From: Dang, Quynh (Fed)
To: Moody, Dustin (Fed)
Subject: Re: PQC meeting summary
Date: Friday, August 30, 2019 8:38:17 AM

Hi Dustin,

I would like to know what the performance improvements for NTRU if they are changed to allow the decryption failure rates around their security levels.

That is one of the 2 things that I would like to know in order to compare NTRU/NTRUprime with Saber/Kyber/NewHope.

Should I ask John Schank that question ?

Quynh.

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Thursday, August 29, 2019 4:02:13 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: PQC meeting summary

Dustin,

My understanding is that the KDFs currently support adding additional randomness in, which is a quick way to do a hybrid scheme. But they need a variant to handle key material from multiple schemes in their "shared secret" field.

--John

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, August 29, 2019 at 15:38
To: internal-pqc <internal-pqc@nist.gov>
Subject: PQC meeting summary

Everyone,

Thanks for all the lively discussion! Here's a recap of what we talked about. If I got anything wrong, feel free to correct it.

- Daniel A. will present Picnic on Sep. 17th. John will schedule a time for SPHINCS+. (Those are the last 2 we have to cover).
- We agreed that removing the lifting technique from LUOV would be a system re-design, and not just a tweak. Even though we'd like to have an unbalanced oil and vinegar scheme, this goes against our rules.

- NSF funding. Dustin will continue to talk with Andrew Pollington from the NSF about how we can help them to promote research in the field. We can recommend specific areas we'd like to see, for example, cryptanlaysis, hardware, gap in lattice schemes between practical instantiations and provable security. Carl also mentioned that there is an initiative coming out of UMD that they are hoping the NSF will fund. He'll tell us more soon.
- Daniel A. will follow up with Jens-Peter about why his numbers seem off. Also with Kris Gaj's suggestion to add 2 more hardware platforms for focus. Perhaps post on the pqc-forum to see if they will increase activity there.
- Angela graciously volunteered to try and create a document about some of our target applications/possible tradeoff scenarios we might be interested in.
- We all seem to be in agreement that we will need to have a 3rd round. We will post on the forum our future plans to let people know.
    - We'd like teams to have announced (or have finished?) mergers by Feb 14. Do we want to take a more active role in making some mergers happen?
    - We'll inform the community that roughly after April 15 we may not be able to consider new implementations, research, etc as we make our decisions. So make sure you get stuff done before then!
    - We tentatively plan that sometime in June-ish we will be ready to announce 3rd round candidates. This may include indicating that we have more confidence in some schemes, and others we want more research, etc. (buckets)
    - We should let the community know that we also may pare out some of the parts of a submission, to narrow down parameter sets.
- The group working on 56-C will look at including additional information in KDF's, that may help with a hybrid mode. We may want to re-state NIST's position/advice about hybrid modes
- We potentially could try to organize some more workshops, but we will try to encourage others to host workshops for the various families, and promise our help, participation and support. We'd encourage having tutorials associated with these.
- For PQCrypto 2022, we will continue to be available as a host if needed, but it might be nice to have a local university host? We will talk with Sara more about this.
- We also recapped the IP situation, and some notes from a meeting with some of our EU colleagues. We have a meeting with NIST's lawyers next week – we'll let you know how it goes.

Thanks! Feel free to add any other comments.

Dustin