From: Chen, Lily (Fed)
To: Mouha, Nicky W. (IntlAssoc); Moody, Dustin (Fed)
Cc: threshold-crypto
Subject: RE: NTCW calendar, meeting today?
Date: Friday, February 1, 2019 1:25:00 PM

Dustin is in downtown today for a workshop. I can stop by.

Lily

From: Mouha, Nicky W. (IntlAssoc)
Sent: Friday, February 01, 2019 1:17 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: threshold-crypto <threshold-crypto@nist.gov>
Subject: Fw: NTCW calendar, meeting today?

Hi Lily, Dustin,

We're meeting from 15:30-16:00 in the small conference room to discuss the program of the NIST Threshold Workshop.

Given that we're considering some talks on NIST standards (the general process, PQC, X22519,...), we thought it could be a good idea to coordinate. Let us know if you have the time to swing by. Sorry for the late invitation.

Regards,

Nicky

From: Brandao, Luis (IntlAssoc)
Sent: Friday, February 1, 2019 1:05 PM
To: Mouha, Nicky W. (IntlAssoc); Vassilev, Apostol (Fed)
Subject: Re: NTCW calendar, meeting today?

Hi,

Just reserved the small conference room with Diane, for 3:30pm.

If Lily is coming today, then I suggest we invite Dustin today as well (if he's around).

If there's time available after talking with them, then I'd suggest we stay for a little longer to discuss a few other logistic aspects.

Regards,

Luís

From: Mouha, Nicky W. (IntlAssoc)
Sent: Friday, February 1, 2019 12:18:04 PM
To: Vassilev, Apostol (Fed)
Cc: Brandao, Luis (IntlAssoc)
Subject: Re: NTCW calendar, meeting today?

Hi Apostol,

Yes, that's precisely the reason. We should give Lily some insights into the preliminary program. This will be necessary for her to prepare her own talk, and to coordinate with the other talks on PQC/X25519/CMVP. I expect that she will also have some useful feedback for us.

Regards,

Nicky

From: Vassilev, Apostol (Fed)
Sent: Friday, February 1, 2019 12:09 PM
To: Mouha, Nicky W. (IntlAssoc)
Cc: Brandao, Luis (IntlAssoc)
Subject: Re: NTCW calendar, meeting today?

Nicky,

I spoke with Luis earlier today and seems he will be available but will let him confirm. FYI, I spoke with Lily yesterday and invited her to give the talk at the workshop. She accepted. Do you have something else for her to do today?

Thanks,
Apostol

> On Feb 1, 2019, at 11:45 AM, Mouha, Nicky W. (IntlAssoc) <nicky.mouha@nist.gov> wrote:
>
> Hi Luis,
>
> Can you confirm if 15:30 works with you? If so, I'll check if Lily is available as well.
>
> Regards,
> Nicky
>
> From: Vassilev, Apostol (Fed)
> Sent: Friday, February 1, 2019 9:25 AM
> To: Mouha, Nicky W. (IntlAssoc)
> Cc: Brandao, Luis (IntlAssoc)
> Subject: Re: NTCW calendar, meeting today?
>
> I just got into the office, delayed by the slow traffic. Let’s shoot for the afternoon at 15:30 please.
>
> Thanks,
> Apostol
>
> > On Feb 1, 2019, at 9:16 AM, Mouha, Nicky W. (IntlAssoc) <nicky.mouha@nist.gov> wrote:
> >
> > I can make myself available in those two slots as well.
> >
> >
> > From: Brandao, Luis (IntlAssoc)
> > Sent: Thursday, January 31, 2019 4:13 PM
> > To: Vassilev, Apostol (Fed)
> > Cc: Mouha, Nicky W. (IntlAssoc)
> > Subject: Re: NTCW calendar, meeting today?
> >
> > I'll be here during those two slots, available to meet in any of them.
> >
> >
> > From: Vassilev, Apostol (Fed)
> > Sent: Thursday, January 31, 2019 15:16
> > To: Brandao, Luis (IntlAssoc)
> > Cc: Mouha, Nicky W. (IntlAssoc)

