

From: [Moody, Dustin \(Fed\)](#)
To: [Kerman, Sara J. \(Fed\)](#); [Peralta, Rene C. \(Fed\)](#); [internal-pqc](#)
Subject: RE: 2nd NIST PQC workshop
Date: Wednesday, March 7, 2018 1:22:43 PM

I'd guess we'll probably want Saturday then.

Ugh. I don't like Saturday workshops!

From: Kerman, Sara J. (Fed)
Sent: Wednesday, March 07, 2018 1:05 PM
To: Peralta, Rene (Fed) <rene.peralta@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>;
internal-pqc <internal-pqc@nist.gov>
Subject: RE: 2nd NIST PQC workshop

I heard back from UCSB and Crypto typically goes until lunch on Thursday. Crypto uses the Corwin Pavilion which is the same space PQC would use. The earliest we could start is Thursday after lunch (unless their agenda were to change)

Sara

-----Original Message-----

From: Chen, Lily (Fed)
Sent: Wednesday, March 07, 2018 9:14 AM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: FW: CRYPTO, CHES, PQC 2019

Hi, Sara,

The next step we may want to know is whether we can start Thursday morning using Corwin Pavillion. I am sure that you and Sally will work out a good plan for whatever we determine to do.

Lily

From: Peralta, Rene (Fed)
Sent: Wednesday, March 07, 2018 8:12 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: 2nd NIST PQC workshop

I think we should plan to go into Saturday.

Rene.

From: Moody, Dustin (Fed)
Sent: Wednesday, March 7, 2018 8:02 AM
To: internal-pqc
Subject: 2nd NIST PQC workshop

Everyone,

It may seem a bit early to be looking so far out, but we going to co-locate our 2nd NIST workshop with Crypto, in August 2019. We need to determine how much time we want. Crypto ends Thursday, August 22nd, and they usually are done by lunch. We could either start Thursday morning with a parallel track going on the same time as Crypto, or wait and start Thursday afternoon. We can end on Friday, or if we want more time we could go into Saturday.

What are your thoughts? How much time do we want for our 2nd workshop? For reference, the 2nd SHA workshop (which was also co-located with Crypto) was 2 full days, held on a Monday/Tuesday. Each of the 14 candidates in Round 2 was given 12 minutes to give an update. The rest of the time was filled up with other talks on security/performance analysis of the candidates, as well as some time for open discussion.

Dustin