From: Moody, Dustin (Fed)
To: Kelsey, John M. (Fed); internal-pqc
Subject: Re: Report convention
Date: Monday, June 15, 2020 11:04:30 AM

I'd say we can call out the competitors if it seems appropriate to do so. We don't need to go out of our way and insert it in just because.

I agree with the list of who's competing with who.

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Monday, June 15, 2020 10:54 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Report convention

Should we be explicitly calling out the likely competitors for each scheme? I wasn't sure whether this was reasonable to do.

As an example, I'd say we have the following competitors—we're going to standardize at most one of them.

KEMS:

a. Kyber, Saber, NTRU, (NTRU Prime)
b. (BIKE), (HQC)
c. (Sike) (no obvious competitors)
d. Classic McEliece (no obvious competitors)

Signatures:

e. Dilithium, Falcon
f. Rainbow, (GeMSS)
g. (SPHINCS+), (Picnic)

It would be clearer in our writeups to say what we think the competitors are, and we do say that in a couple places. Should we just say it for all the algorithms that have clear competitors?

--John