From: Moody, Dustin (Fed)
To: (b) (6) [redacted]; Dang, Quynh H. (Fed)
Cc: Smith-Tone, Daniel C. (Fed)
Subject: Re: Our Kyber and Saber review slides.
Date: Friday, October 29, 2021 9:51:23 AM

Thanks, Daniel.

Looks fine. We'll cover everything at some point of one of our slides.

From: Daniel Smith (b) (6) [redacted]
Sent: Friday, October 29, 2021 9:47 AM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>
Subject: Re: Our Kyber and Saber review slides.

Hi,

I made some slides for NTRU. Nothing really except a description of the scheme. There is nothing really new to report except for things that are already in the comparison, so I don't think that there is much more I can do.

Let me know if you want me to change anything.

Cheers,
Daniel

On Thu, Oct 28, 2021 at 1:30 PM Dang, Quynh H. (Fed) <quynh.dang@nist.gov> wrote:

> q for Kyber was wrong.
>
> q for Saber is 2^13.
>
> ---
>
> **From:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
> **Sent:** Thursday, October 28, 2021 10:35 AM
> **To:** Daniel Smith (b) (6) [redacted]; Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
> **Cc:** Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>
> **Subject:** Re: Our Kyber and Saber review slides.
>
> Greetings to you too, earthling,
>
> If you want to give a few slides on NTRU, I think that'd be good. Quynh will cover Kyber and Saber. Then you can go.
>
> I agree that we can go through these fairly quickly, spending more time on comparing, contrasting, and discussing.

> I've attached my most recent version of the slides. Let me know if you have corrections.
>
> As for Tuesday - I sent out a meeting summary. Did you get it?
>
> We did have a meeting with the NSA last week.   They mainly told us about their approach to hybrid schemes. Andy sent an email summarizing it. Did you get that?
>
> Dustin
>
> ---
>
> **From:** Daniel Smith (b) (6)
> **Sent:** Thursday, October 28, 2021 10:32 AM
> **To:** Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
> **Cc:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>
> **Subject:** Re: Our Kyber and Saber review slides.
>
> Hi, fellow humans (so far),
>
> In preparation for the zombie apocalypse I read through the slides you sent. I'm not sure what is left for me to do! My plan is to look through the spec for anything that stands out to me when I consider the perspective we've developed on our situation through the third round and to write down some notes and talking points. Is there anything specific you would like me to include in the discussion?
>
> I have noticed a few typos in the slides, but it is worthless to correct them if the figures are then incorrect. So I will wait in case you have another version.
>
> I have a feeling that it would be best to go rather quickly through the data and points on the slides and spend more time on the discussion. That way we can be sure to make progress. (Since recalling data likely won't help form opinions, but discussing it might.)
>
> Also, I'm sorry I couldn't attend on Tuesday. What did I miss? Also, wasn't there a meeting with NSA recently? Is there anything that I should know from that? Thanks.
>
> Cheers,
> Daniel
>
> On Wed, Oct 27, 2021 at 10:45 AM Dang, Quynh H. (Fed) <quynh.dang@nist.gov> wrote:
>
>> I think the m4 version of Kyber is optimized for stack, not for speed (even though it has some cycle improvements over its clean version).
>>
>> I think a Kyber optimized for speed version would be faster than Saber's speed optimized version.
>>
>> Quynh.
>>
>> ---

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, October 27, 2021 10:32 AM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
Subject: Re: Our Kyber and Saber review slides.

I'll use m4 of Kyber for both then. Same for NTRU (meaning use the same for both speed-optimized and memory-optimized)

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Wednesday, October 27, 2021 10:29 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
Subject: Re: Our Kyber and Saber review slides.

m4 of Kyber for both. See my comparison slides. Kyber has much less memory requirements.

If only one implementation m4 of kyber, then kyber is truly amazing.

If there are 2 versions of kyber m4 (one for speed and the other for stack), then that is fine (the same with Saber).

