Carl

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Date: Tuesday, August 3, 2021 at 10:16 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>

Subject: Re: Security proof for Dilithium

Hi Dustin –

Ok. I think I'll first see if I can similarly deconstruct the security proof for Falcon. Doing a talk (or doing 2 talks) about both schemes is probably more useful from the perspective of the group right now. Thanks.

-Carl

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Date: Monday, August 2, 2021 at 11:00 PM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Subject: Re: Security proof for Dilithium

Carl,

Thanks for doing this. Yeah - I'm not sure what would be better. A talk now (while you're remembering all the details) or doing a later talk comparing the same for Falcon. do you have a preference? or should we ask the group?

Dustin

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Monday, August 2, 2021 2:09 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Security proof for Dilithium

Hi Dustin –

I've been doing a deep study lately of Dilithium. (I choose it mainly because, among our finalists, it seemed like one that I could easily get a handle on.) I've got a pretty good understanding of the security proof at this point. I was just wondering: is there anything I could do with what I've learned that might be useful to the PQC group?

This is the main paper I've read:

A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model

https://link.springer.com/chapter/10.1007/978-3-319-78372-7_18

I thought of possibly trying to give a talk about the paper to our group. But I don't know -- that might be premature, and could be better saved until we know what signatures we're actually

standardizing. Another possibility would be to do a similar study of security proofs for Falcon, and then try to qualitatively compare the two …

Anyway, I just thought I'd write to you to see if you had any ideas. Hope things are well on your end.

-Carl