From:	Moody, Dustin (Fed)
To:	Mouha, Nicky W. (Assoc)
Subject:	Re: Threshold Crypto Workshop
Date:	Wednesday, February 6, 2019 7:18:57 AM

Nicky,

For a title, let's go with: "NIST status update on elliptic curves and post-quantum crypto"

From: Mouha, Nicky W. (IntlAssoc)
Sent: Tuesday, February 5, 2019 11:15:54 AM
To: Moody, Dustin (Fed)
Subject: Re: Threshold Crypto Workshop

Hi Dustin,

I think that you have a valid point. Perhaps my comment was meant to try to avoid NIST publication numbers (e.g., SP 800-186, FIPS 186-5) if possible, rather than to suggest to include Curve25519 and Curve448.

As you're suggesting, something along the lines of "elliptic curves" or "new elliptic curves" should also be fine. Let us know when you've decided on a final title.

By the way, we've just put a skeleton of the program online, along with a list of accepted submissions: https://csrc.nist.gov/Events/2019/NTCW19

Regards,
Nicky

From: Moody, Dustin (Fed)
Sent: Tuesday, February 5, 2019 11:08 AM
To: Mouha, Nicky W. (IntlAssoc)
Subject: RE: Threshold Crypto Workshop

Got it.

If I am to put Curve 25519, Curve 448 and Post-quantum cryptography all in the title, that seems like it will be really long. Even just the simple “NIST status update on elliptic curves and post-quantum crypto” is lengthy already.

From: Mouha, Nicky W. (IntlAssoc)
Sent: Tuesday, February 05, 2019 11:03 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>

Cc: Chen, Lily (Fed) <lily.chen@nist.gov>; ntcw2019 <ntcw2019@nist.gov>
Subject: Re: Threshold Crypto Workshop

Hi Dustin,

Thanks for accepting! It's great to have you at the workshop.

I'm not sure if the new curves will appear in SP 800-186 or FIPS 186-5. It seems that the information on the NIST website is conflicting about this. But I'm indeed referring to this upcoming NIST standard.

I personally think that it might be a good idea to have some more recognizable algorithm name (e.g., Curve25519/Curve448) in the title of your talk. Nevertheless, choosing the title of your talk is of course up to you...

Regards,
Nicky

From: Moody, Dustin (Fed)
Sent: Tuesday, February 5, 2019 7:31 AM
To: Mouha, Nicky W. (IntlAssoc)
Cc: Chen, Lily (Fed); ntcw2019
Subject: RE: Threshold Crypto Workshop

Sure, Nicky. I'd be happy to do that. By Curve 25519, you mean in regards to FIPS 186?

Dustin

From: Mouha, Nicky W. (IntlAssoc)
Sent: Monday, February 04, 2019 5:23 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>; ntcw2019 <ntcw2019@nist.gov>
Subject: Threshold Crypto Workshop

Hey Dustin,

We see that you've blocked out March 11-12 in your calendar for the threshold workshop. Great! Your participation in the workshop will make a big difference.

We'd like to invite you to give a status update on the upcoming NIST standards for PQC and

Curve25519, right after Lily's talk on how NIST develops cryptographic standards.

Would this be okay for you? We're currently considering a 20-minute slot (including questions) for your presentation, more specifically 11h40-12h00 on March 11.

Regards,
Nicky
On behalf of the workshop organizers