From:	Moody, Dustin (Fed)
To:	Barker, William C. (Assoc); Regenscheid, Andrew R. (Fed)
Cc:	Stine, Kevin M. (Fed)
Subject:	Re: ERB reader comments for PQC report
Date:	Monday, March 7, 2022 9:25:53 AM

Curt,

Thank you for the quick read! I'm sure the ERB will catch up to you at some point.

Yes, the comment format is fine. I'll take a look and make corrections.

Dustin

From: Barker, William C. (Assoc) <william.barker@nist.gov>
Sent: Monday, March 7, 2022 9:24 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
Cc: Stine, Kevin M. (Fed) <kevin.stine@nist.gov>
Subject: ERB reader comments for PQC report

Hi, Dustin. I've nothing yet from ERB, but my comments are attached and appended.
The comments provided are discretionary. Most actually have to do with commas. Those I thought were potentially significant or are questions are **bolded.**
I hope that the comment format works for you. I had real trouble with commenting the LaTex and/or .pdf as compiled. That's probably due to my not being familiar with the tool.
I do approve the NISTIR. As stated above, my comments are discretionary, and I'm sure that the community is waiting eagerly for the report's being posted.

ERB Reader Comments on NISTIR 8413

1) In the List of Figures, the Figure 2.10 identifier crowds into the title of the figure. The table formatting needs to be checked.
2) In 1.0 Introduction, the second sentence of thew fourth paragraph is broken up by a comma that does not belong.
3) In the Table 1.1 Timeline on Page 3, NISTIR 8309 (July 2020) and NISTIR 8413 (March 2020) probably shouldn't be hyphenated. The break is in the wrong place, if hyphenation is necessary (NIS-TIR rather than NIST-IR).
4) On Page 4, the last sentence of the Section 4 description in Section 1.1 would read better as: "This report presents reasons why candidate algorithms were selected for standardization, or for the fourth round as well as reasons why the other candidate algorithms were not selected."
5) On Page 4, the Section 5 description would read better as: "More details are provided on the process for standardizing the algorithms selected, and on the process for evaluating candidate algorithms selected for the fourth round."
6) In Section 2.1 on Page 4, the fifth sentence of the first paragraph might read better as: "Some of the alternate candidates have worse performance characteristics than the

finalists but might yet be selected for standardization based on NIST's high confidence in their security."

7) **In Section 2.1 on Page 4, the first two sentences of the second paragraph might read better as: "The seven finalists included four key-establishment mechanisms (KEMs) or public-key encryption schemes and three digital signature mechanisms. Of the eight alternates, five were KEMs or encryption schemes, and three were digital mechanisms.**
8) In Section 2.2.1 on Page 6, the comma is not really needed in the third sentence of the second paragraph on the page (fourth paragraph of the section). Just "IND-CCA2 security is not required in strictly ephemeral use cases and attempting to meet the more stringent requirements of IND-CCA2 security may incur significant performance penalties for some schemes" is better.
9) In the second sentence of the third paragraph on Page 6 (fifth paragraph of Section 2.2.1), a comma is needed: "In some cases, questions have arisen regarding whether various parameter sets meet their claimed security strength categories."
10) In the second sentence of the fourth paragraph on Page 6 (sixth paragraph of Section 2.2.1), "real world" needs to be hyphenated (real-world).
11) In the third sentence of the first paragraph on Page 7 (the eighth paragraph of Section 2.2.1), "third round" needs to be hyphenated (third round).
12) **In the first sentence of the second paragraph on Page 7 (the ninth paragraph of Section 2.2.1), it might be more clear to say: "During the first, second, and third rounds of the NIST standardization process, a number of cryptanalytic results dramatically reduced the security assumed for some submitted schemes and undermined NIST's confidence in the maturity of others." Actual security afforded may be affected by not yet identified attacks.**
13) In the first sentence of the third paragraph on Page 7 (the tenth paragraph of Section 2.2.1), since the third round is complete, it might be better to say: "Progress was also made.."
14) **In the third sentence of the fourth paragraph on Page 7 (the eleventh paragraph of Section 2.2.1), would it be more accurate to say: "NIST does not feel the need to establish these standards all at once" rather than "NIST does not feel the need to choose these standards all at once"? We're choosing mechanisms that will be the basis for standards.**
15) In the first full sentence on Page 11 (I think the 13th paragraph of Section 2.2), the comma is not really needed (…the figure does not include the cost of key generation since signature keys are not generated on a per-transaction basis).
16) In the first sentence of the last full paragraph on Page 12 (immediately following Figure 2.5), a comma is needed between Figure 2.7 and Figure 2.8 references.: "Figure 2.7 shows the computational performance numbers from [34] for the ARMCortex-M4 processor for the security category 1, 2, and 3 parameter sets of Dilithium and FALCON parameter sets, and Figure 2.8 shows the "total costs" when an estimated 2000cycles/byte transmission cost is added."
17) In the second sentence of the last full paragraph on Page 16, "real world" should probably be hyphenated (The 3rd Round saw some real-world experiments…).
18) On Page 17 in the fourth sentence of the third paragraph of 2.3, it would be better to say: "three other KEM alternates (BIKE, HQC, and SIKE) are better suited than FrodoKEM for this

role" rather than "three other KEM alternates (BIKE, HQC, and SIKE) are better situated than FrodoKEM for this role."

