From: David A. Cooper
To: Moody, Dustin (Fed); internal-pqc
Subject: Re: PQC
Date: Tuesday, June 30, 2020 9:41:37 AM

I'm not particularly concerned with whether we explicitly say something in our report about what we would do in the unlikely event that all structured lattice KEMs are broken (or some similar event). We can deal with that when/if it happens. I also agree with Daniel that we may need to strongly consider extending the third round if that were to happen.

I'm okay as long as it is agreed that we will not standardize something currently on the alternate list at the end of the third round without providing advance notice to the community that this is a possibility. Whether we explicitly say that in the report is much less important.

On 6/30/20 8:59 AM, Daniel Smith wrote:

> I don't think that we need any language in the report stating that we may elevate an alternate to the status of finalist. I think that any circumstance that would make us go that route will likely be a big enough event that it would be no surprise to anyone that we may need to pause and regroup--- re-organize the project. I don't think that we should get hung up on low probability events that muddy the description of the project.

On 6/30/20 8:58 AM, Moody, Dustin (Fed) wrote:

> I don't think we are as confused as we think we are.
>
> 1) From what I'm seeing (and we've discussed before), we seem to agree that if nothing happens to the finalists, then we would only standardize finalists at the end of the third round. Part of our decision process was that in this scenario, any alternate we wanted to standardize could wait, since we have good finalists.
>
> 2) If there is some new research that breaks some of the finalists, then we would obviously want to make some changes. That may include deciding to consider some of the alternates sooner/more seriously.
>
> 3) Lastly, if we are considering standardizing something at the end of the third round, then it should be a finalist. I think that's what we understood, and made our decisions what that in mind. Schemes like Sphincs+ and Frodo we said were good backups, in case of some attack on structured lattices. But if the structured lattices weren't broken, we were okay to get our high priority ones standardized first, and these other schemes could wait a bit. That's explained in our write-ups.
>
> We can discuss at 10am for anybody that is around. Andy's suggested text fits in

with the above very easily.

Dustin