From: Kerman, Sara J. (Fed)
To: Chen, Lily (Fed); Moody, Dustin (Fed)
Subject: RE: NIST PQC 2019
Date: Wednesday, August 23, 2017 12:27:31 PM

The First SHA-3 conference was Feb 2009 and second was August 2010 - which is just a little longer than our early-April 2018 and potential August 2019 PQC dates.

-----Original Message-----
From: Chen, Lily (Fed)
Sent: Wednesday, August 23, 2017 12:23 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: NIST PQC 2019

Actually, if we have conference in August, more or less, the submission deadline will be sometime in June, which is about 14 months after the first conference. Is the period for people to do analysis a little too short?

If we do not co-locate with crypto, we might have the conference a little later than August, say October in NIST.

These are just something to think about.

Lily

On 8/23/17, 9:09 AM, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:

> Perhaps you could just talk to her and say we are strongly considering it. We could then wait to make a final decision.
>
> My only concern might be is that if someone were to attend ours, Crypto, and CHES that would be a really long time for them to be there.
>
> Dustin
>
> -----Original Message-----
> From: Chen, Lily (Fed)
> Sent: Wednesday, August 23, 2017 12:07 PM
> To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
> Subject: NIST PQC 2019
>
> Hi, Dustin and Sara,
>
> This is some initial information I got. Crypto 2019 will be collocated with CHES. Crypto 2019, as usual, starts Sunday evening and ends Thursday at noon. Then CHES will be Thursday, Friday and maybe half day Saturday.
>
> Then our conference may have to be the week before Crypto 2017. I haven't talked with IACR president yet. I mentioned to Sally (Sara may remember her. She has been in conference service in UCSB for a long time, as far as I came to crypto). They haven't announced general chair of crypto 2019 yet. The general chair should be determined this afternoon at the member meeting.
>
> The question to us is whether we want to do it before Crypto. Any thoughts?
>
> Lily