From: Kelsey, John M. (Fed)
To: Moody, Dustin (Fed)
Subject: Re: Terminology
Date: Thursday, June 25, 2020 2:45:31 PM

If the track 2 algorithms for round 3 are candidates, what do we call all the algorithms in round 2? They are currently also called candidates, I think.

--John

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, June 25, 2020 at 14:39
To: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: Re: Terminology

FYI - since our report was stable with no changes for a few days, I sent it to Jim and Sara to begin the WERB/approvals process. We can still make some edits if we want. The reviewers will probably have some comments for us to resolve.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, June 25, 2020 2:32 PM
To: Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Terminology

John,

I tried to unify this. I put in a couple of sentences that the 7 finalists are called "finalists" and that other 8 advancing on are called "candidates". We often add an adjective to the candidates, such as "additional candidates" or "alternate candidates". Did you find somewhere where "candidates" is being used to apply to the finalists?

Dustin

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Thursday, June 25, 2020 2:22 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Terminology

Everyone,

I'm going over the document again after not looking at it for a few days. One problem I keep noticing—we do not have consistent terminology for our track 1 candidates, our track 2 candidates, and for all the stuff in round 2.

The best terminology I've seen in our document for this is:

a. Track 1 candidates are “finalists.”
b. Track 2 candidates are “alternates,”
c. All the algorithms in the second round are “candidates.”

We can always put “algorithm” after that term—“finalist algorithm” or “alternate algorithm” or “candidate algorithm.” But I think we’d be much more clear if we tried to stick to this (or some other) consistent terminology for the different algorithms across the whole document. I keep seeing places where we use slightly different terminology for them in different sections (probably because each of us uses slightly different terminology).

Thanks,

--John