From:	Kelsey, John M. (Fed)
To:	Dang, Quynh H. (Fed); Apon, Daniel C. (Fed); Perlner, Ray A. (Fed); Moody, Dustin (Fed); internal-pqc
Subject:	Re: The path to standardization
Date:	Friday, June 12, 2020 2:07:00 PM

How long after a major change in an algorithm would we feel like we needed to wait before moving forward with standardization? I mean, if GeMSS has that major of a tweak, I'd want to consider it as a round 4 alternate, not a fallback for round 3.

--John

From: "Dang, Quynh H. (Fed)" <quynh.dang@nist.gov>
Date: Friday, June 12, 2020 at 13:58
To: "Apon, Daniel C. (Fed)" <daniel.apon@nist.gov>, "Perlner, Ray A. (Fed)" <ray.perlner@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: Re: The path to standardization

Agree! However, how many times have crypto proofs with errors/ gaps gone unnoticed for a long time ?

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Friday, June 12, 2020 1:56 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: The path to standardization

I still believe it's worth hearing out the science first before reaching this conclusion

---

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Friday, June 12, 2020 1:52 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: The path to standardization

Kyber512 is an example that something we did not see; we had complete confidence on it. But, it turned out there is something we should examine more.

It is bad that we make an impression that we weaken security and if something went wrong, we would be in really bad spot.

So, it is not worth the risk since likely GeMMS is not going to be standardized

---

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Friday, June 12, 2020 1:47 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: The path to standardization

Probably it's worth hearing the details about collision probabilities in the Feistel construction before pre-judging whether 3 rounds or 4 rounds makes sense for GeMSS.

I don't think Kyber has anything to do with that

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Friday, June 12, 2020 1:44 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: The path to standardization

Do we need to take this risk ? what is the proof is wrong has an error ? Look at Kyber512.

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Friday, June 12, 2020 1:42 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: The path to standardization

That's why security proofs are valuable!

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Friday, June 12, 2020 1:41 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: The path to standardization

what if we are wrong or new attacks that break 3 but not 4 that we have not seen ?

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Friday, June 12, 2020 1:38 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: The path to standardization

The point is that 3 rounds appears to meet the required security level

---

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Friday, June 12, 2020 1:38 PM
To: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: The path to standardization

I think we should not ask people to lower security of a scheme.

From: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Sent: Friday, June 12, 2020 1:31 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: The path to standardization

I also mostly agree with the summaries with a couple of quibbles:

I second Daniel A's point that NTRU's main path to standardization involves IPR concerns for the newer lattice schemes.

Regarding tweaks. Daniel and I have been considering a specific tweak to GeMSS (3 instead of 4 rounds for the Feistel Patarin construction, leading to somewhat better performance.) You currently have that listed as tweaks discouraged.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Friday, June 12, 2020 1:26 PM
To: Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: The path to standardization

John,
I mostly agree with those informal explanations. I think for SIKE though, the description might not be completely right. I don't think SIKE needs big tweaks. The actual algorithm is very stable. We'd like more confidence in the security, but mostly we want improved performance.

I think we can include some of this type of reasoning in the report, and people should add what they think is needed. Some of it is already covered, or is probably clear enough (I think the lattice finalists know they need to beat each other, as we state that we'll only choose one).

Dustin

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Friday, June 12, 2020 12:48 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: The path to standardization

Everyone,

This is my attempt to very briefly and informally state the path to standardization. In this list, I consider three categories: finalists, fallback alternates, and round 4 alternates.

My question is, does this more-or-less succinctly capture the path to standardization for each algorithm? Obviously we'll state this in a more polished and formal way in the report, but am I missing anything or wrong about anything?

Thinking about the algorithms this way makes me think we should be more clear about the distinction between round 3 finalists, round 3 fallbacks, and round 4 alternates, because these are quite different. We want minimal tweaks for finalists and fallbacks, but we encourage tweaks for our alternates—they won't be standardized until after somethink like a fourth round.

Finalists:

a. Classic McEliece
- Don't get broken

b. Kyber

c. Saber

d. NTRU
- Beat the other two, don't get broken
- NTRU: Be the last one standing when K and S both look shaky due to excessive optimization or insufficient grey hairs.

e. Falcon

f. Dilithium
- Beat the other one, don't get broken
- Falcon: Show your floating point stuff doesn't drag you down

g. Rainbow
- Don't get broken AND
- Don't be too terrible on IP issues

Alternates (Fallbacks): (Tweaks discouraged)

h. HQC
- BIKE doesn't go forward AND
- We see need for another code-based KEM.

i. GeMSS

- Rainbow doesn't go forward AND
- We see need for another multivariate signature (aka everything in signature finalists dies)

j. SPHINCS+

- Dilithium and Falcon get broken

OR

- We see demand for a paranoid signature option

k. NTRU Prime

- Advances in structured lattice analysis undermine Saber, Kyber, and NTRU AND
- Those advances do not undermine NTRU Prime AND
- We are comfortable with NTRU Prime's parameter selection based on their costing of attacks

l. Frodo

- Advances in structured lattice analysis undermine Saber, Kyber, and NTRU AND
- Those advances do not undermine Frodo

OR

- We see a need for a paranoid lattice KEM option

Alternates (Round Four): (Tweaks encouraged)

m. PICNIC

- Continued progress gives much better performance that SPHINCS+ AND
- We see need for a symmetric-only signature AND
- Scheme ripens enough that we're sure it's nailed down including LowMC security

n. BIKE

- Nail down decryption failures, add level 5 parameters AND
- We see need for another code-based KEM

o. SIKE

- Don't get broken AND
- Scheme and problem ripen enough we're comfortable standardizing it