From: (b) (6)
To: Moody, Dustin (Fed); Perlner, Ray A. (Fed); Liu, Yi-Kai (Fed)
Cc: Chen, Lily (Fed); Jordan, Stephen P (Fed); Peralta, Rene C. (Fed)
Subject: Re: Latest version of the CFP
Date: Monday, June 6, 2016 1:11:17 PM

I also want some small amount of specificity, but I think that the section seems too academic and congested if we put that in the section itself.

With no explanation we run the risk of everyone choosing their own arbitrary definition after which we need to spend much more time deriving results that should be the responsibility of the submitters. Even with reasonable effort and honesty from submitters, there could be a lot of discrepancy if we don't provide some guidance on this.

I still don't think that specifics should be in the section itself because it detracts from the point of the section, saying what security strengths we want. I think that the FAQs is a good idea.

I would add that it might be a good idea to not be so specific as to regret it later. We should specify the basic idea, with little more detail than Ray said in the previous email.

Cheers,
Daniel

Sent from my T-Mobile 4G LTE Device

-------- Original message --------
From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date:06/06/2016 7:56 PM (GMT+02:00)
To: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, Daniel (b) (6), "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>
Cc: "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, "Peralta, Rene (Fed)" <rene.peralta@nist.gov>
Subject: Re: Latest version of the CFP

I think the FAQ is a good idea. That makes 2 topics so far - the other being more on hybrid modes.

Dustin

From: Perlner, Ray (Fed)
Sent: Monday, June 6, 2016 12:55:16 PM
To: Daniel; Moody, Dustin (Fed); Liu, Yi-Kai (Fed)
Cc: Chen, Lily (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed)
Subject: RE: Latest version of the CFP

On further consideration, I think we are probably better off being explicit about how we handle parallelism. This means stating that our block cipher definition implies that computational complexity is measured by depth times space when measuring classical security and depth times squareroot space when measuring quantum security. I realize there was some disagreement over this. I'm ok with including this statement in a FAQ instead, but I think people will get confused if we aren't explicit about it.

From: Daniel (b) (6)
Sent: Monday, June 06, 2016 12:49 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
Subject: Re: Latest version of the CFP

Ray sent me a note discussing 4.A.4 again. I think he may have a further suggestion. Maybe we should slightly tweak the section further.
Sent from my T-Mobile 4G LTE Device

-------- Original message --------
From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date:06/06/2016 7:29 PM (GMT+02:00)
To: "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, Daniel Smith (b) (6) , "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Cc: "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, "Peralta, Rene (Fed)" <rene.peralta@nist.gov>
Subject: Re: Latest version of the CFP

Everyone,

The lawyers are moving fairly quickly along in the process for us to get a notice in the FRN about our Call for Proposals. They're sending it downtown to the lawyers there. Andy needed the latest "clean" version, so I used Daniel's text for section 4.A.4. If you have any changes you want made to what Daniel wrote, please let me know soon. I've attached the latest version.

Thanks!

Dustin

From: Liu, Yi-Kai (Fed)
Sent: Thursday, June 2, 2016 2:30:10 PM
To: Moody, Dustin (Fed); Daniel Smith; Perlner, Ray (Fed)
Cc: Chen, Lily (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed)
Subject: Re: Latest version of the CFP

Hi Daniel,

Thanks for working on this! I think your version looks fine. I like the more assertive tone, and the brevity.

Cheers,

--Yi-Kai

From: Moody, Dustin (Fed)
Sent: Thursday, June 2, 2016 1:12 PM
To: Daniel Smith; Perlner, Ray (Fed)
Cc: Chen, Lily (Fed); Liu, Yi-Kai (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed)
Subject: Re: Latest version of the CFP

Daniel,

Thanks for the suggestions. Can you work with Ray/Yi-Kai to further edit this section? Or do you want to discuss it in a meeting? Thanks.

Dustin

From: Daniel Smith (b) (6) [redacted]
Sent: Thursday, June 2, 2016 11:06:17 AM
To: Perlner, Ray (Fed)
Cc: Moody, Dustin (Fed); Chen, Lily (Fed); Liu, Yi-Kai (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed)
Subject: Re: Latest version of the CFP

Hello,

Please find attached another potential version of section 4.A.4. I don't like the previous version very much, and I'm not sure if I like my current suggestion much better. (In both cases, for example, the paragraph on special-purpose hardware, though certainly related to a practical determination of the security of a scheme, doesn't seem to fit well with the focus of the rest of the section.)

My complaint on the previous version is that it seems too much like academic justification of concepts as opposed to a technical description of requirements for our process. My concern in my version is that I've removed too many details for the motivation (for which the previous version clearly strived) for the reasonableness of the approach to be seen. I'm wondering if it is possible to have a middle ground in which we use something more spare and precise and offer a resource for justification.

Anyway, I submit this version for dissection and consideration. I've included it in a separate file (Section 4A4.docx) since it is a dramatic reordering of the material and I don't want to destroy notes if you think this approach is not worthwhile.

Cheers,
Daniel

On Wed, Jun 1, 2016 at 11:53 AM, Daniel Smith (b) (6) [redacted] wrote:
4.A.4 is quite complicated now. It seems pretty precise, but it is very complicated. It almost reads like a call to the community to figure out quantum security so that we can have an opinion instead of an explanation of the security levels we're calling for.

I don't think that I like the organization of it. As it is, a description of our requested security levels and a lengthy explanation afterwards, it reads like we are trying to make up an explanation for our claims, but that we don't know what we are doing and are taking a wild guess; I don't think that this is what we want to come across as saying. I think that the language needs to be more assertive and the order changed.

I'm not working today, and I don't have enought time to produce a version reflecting exactly what I'm trying to say, but here's a rough outline of how 4.A.4 should be arranged in my opinion. I hope that it can illustrate my idea of how the section should be.

The section should consist of four points (not numbered as below):
I. A statement similar to what is currently in the section saying that quantum security levels are something for which there is no current consensus.
II. An assertion that we intend to use the definition based on block ciphers as written in the current version acknowledging that that definition may change.
III. The list of desired security levels presented in a submission.
IV. A statement about our consideration of security against special purpose technology.

I don't think that more explanation than this is needed, and I also think that presenting the message this way shows that our decision on this is a mature one and not a desperate edit after the document was written. The rest of what is written in the current version of 4.A.4 seems more like part of an introduction to an academic paper (which perhaps it should be), but doesn't seem appropriate to me for the CFP.

Cheers,
Daniel

On Wednesday, June 1, 2016, Perlner, Ray (Fed) <ray.perlner@nist.gov<mailto:ray.perlner@nist.gov>> wrote:
Here are some suggested edits for sections 4.A.4 and 2. B. 4

From: Moody, Dustin (Fed)
Sent: Tuesday, May 31, 2016 11:05 AM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu) <daniel-c.smith@louisville.edu>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
Subject: Latest version of the CFP

Everyone,
Hope everyone had a nice long weekend. I've attached the latest version of the CFP, which incorporates some changes to clarify some of the things the NSA comments discussed. Most of them are minor. The biggest addition is to the quantum security section in 4.A.4, which Ray and Yi-Kai wrote. We also removed any mention of FIPS or validation when talking about hybrid modes. We can address that in a FAQ on our website. Let me know if there are any comments on anything. Thanks!

Dustin