

From: [Brandao, Luis \(IntlAssoc\)](#)
To: [Sonmez Turan, Meltem \(Fed\)](#); [Smith-Tone, Daniel C. \(Fed\)](#); [Robinson, Angela Y. \(Fed\)](#); [Moody, Dustin \(Fed\)](#); [McKay, Kerry A. \(Fed\)](#); [Regenscheid, Andrew R. \(Fed\)](#); [Chen, Lily \(Fed\)](#)
Cc: [Dworkin, Morris J. \(Fed\)](#); [Kelsey, John M. \(Fed\)](#); [Peralta, Rene C. \(Fed\)](#)
Subject: Re: Crypto Rump Session - NIST Update
Date: Friday, August 20, 2021 2:07:30 PM

Links to the videos:

NIST Crypto Update 2021:

<https://www.youtube.com/watch?v=0YyL5adp9sl#t=51m31>

NIST Crypto Exploratory Projects: PEC, Threshold, Masking:

<https://www.youtube.com/watch?v=0YyL5adp9sl#t=1h12m39>

From: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Sent: Tuesday, August 17, 2021 12:22
To: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Subject: RE: Crypto Rump Session - NIST Update

Hi everyone,

I just submitted the crypto rump session slides (attached).

Currently listed authors: Meltem, Dustin, Angela, Daniel ST, Kerry, Lily. I can add more names, please let me know.

Presenter: Meltem

Comments welcome. We are allowed to make changes until 3:40pm today.

Thanks,
Meltem

From: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Sent: Monday, August 16, 2021 7:25 PM
To: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>; Smith-Tone, Daniel C. (Fed)

<daniel.smith@nist.gov>; Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>

Cc: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>

Subject: Re: Crypto Rump Session - NIST Update

Slide-deck on exploratory projects: PEC, Threshold, Masking

<https://www.overleaf.com/6986899581fqdvxrfdcrw>

P.S. The strawberries are based on this year's "swag" motif:

<https://crypto.iacr.org/2021/swag.php>

From: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>

Sent: Tuesday, August 10, 2021 11:55

To: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>

Cc: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>

Subject: RE: Crypto Rump Session - NIST Update

Looks good now. Thanks Daniel.

From: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>

Sent: Tuesday, August 10, 2021 9:30 AM

To: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>; Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>

Cc: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>

Subject: RE: Crypto Rump Session - NIST Update

Oh... Whoops!

I guess I should have spent 100 seconds instead of 50. It also helps reading the error messages. I forgot to put brackets for the nodes. That is a requirement in tikz. There are no error messages now. Do you still want me to make it an included pdf or is it fine now?

Cheers,
Daniel

From: Smith-Tone, Daniel C. (Fed)
Sent: Tuesday, August 10, 2021 9:25 AM
To: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>; Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Subject: RE: Crypto Rump Session - NIST Update

Hi,

I'll try to put the timeline in a pdf image a bit later. I only tried for about 50 seconds, but I couldn't see an easy way to fix the errors. It has something to do with node labels in macros. It may be a difference between def and parameters for newcommand. Not worth my time to fix, though since it compiles anyway. I'll just throw the code in a standalone document and generate a pdf to include.

Cheers,
Daniel

From: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Sent: Monday, August 9, 2021 4:19 PM
To: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Subject: Crypto Rump Session - NIST Update

Hi everyone,

We have updated to the *NIST Crypto Update 2021* presentation to only include the following three projects: PQC, LWC, and Publication Review. (Luis plans to submit a separate presentation for the projects he is participating)

Talk will be on Wednesday (August 18) after 5:30 PM local time. Any volunteers to present? I am available to present as well.

For the speaker, I can provide speaker notes for the LWC and publication review projects. Angela can you provide notes for the PQC project? For now, we can assume to have around 60-90 seconds per project.

Daniel, the PQC timeline is producing two errors, would you be able to fix them? How about including the timeline as a pdf image?

Thanks,
Meltem