The fact is that depending on a user's purpose, what direction they would like to write their code.

Quynh.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, October 27, 2021 10:24 AM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
Subject: Re: Our Kyber and Saber review slides.

Well, what is the right comparison?

Saber has 2 versions - stack and for speed.
Kyber only has one - presumably speed.

I do have a chart showing memory used. Kyber is a little less than Saber.

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>

Sent: Wednesday, October 27, 2021 10:22 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
Subject: Re: Our Kyber and Saber review slides.

saber has both for stack and speed. kyber: m4 for both speed, and memory under Memory Evaluation.

The m4 for kyber could be 2 different implementations, but that is not matter.

Quynh.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, October 27, 2021 10:15 AM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
Subject: Re: Our Kyber and Saber review slides.

Quynh,

pqm4 seems to only have memory-optimized for Saber. So how can we compare that?

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, October 27, 2021 10:06 AM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
Subject: Re: Our Kyber and Saber review slides.

I can add the memory optimized numbers to give a more complete picture.

Thanks.

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Wednesday, October 27, 2021 10:04 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
Subject: Re: Our Kyber and Saber review slides.

Hi Dustin,

I think your performance slides for Kyber and Saber are kinda wrong.

For pqm4, there are 2 options: optimized for speed or optimized for memory usage.

For the former, you are correct that Saber is about 10% better, but for the latter Kyber is about 25-30% better.

For pqm4 and constrained devices, the big gap in memory usage is important and 10% cycle count difference is not that important in comparison.

Quynh.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, October 27, 2021 9:32 AM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith <(b) (6)
Subject: Re: Our Kyber and Saber review slides.

Quynh,

You have two slides where you copied performance charts from the Kyber and Saber spec documents. The aspect ratio is changed so that the perspective in your slides makes them look off. Maybe try copying them again, and when you re-size them, hold down the shift key so that the ratio of the dimensions stay the same.

Dustin

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Wednesday, October 27, 2021 9:26 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
Subject: Re: Our Kyber and Saber review slides.

Hi Dustin and Daniel,

Attached is updated slide deck. Again, comparisons slides are for back-up just in case we need them.

Quynh.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Monday, October 25, 2021 2:29 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
Subject: Re: Our Kyber and Saber review slides.

Quynh,

Thanks for adding NTRU. As my part - I'll make sure to take over the comparisons. I'll have some more slides soon.

Dustin

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Monday, October 25, 2021 2:27 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith <(b) (6)
Subject: Re: Our Kyber and Saber review slides.

Sorry, the correct version is attached.

Quynh.

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Monday, October 25, 2021 2:25 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith <(b) (6)
Subject: Re: Our Kyber and Saber review slides.

Attached is updated slide deck.

I included more slides to include NTRU.

I did not have all NTRU levels, I used only 2 of them to show that Saber and Kyber are clearly better in performance than NTRU.

Quynh.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Monday, October 25, 2021 11:08 AM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
Subject: Re: Our Kyber and Saber review slides.

Quynh,

The slides look good to me. My only question is if we want to do your Kyber/Saber comparison slides at the end of your part, or if we want to wait and do a combined NTRU/Kyber/Saber comparison after you and then Daniel.

> > I do think we want to help provide info to answer 2 questions:
> >
> > 1. which of kyber/ntru/saber do we prefer (considering IP issues)
> > 2. If IP wasn't an issue, do we prefer kyber/saber over NTRU? And if so, which of kyber/saber?
> >
> > Dustin
> >
> > ---
> >
> > **From:** Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
> > **Sent:** Monday, October 25, 2021 10:30 AM
> > **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
> > **Subject:** Our Kyber and Saber review slides.
> >
> > Hi Dustin and Daniel,
> >
> > Attached is a slide deck that I have created.
> >
> > If you like to improve them, please do.
> >
> > Quynh.