From: Chen, Lily (Fed)
To: Peralta, Rene (Fed)
Subject: RE: [NIST PQC Hardware Day] Talk Program and Arrival Instructions
Date: Tuesday, April 30, 2019 2:07:00 PM

Hi, Rene,

Yes. We surely can. I think we will have space. If you have time, you can come to the room.

Lily

From: Peralta, Rene (Fed)
Sent: Tuesday, April 30, 2019 2:06 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: [NIST PQC Hardware Day] Talk Program and Arrival Instructions

Hi Lily,

Can we ask speakers to give us their slide decks?

There are a couple of talks that I might be interested

in.

Thanks, Rene.

From: Chen, Lily (Fed)
Sent: Tuesday, April 30, 2019 1:19 PM
To: Kerman, Sara J. (Fed)
Cc: Apon, Daniel C. (Fed); Moody, Dustin (Fed); Bajcsy, Zuzana (Fed); internal-pqc
Subject: RE: [NIST PQC Hardware Day] Talk Program and Arrival Instructions

We had a head count today for the NIST team members who plan to attend Hardware Day: Daniel Apon, Dustin, Matt, Ray, Jacob, John, Dave, Quynh. Angela. I did not get a chance to ask Daniel Smith-Tone. Now we have about 10.

Lily

Beginning of PQC Hardware Day.

9:30am-10:00am:

(*Chaperoned***)** Arrival at Building 222 (lobby), NIST campus

10:00am-10:15am:

Title: Overview of the NIST PQC Standardization Project

Speaker: Dustin Moody -- NIST, USA

10:15am-11:00am:

Title: Progress in Hardware and ARM Implementations of SIKE

Speaker: Reza Azarderakhsh -- Florida Atlantic University, USA

11:00am-11:45am:

Title: A Brief Introduction to Lattice-Based Cryptography in Hardware

Speaker: James Howe -- University of Bristol, UK

11:45am-12:30pm:

Title: PQM4: Benchmarking PQC on the Cortex-M4

Speaker: Matthias Kannwischer -- Radboud University Nijmegen, Netherlands

Lunch.

12:30pm-12:35pm: **(***Chaperoned***)** Travel from Building 222 to NIST cafeteria

12:35pm-1:25pm: Lunch in the NIST cafeteria

1:25pm-1:30pm: **(***Chaperoned***)** Travel from NIST cafeteria to Building 222

1:30pm-2:30pm:

Title: Hardware and Software/Hardware Benchmarking of PQC Schemes

Speaker: Kris Gaj -- George Mason University, USA

2:30pm-3:00pm:

Title: Evaluation of PQC Candidates using FOBOS and XXBX

Speaker: Jens-Peter E Kaps -- George Mason University, USA

3:00pm-3:45pm:

Title: Power, Performance, Area and Security (PPAS) Trade-offs of Post-Quantum Cryptography

Speaker: Kanad Basu -- New York University, USA

3:45pm-4:30pm:

Title: FA-PQC: Efficient Implementation of Polynomial Multiplication for Lattice-based Cryptography

Speaker: Jiafeng Xie -- Villanova University, USA

4:30pm-5:00pm: Open Discussion

End of PQC Hardware Day.
5:00pm-5:15pm: **(***Chaperoned***)** Departure to Building 222's parking lot