

From: [Miller, Carl A. \(Fed\)](#)
To: [Chen, Lily \(Fed\)](#)
Subject: Re: Talk on Dilithium and Falcon (Tuesday, Sept. 14th, 10:00am EDT)
Date: Thursday, September 16, 2021 10:20:45 AM

Hi Lily –

Ok -- I'll think about a possible future talk.

-Carl

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Date: Thursday, September 16, 2021 at 9:55 AM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Subject: Re: Talk on Dilithium and Falcon (Tuesday, Sept. 14th, 10:00am EDT)

Hi, Carl,

Don't worry about crypto background. I am sure that you will gain the background quickly by working on the PQC project, especially when we start to draft standards. I think a talk on Kyber and Saber will be great. I look forward to it.

Lily

From: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Date: Wednesday, September 15, 2021 at 11:22 AM
To: Lily Chen <lily.chen@nist.gov>
Subject: Re: Talk on Dilithium and Falcon (Tuesday, Sept. 14th, 10:00am EDT)

Hi Lily –

Things are pretty good. UMD has fully reopened, so I'm spending time at QuICS these days. I got an opportunity recently to write an article for the AMS Notices, and I'm hoping to use that to possibly shepherd more people towards quantum & crypto ...

I'm looking for ways to contribute to the postquantum crypto project. (It can be challenging, since there are many people who have more crypto background than me.) If the talk I gave yesterday was helpful, I could possibly do a similar talk on Kyber & Saber some time ...

-Carl

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Date: Wednesday, September 15, 2021 at 9:10 AM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>

Subject: Re: Talk on Dilithium and Falcon (Tuesday, Sept. 14th, 10:00am EDT)

Hi, Carl,

Thanks. The talk was very helpful to me. How are you? Hope everything is going well.

Lily

From: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>

Date: Tuesday, September 14, 2021 at 1:06 PM

To: internal-pqc <internal-pqc@nist.gov>

Subject: Re: Talk on Dilithium and Falcon (Tuesday, Sept. 14th, 10:00am EDT)

Here are the slides from my talk today. (They're also on sharepoint.)

-Carl

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>

Date: Monday, September 13, 2021 at 3:07 PM

To: internal-pqc <internal-pqc@nist.gov>

Subject: Talk on Dilithium and Falcon (Tuesday, Sept. 14th, 10:00am EDT)

Hi PQC folks –

This is just a reminder that I'm going to give a talk tomorrow (Sept. 14th) at 10:00am. The title of the talk is "Security for Dilithium and Falcon in the QROM." The Google Meet link is in Dustin's e-mail below. See you then!

-Carl

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>

Date: Tuesday, September 7, 2021 at 2:48 PM

To: internal-pqc <internal-pqc@nist.gov>

Subject: internal PQC meeting

Carl will speak on the security assumptions for Dilithium and Falcon



(b) (6)

[REDACTED]

[REDACTED]

(b) (6)