From:	Miller, Carl A. (Fed)
To:	Moody, Dustin (Fed)
Subject:	Re: Upcoming review process
Date:	Monday, October 25, 2021 4:38:39 PM

Ok – they wrote back. Thanks.

-Carl

--
Carl A. Miller
Mathematician, NIST Computer Security Division
Fellow, Joint Center for Quantum Information and Computer Science (QuICS)
https://camiller.iacs.umd.edu

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Date: Monday, October 25, 2021 at 11:57 AM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Subject: Re: Upcoming review process

Just chatted with Ray - he'll respond after lunch.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Monday, October 25, 2021 11:53 AM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Subject: Re: Upcoming review process

Carl,

Thanks for letting me know. Let me see if I can get ahold of them. It'd be good to have all of you helping, not just you!

Dustin

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Monday, October 25, 2021 11:52 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: FW: Upcoming review process

Hi Dustin –

I just wanted to check in with you about our upcoming PQC review presentations. I've written to Ray

& John twice about our SPHINCS+/Classic McEliece presentation, and I've gotten no response.

I could try to talk to them about it at the next PQC meeting. But, if they're not enthusiastic about this presentation, I don't really want to be the person bugging them to get it done …

I could just put together a presentation of part of SPHINCS+/Classic McEliece on my own (and let them know what I'm doing, so they'll be able to cover other stuff). I'd be most comfortable talking about the abstract aspects of the protocols: protocol design, security proof & assumptions, and maybe something about performance. (I'd review any relevant resources while I'm preparing the talk.) What do you think?

-Carl

--
Carl A. Miller
Mathematician, NIST Computer Security Division
Fellow, Joint Center for Quantum Information and Computer Science (QuICS)
https://camiller.iacs.umd.edu

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Date: Thursday, October 21, 2021 at 12:06 PM
To: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>, Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Subject: Re: Upcoming review process

Hi Ray & John –

This is a reminder that we should talk about how to present SPHINCS+ and Classic McEliece. Please let me know what you think. (We could also do a videoconference.)

I expect most of the work will be on achieving full coverage of the resources that Dustin has listed, and then writing and assembling the presentation slides.

-Carl

--
Carl A. Miller
Mathematician, NIST Computer Security Division
Fellow, Joint Center for Quantum Information and Computer Science (QuICS)
https://camiller.iacs.umd.edu

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>

Date: Thursday, October 14, 2021 at 8:45 AM
To: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>, Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Subject: Re: Upcoming review process

Hi Ray & John –

Shall we talk a little about our presentations of SPHINCS+ and Classic McEliece? We can figure out how to divide up the work. Some thoughts:

- Two things that I'm a good position to help with are (1) giving the audience a refresher about how the schemes work and (2) giving an overview & discussion of the security arguments. (Also, there's elementary stuff, like just re-reporting performance numbers, that I can certainly also do.)
- Since there's no particular relationship between them, it might make sense to have two separate presentations back to back (rather than one unified presentation).

-Carl

--
Carl A. Miller
Mathematician, NIST Computer Security Division
Fellow, Joint Center for Quantum Information and Computer Science (QuICS)
https://camiller.iacs.umd.edu

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Date: Wednesday, October 13, 2021 at 11:54 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Upcoming review process

Everyone,

Just thought I'd try and collect some ideas of what to consider/include as you work on our review presentations. Recall our assignments. I'd suggest teams work together to decide how they want to approach this.

- Kyber/Saber/NTRU
  - Quynh, Dustin, Daniel ST
- Falcon/Dilithium
  - Daniel Apon, David, Rene
- Classic McEliece. Sphincs+
  - Ray, Carl, John
- Alternate KEMs: Frodo, NTRUprime, BIKE, HQC, SIKE

        - Angela (Bike, HQC), Yi-Kai (SIKE, NTRUprime), Gorjan
    - Signatures: Rainbow, GeMSS, Picnic
        - Jacob, Ray, Thinh

A list of some resources or things to look at:

- The submission team specifications
    - Most teams also have a website
- Official comments and discussions on the pqc-forum
- Submission team presentations during the 3rd workshop
- IP statements, or anything known regarding patents
- Our Round 2 report, as well as any tweaks made at the start of the 3rd round
- Research papers
    - Add relevant ones to our master list on sharepoint
- Internal team presentations on sharepoint
- Our Round 3 Bullet Points document on sharepoint. Also list important questions here
- Benchmarking websites
- Feedback sent to us via pqc-comments@nist.gov. (We asked for feedback by Oct 31)
- Probably others that I am forgetting

Keep in mind our evaluation criteria. Here's a summary:

- Security
    - Security categories offered, (confidence in) security proof, any attacks, classical/quantum complexity
- Performance
    - Size of parameters, efficiency of KeyGen, Enc, Dec, Sign, Verify in software/hardware, decryption failures or other implementation issues to be aware of, real-world experiments
- Algorithm and implementation characteristics
    - Advantages and disadvantages, IP status, side-channel resistance (constant-time code?), simplicity and clarity of documentation, flexibility

For candidates that have other candidates to directly compare to, it'd be good to have comparisons for the evaluation criteria to help us decide.

Please add any comments or suggestions! Thanks,

Dustin