From: Celi, Christopher T. (Fed)
To: Chen, Lily (Fed)
Cc: Booth, Harold (Fed); Moody, Dustin (Fed)
Subject: RE: Post-Quantum Crypto Competition
Date: Monday, December 18, 2017 11:27:05 AM

Thanks for the information. For some reason when I searched earlier I couldn't find that page on the CSRC, so thank you for the link. I requested to join the mailing list. What you suggested is essentially what I'd like to do with these algorithms. As I understand there are a handful of structures that many are based on. I look forward to receiving the list of qualified candidates.

Thanks,
Chris Celi

From: Chen, Lily (Fed)
Sent: Monday, December 18, 2017 11:14 AM
To: Celi, Christopher T. (Fed) <christopher.celi@nist.gov>
Cc: Booth, Harold (Fed) <harold.booth@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Post-Quantum Crypto Competition

Hi, Chris,

Thank you for reaching out. You are welcome to join the mailing list and meetings for post-quantum cryptography standardization. We received about 82 submissions. Right now, our team is opening packages and checking whether a package is "complete and proper". We will post qualified submissions very soon (probably before Xmas). I include our project lead, Dustin Moody, in this e-mail.

We have a rough timeline (see https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline). We probably will not make any "narrowing down" until 2019 and any tentative selection until 2020 or even 2021. To prepare testing, for such a large number of candidates, I think it is important to understand the different categories and their implementations. Once we post all the qualified candidates, you can study the implementations submitted by the design teams.

One thing I like to remind is that we do not consider it as a "competition" as in SHA-3 competition. We call it a "process". On the other hand, the internal discussions are confidential as in SHA-3. If you participate in the meetings and receive e-mails, please consider that all the internal discussions are confidential.

If you have any question, please let us know. We are more than happy to help you to prepare for the future testing of PQC standards.

Thanks,

Lily

From: Celi, Christopher T. (Fed)
Sent: Friday, December 15, 2017 6:24 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: Booth, Harold (Fed) <harold.booth@nist.gov>
Subject: Post-Quantum Crypto Competition

Hi Lily,

I'm Chris and I'm working with Harold and Apostol on the ACVP to eventually replace CAVS.

One of the things that Sharon did in the past was sit in on meetings the CT Group has had to talk about upcoming drafts and proposals for new algorithms and standards. As well, for the future, we want to be able to support the testing and validation of algorithms as they are released rather than have a period of time playing catch-up.

Would it be possible for me to join the email list or group to learn more about the finalists for the Post-Quantum Crypto Competition, and potentially participate in the meetings you all have as the final algorithm is selected and a draft is prepared?

I understand the process towards narrowing down a final algorithm can take several years. The process for developing validation tests for these fundamentally different algorithms could also take some time. It is always beneficial to learn about the algorithms early.

Thanks,
Chris Celi
Security Test, Validation and Measurement Group