From:	Peralta, Rene (Fed)
To:	(b) (6) ; Perlner, Ray A. (Fed)
Cc:	Moody, Dustin (Fed); Chen, Lily (Fed); Liu, Yi-Kai (Fed); Jordan, Stephen P (Fed); Peralta, Rene C. (Fed)
Subject:	Re: Latest version of the CFP
Date:	Thursday, June 2, 2016 11:29:03 AM

I don't have strong feelings about this. My inclination is to tell the submitters that it is incumbent upon them to convince us and the community at large of their security claims (and leave it at that).

Ray told me he expects people to argue security by saying something like
- the best algorithm we can think of is XXX
- an analysis of XXX shows that these parameters are good enough.

I don't like that too much. I would rather see an argument like
- the security seems closely related to well-studied problem XXX (e.g. subset-sum)
- a (very conservative) estimate is that breaking the proposed algorithm with this parameter set is at least as hard as solving XXX of a given size. Ergo my security claim.

I guess I would rather not steer the submitters to a particular security argument.
But I am willing to go with whatever the rest of the team wants.

Rene.

From: Daniel Smith (b) (6)
Sent: Thursday, June 2, 2016 11:06 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) 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> 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