From: Apon, Daniel C. (Fed)
To: Moody, Dustin (Fed)
Subject: Re: My current point of view on standardization decisions
Date: Thursday, September 30, 2021 8:49:37 PM

Perfect.

I look forward to December 2021. =)

https://www.youtube.com/watch?v=ku7ohU1IGls

[OFFICIAL VIDEO] God Rest Ye Merry Gentlemen - Pentatonix

NEW ALBUM 'THE BEST OF PENTATONIX CHRISTMAS' OUT NOW! BUY: https://smarturl.it/bestofPTXmas?IQid=yt STREAM: https://smarturl.it/bestofPTXmas?IQid=yt A PENTATONIX CHRISTMAS TOUR 2019. TICKETS ON SALE AT https://ptxofficial.com/tour

www.youtube.com

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, September 29, 2021 9:00 AM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Re: My current point of view on standardization decisions

Thanks.

I'll hold onto this and we'll see if it changes in the next few months!

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Tuesday, September 28, 2021 7:42 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: My current point of view on standardization decisions

KEMs:

Kyber/NTRU
HQC

SIKE

Sigs:

Falcon
LMSS
Standard UOV

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Tuesday, September 28, 2021 7:41 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: My current point of view on standardization decisions

(which is an argument for skipping SPHINCS+)

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Tuesday, September 28, 2021 7:41 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: My current point of view on standardization decisions

eventually HQC (or BIKE) and maybe 1 new signature like
MAYO https://eprint.iacr.org/2021/1144.pdf or just Standard UOV.

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Tuesday, September 28, 2021 7:40 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: My current point of view on standardization decisions

oh-- obviously SIKE should be standardized at some point, if people can be convinced they understand its security argument

So, dream world for me is something like:

Kyber/SIKE/Falcon, and maybe SPHINCS+

or as a backup

NTRU/SIKE/Falcon, and maybe SPHINCS+

From: Apon, Daniel C. (Fed)
Sent: Tuesday, September 28, 2021 7:36 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: My current point of view on standardization decisions

Hi Dustin,

I expect there's very little that will come up in a few months that will change my opinions on standardization choices (although, who knows!) so I thought I would go ahead and share them with you.

The only proposal I've heard so far is something close to "Standardize Classic McEliece and move all lattices into a 4th round."
This, as you well know, would be an absolute, unmitigated disaster, and an abject failure of our job responsibilities.

That said--

Kyber/Saber/NTRU:
If the IP situation can be resolved (seems unlikely) or we are confident with moving forward despite the IP situation, then I would pick Kyber.
There is no world in which I believe Saber should be standardized.
If we want to yield to CNRS (and flame them publicly), then NTRU is a fine enough choice (but unfortunate we're forced into a scientifically lesser position by global politics).
It's certainly a major disappointment if we go with NTRU, but I guess we seem to be stuck with it.

Classic McEliece:
I would tend 20/80 towards not standardizing it. There would have to be an extremely strong and new argument to convince me that it's worth standardizing. Fundamentally, it's too expensive.

Dilithium/Falcon:
Currently, I lean 55/45 towards picking Falcon over Dilithium (based on the significant difference in performance profile), but I could be convinced otherwise. Both schemes seem generally secure, but I also have some concerns about 'optimizations' in Dilithium's design that I worry will weak its security claims going forward.

SPHINCS+:
I am entirely 50/50 here. There is a solid argument for going ahead with standardization for some signature scheme that's not lattice-based. Yet, on the other hand, it's so cumbersome in performance that I really don't know anyone who want to use it (particularly in the context of stateful hash-based signatures already being standardized).

Picnic:
There's been too many updates to believe the design is stable. There are many improvements

to the design that are in published works in the past year and half or so. I believe an updated MPCitH design, or multiple?, should be crafted (in order to be stable, if possible) and submitted to the on-ramp. It should not be standardized as-is.

Rainbow/GeMSS:
Nope. Send a new UOV version to the on-ramp if anything. (More generally, I'm not entirely convinced the on-ramp will lead to good outcomes, but maybe I'm wrong.) I'm not yet confident in this projection enhancement technique for the GeMSS design either.

Frodo/HQC/BIKE:
I think all of these should move on to a 4th Round and be considered later on. My preference is for HQC over BIKE, unless BIKE can provide a proper analysis. Arguments from experiments and projections of curves on graphs are unique to BIKE, and should not constitute valid evidence for its security. Frodo should be considered in the context of a superior version of McEliece in the future.

NTRUPrime:
Nope. Further, it should not advance to a 4th Round.