> > Subject: Re: NTCW calendar, meeting today?
> >
> > Tomorrow is a bit difficult for me schedule-wise but here is my availability:
> >
> > 09:15-09:45
> > 15:30-16:00
> >
> > Thanks,
> > Apostol
> >
> > > On Jan 31, 2019, at 2:26 PM, Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov> wrote:
> > >
> > > Okay, not meeting today. (We had scheduled it on our Tuesday meeting)
> > > I put it as a question because Nicky did say being busy and possibly not being able to make it.
> > >
> > > How about meeting tomorrow, Friday, for 30 min (if longer is not an option)? I'm available at any time, except 10am-11am.
> > > I'd suggest two items:
> > > - considerations about the schedule;
> > > - communications to do. For example, I think we should communicate with the panels' organizers to inform them of related talks that are preceding the panels, and based on that ask/suggest which duration is reasonable for the panel.
> > >
> > > Regards,
> > > Luís
> > >
> > >
> > > From: Mouha, Nicky W. (IntlAssoc)
> > > Sent: Thursday, January 31, 2019 13:50
> > > To: Vassilev, Apostol (Fed); Brandao, Luis (IntlAssoc)
> > > Subject: Re: NTCW calendar, meeting today?
> > >
> > > As I explained to Luis: I'm caught up with urgent lightweight stuff right now. Kerry works at home on Friday and Monday, and unfortunately we have some things that can't wait until Tuesday...
> > >
> > > Therefore, I will be unavailable for the impromptu meeting today, but I'll check my e-mails.
> > >
> > > From: Vassilev, Apostol (Fed)
> > > Sent: Thursday, January 31, 2019 1:44 PM
> > > To: Brandao, Luis (IntlAssoc)
> > > Cc: Mouha, Nicky W. (IntlAssoc)
> > > Subject: Re: NTCW calendar, meeting today?
> > >
> > > I am for meeting. See you at 2pm.
> > >

> > > Thanks,
> > > Apostol
> > >
> > > > On Jan 31, 2019, at 1:40 PM, Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov> wrote:
> > > >
> > > > Hi,
> > > >
> > > > We still have the library (2nd floor) reserved between 2pm and 4pm. Do you want to meet for a while ... not necessarily till 4pm?
> > > >
> > > > Did some extra test-puzzling on the schedule (sheet "experiment 5"), now uploaded to svn. Some rational below. Please check what looks good and/or feel free to edit suggestions directly in the draft calendar.
> > > >
> > > > Some notes:
> > > >
> > > > - Mentioned to Sara that perhaps we would consider having the rump/pitch sessions not be broadcast. Sara said that technically NIST could pay for extra time, but that on the other hand it may be easier to indeed not do broadcast because we do not want to have to request a form signing by everyone.
> > > >
> > > > - Sara says the mandatory video is about 3 min, and that usually is displayed by the welcoming person ... as we currently have in our calendar.
> > > >
> > > > - Moved side-channel circuit design session to early in 2nd day, so that the panel is not in the end of the day.
> > > >
> > > > - Opened a new "final pitches" slot in the end of the 2nd day for open comments. Will be a new opportunity (after having heard all talks) for people to make final remarks/suggestions
> > > >
> > > > - Moved the "recommendations" talk to be the last one, before the "final pitches" session, since it is related. Also, the author acks that it it a "short talk" and himself said it can be done in 20 min including questions.
> > > >
> > > > - Upon the above changes, we can have the 2nd keynote (which is intended to be on applications) be before the talks about applications. A though is that, at this point in the conference, after having heard a lot of math, perhaps the apps talks could be shorter (also 20 min). The savings of 5 min here and there makes things fit.
> > > >
> > > > - One unexplored time saving could be to ask panel organizers how much time would they ideally like to have, considering the set of talks that preceded them. For example, if the circuits panel may want less that 75 min (in case not all 6 panelist come, and/or considering the previous 4 talks), then we get some extra time saving.
> > > >
> > > > - Sara mentioned that since the lunch is in a reserved place it actually ends to be quick. This

means we can, if need-be play with having slightly less than 85 min.
> > > >
> > > > - I thought of where the extra potential invited talk on distributed systems could fit. I think topic-wise it does not fit well in the 2nd day. Also, for the 1st day it would not fit in size as a large 45 min talk. One possibility (currently edited) is to have it be as a regular sized talk (25 min), instead of 45 min. Another possibility, is to simply remove it, e.g., if the 1st keynote speaker prefers having a full hour. For now I'd prefer waiting to confirm the 1st keynote before proceeding to invite the distributed systems talk.