From: Moody, Dustin (Fed)
To: (b) (6)
Subject: Re: Kyber"s response discussion tomorrow ?
Date: Thursday, June 4, 2020 3:18:31 PM

Gracias.

From: Daniel Smith (b) (6)
Sent: Thursday, June 4, 2020 3:14 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Kyber's response discussion tomorrow ?

I am working towards it. I have been looking again at the specs so that I can see if there is anything more meaningful for me to say on the schemes. I think that there are some meaningful things I can say to the GeMSS team. (Quynh asked me if I could cover that one and I agreed.)

I'm not putting off Section 3 (the contentious one), so don't worry. I just think that I'll have a better grasp of how that one will go when I decide on the content with respect to the schemes I'll be addressing specifically.

On Thu, Jun 4, 2020 at 2:51 PM Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

> Daniel,
>
> Are you planning on editing the report sometime? Just checking. I am trying to keep the revision moving along. Thanks,
>
> Dustin
>
> ---
>
> **From:** Daniel Smith (b) (6)
> **Sent:** Thursday, June 4, 2020 2:23 PM
> **To:** Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
> **Cc:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>; Dang, Thinh H. (Fed) <thinh.dang@nist.gov>
> **Subject:** Re: Kyber's response discussion tomorrow ?
>
> Hmmm...
>
> They are calling us out explicitly to offer our position on this. It is a muddy issue in my mind.
>
> I have a bit of a problem with saying, "We are secure because of other stuff that we can't measure really well." For other areas we have been requiring them to ignore memory costs even when that makes a difference for them.
>
> A clear example comes to mind: GeMSS. For GeMSS they had a quite exhaustive analysis of known techniques applied to GeMSS. They quite conservatively used analyses and

coefficients that are unrealistic even with zero cost of memory and memory access (which is why confusingly they chose to report some of the numbers as lower than the security bounds when actually they should be fine). When you consider the hidden polynomial factors or actual coefficients, the least costly attack (and the one they are basing the parameters on) is the direct algebraic attack. They are being super conservative and choosing a linear algebra exponent of 2 for dense linear algebra (I think that we can't use sparse techniques here because of the number of solutions (or the density after fixing variables)), but if we take memory into account, then the complexity is altogether different. If our metric is New York City, then this scheme should benefit fairly significantly.

On a historical note, Ray and I argued fairly extensively about this memory issue when we were drafting the CFP. I recall having discussions about the physical feasibility of converting Jupiter into atomic scale memory that violates causality with the speed of its access (sending replies and being set to different values before being asked to) leading up to the release of this document. The issue as I recall was allowing the community to address some complexity issues that had not been pinned down yet at the time and for the community to come to a consensus on how to address these things. Still, we need to have some standard metric for comparisons between schemes.

I think that it is entirely reasonable to address memory and memory access in a cost model. A problem occurs when we lack justification and when we lack consistency in how we apply restrictions in these analyses. Ray and I were arguing on the level of Jupiter and breaking the laws of physics, whereas Kyber is arguing on the level of the 5 boroughs.

I would be open to allowing teams to specify their cost model addressing memory (in communication with us and with clear justification and theoretical support), and to adjust parameters accordingly. This would need to take place extremely quickly, though, to not make analysis placed on a moving target.

The easiest way to handle the situation is exactly the opposite, though. That is to let the teams do what they are doing and then judge them by our own metrics. The downside of this approach is that there is plenty of room for bias and plenty of reason for skepticism in our choices if any parts of our community think that we are cutting corners unreasonably.

If we chose to allow memory access cost as part of the complexity analysis, there will be consequences. We may have to communicate with each team explicitly, but I think we should make it clear (if we go that route) that they should analyze the memory concerns with strong justification for **minimal** cost models that they can then incorporate. We also need to assess the feasibility of these models and the appropriateness of the bounds they suggest.

I think that we have plenty to talk about, but we'll follow your lead, Dustin.

Cheers,
Daniel

On Thu, Jun 4, 2020 at 1:47 PM Dang, Quynh H. (Fed) <quynh.dang@nist.gov> wrote:

> I think so. If more people think that a talk tomorrow would be good, then I would ask you to consider that.
>
> ---
>
> **From:** Moody, Dustin (Fed) <dustin.moody@nist.gov>

Sent: Thursday, June 4, 2020 1:41 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>; Daniel Smith (b) (6) [redacted]; Dang, Thinh H. (Fed) <thinh.dang@nist.gov>
Subject: Re: Kyber's response discussion tomorrow ?

I think we can discuss via email.

I don't think we need to have a meeting tomorrow. Maybe on Tuesday.

Let me know if you think otherwise.

Dustin

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Thursday, June 4, 2020 1:34 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>; Daniel Smith (b) (6) [redacted]; Dang, Thinh H. (Fed) <thinh.dang@nist.gov>
Subject: Kyber's response discussion tomorrow ?

Hi Dustin,

Are we going to discuss Kyber's response tomorrow at 10 ?

Quynh.