Hi Dustin,

Thanks for looking over the document. As you say, it may be necessary to schedule a meeting in order to get people to comment on the issues I raised. I had hoped that sending out that email would have been enough to get other people assigned to work on the specification (John and Thinh) to look at it.

Perhaps we can use some time at a weekly PQC meeting to discuss some of the issues related to SPHINCS+.

David

On 6/13/22 10:34 AM, Moody, Dustin (Fed) wrote:

> David,
>
> I read through it all straight through, without doing a deep dive to check the algorithms. I made some small edits and made a few comments. It may be good to schedule a meeting to force people to answer the questions you want answered! We could use some of the time in our weekly PQC meetings if desired.
>
> Dustin
>
> ---
>
> **From:** Cooper, David A. (Fed) <david.cooper@nist.gov>
> **Sent:** Wednesday, June 1, 2022 2:49 PM
> **To:** Dang, Thinh H. (Fed) <thinh.dang@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
> **Cc:** internal-pqc <internal-pqc@nist.gov>
> **Subject:** SPHINCS+ write-up
>
> Hi all,
>
> I've started work on the SPHINCS+ specification. So far, I've written up all of the algorithms and some figures, but have written practically no text.
>
> I've started to collect a set of issues to be addressed by the group, some technical issues and some presentation issues. They are in the file notes.tex and appear in the document on page ii under "Note to Reviewers." Anyone who is interested is welcome to review and comment on the questions that I've asked in that file or to add additional questions to the notes.tex file.

Thanks,

David