From: Peralta, Rene (Fed)
To: Chen, Lily (Fed); Moody, Dustin (Fed); Perlner, Ray A. (Fed); Jordan, Stephen P (Fed); (b) (6) ; Liu, Yi-Kai (Fed)
Cc: Bassham, Lawrence E. (Fed)
Subject: perfect forward secrecy
Date: Tuesday, March 29, 2016 9:50:28 AM

I think perfect forward secrecy is overhyped. Long term keys should be both protected and changed with adequate frequency. If you can't do that, then I think you have bigger problems than lack of forward secrecy.

Rene.

From: Chen, Lily (Fed)
Sent: Monday, March 28, 2016 4:04 PM
To: Moody, Dustin (Fed); Perlner, Ray (Fed); Jordan, Stephen P (Fed); Daniel Smith; Liu, Yi-Kai (Fed)
Cc: Peralta, Rene (Fed); Bassham, Lawrence E (Fed)
Subject: RE: My write-up in the PQC call

Attached please see my comments. Some of them are questions to be discussed tomorrow.
Lily

From: Moody, Dustin (Fed)
Sent: Monday, March 28, 2016 12:38 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; (b) (6) Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Subject: RE: My write-up in the PQC call

I've added in a few more comments (mostly questions) also.
Note – our meeting location tomorrow is A-318.
Dustin

From: Perlner, Ray (Fed)
Sent: Monday, March 28, 2016 10:19 AM
To: Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; (b) (6) Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
Subject: RE: My write-up in the PQC call

I've added a few more comments

Good luck everyone,
Ray

From: Jordan, Stephen P (Fed)
Sent: Sunday, March 27, 2016 9:49 PM
To: (b) (6) Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
Subject: Re: My write-up in the PQC call

Dear All,
I've added a few additional comments. The resulting file is attached.
Best regards,
Stephen

From: (b) (6)
Sent: Saturday, March 26, 2016 1:03 AM
To: Liu, Yi-Kai (Fed)
Cc: Moody, Dustin (Fed); Perlner, Ray (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed)
Subject: Re: My write-up in the PQC call

Hello,
Here is my first attempt at giving some sort of minor contribution. A couple of items I didn't know exactly how to handle. The rest is mostly plagiarized from the SHA-3 call so that we at least have a draft to work with.
Also, I'm using Word 2016. I chose compatibility mode,so I hope that there are no issues with this.
Cheers,
Daniel
On Fri, Mar 25, 2016 at 9:29 AM, Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov> wrote:

> Hi everyone,
> Here is a combined version of the document. (Thanks Dustin for your help with this.)
> Could everyone look at it? Please flag any sections that need additional work, and flag any issues that we need to discuss when we meet next Tuesday.
> Many thanks!
> --Yi-Kai
>
> ---
>
> **From:** Liu, Yi-Kai (Fed)
> **Sent:** Thursday, March 24, 2016 5:55 PM
> **To:** Daniel; Moody, Dustin (Fed); Perlner, Ray (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
>
> **Subject:** Re: My write-up in the PQC call
> Hi Daniel,
> (b) (6)
> --Yi-Kai

From: (b) (6)
Sent: Thursday, March 24, 2016 4:38 PM
To: Liu, Yi-Kai (Fed); Moody, Dustin (Fed); Perlner, Ray (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Subject: Re: My write-up in the PQC call

(b) (6)
(b) (6)
(b) (6)
(b) (6)

my T-Mobile 4G LTE Device

-------- Original message --------
From: "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>
Date:03/24/2016 2:10 PM (GMT-05:00)
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, "Peralta, Rene (Fed)" <rene.peralta@nist.gov>, "Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)" <daniel-c.smith@louisville.edu>
Cc:
Subject: Re: My write-up in the PQC call
Hi everyone,
Here is my section of the CFP.
Thanks everyone! Daniel, feel free to send it whenever you're ready.
Later today or tomorrow, I'll try to merge everyone's contributions into one document, and send it around.
--Yi-Kai

From: Moody, Dustin (Fed)
Sent: Wednesday, March 23, 2016 11:49 AM
To: Liu, Yi-Kai (Fed); Perlner, Ray (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Subject: FW: My write-up in the PQC call

From: Bassham, Lawrence E (Fed)
Sent: Wednesday, March 23, 2016 11:32 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: My write-up in the PQC call
My sections. Let me know if you need more.
Larry