19) In the next to the last sentence of the same paragraph, either "this criterion" or "these criteria" would be grammatically correct.
20) On Page 18, in the last sentence of the fifth paragraph of Section 2.3. might it be better to say "With respect to" than "In regards to"?
21) On the bottom of Page 18, in the second sentence of the sixth paragraph of Section 2.3, the comma is not needed (are based on structured codes and would be suitable).
22) In the sixth sentence of the same paragraph on Page 19, the comma is also not needed (Classic McEliece was a finalist, but is not being standardized).
23) In the next sentence, a comma is needed after "however".
24) On Page 19, in the last sentence of the sixth sentence of Section 2.3, the second comma is not needed: "NIST selected Dilithium as the primary signature algorithm that it will recommend for general use and will prioritize its standardization."
25) At the bottom of Page 20, in the first sentence of Section 3.2, it might be more clear to say: "This section presents some of the hard computational problems that are common to multiple code-based, multivariate-based or lattice-based schemes examined in the course of the NIST PQC Standardization Process."
26) In the first sentence of Section 3.2.1 at the top of Page 21, would it be better to say: "The difficulty of the general- and syndrome-decoding problems (and some variants thereof) is a component of the security argument"?
27) Do we need the parentheses in the next sentence?
28) Starting on Page 23, the headings associated with the formal enumeration of security problems may confuse some readers. In some cases, we have a descriptive heading for a set of related problems. In others, we just number the problem and add a parenthetical descriptive label. In yet other, the problem is described but not enumerated. I was able to follow the material, but it's possible that some editors will be confused by the mixed enumeration scheme. This is just an observation. I don't have strong feelings about the observation. Would indentation help here?
29) On Page 25, in the second sentence of the third paragraph of Section 3.3.1, the second paragraph, the comma is not needed. (Roughly speaking, in this model the adversary is granted oracle access to the signing function and must produce a valid signature for a message that has not previously been signed by the oracle.)
30) On Page 26, in the first sentence of 4.1, we could say: " KYBER is a module learning with errors-based (MLWE-based) key encapsulation mechanism the original design of which was presented in…" I could go either way on the hyphenation issue, but the mechanism should be a *which* rather than a *who*.
31) On Page 27, in the second paragraph under KYBER *Security*, the second sentence isn't very clear to me. Are you saying: "Using this variant of the FO transform holds tightly in the ROM [152, 153] and non-tightly in the QROM."?
32) On Page 27, in the first sentence of the first paragraph under *Performance*, we might just say "In comparison, KYBER's bandwidth is smaller than NTRU, but about 10% larger than Saber."
33) Just a nit, but in the last paragraph under performance on Page 27, "efficiently enough" for what? Maybe "has adequate performance in many different environments"?

34) On page 28, at the end of the last sentence of the third paragraph under *Significant events since Round 2,* a period is needed.
35) On Page 28, the last sentence of the last paragraph of Section 4.1 might read better as: "NIST finds the MLWE problem which KYBER is based upon marginally more convincing than the MLWR or NTRU assumptions which Saber and NTRU are respectively based upon."
36) On Page 30, in Section 4.3, in the third sentence of the first paragraph, "second round" should be hyphenated (second-round).
37) On Page 31, in Section 4.3, in the third sentence of the *Performance* paragraph, a comma should follow "However".
38) On Page 31, in Section 4.3, in the first sentence under *Overall assessment*, the comma should be deleted ("NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (in some cases under a different claimed security strength).")
39) At the bottom of Page 31, in the first sentence of Section 4.4, the comma should be dropped. ("The motivation for the HQC framework was to generate a code-based scheme that could benefit from a quasi-cyclic structure but have a more direct security reduction to the problem of decoding a random linear code.")
40) On Page 32, in the second sentence of the first paragraph of Section 4.4., the comma is not needed. (The motivation for the HQC framework was to generate a code-based scheme that could benefit from a quasi-cyclic structure but have a more direct security reduction to the problem of decoding a random linear code.)
41) On Page 32, in the third sentence of the second paragraph under. *Security*, you need to check to see that the hyphen is necessary. (The provably and sufficiently-low decryption failure rate is required for proper application…)
42) On Page 33, in the second sentence of the second paragraph of Section 4.5. the third comma is unnecessary. (In some sense, the isogeny-finding problem can be viewed as a loose analogue of the discrete log problem, but using a large graph (the isogeny graph) rather than an abelian group.)
43) In the next sentence, would it be better to say "currently known" rather than "currently-known"?
44) On Page 34, the second sentence under *Security* might read better as: "This problem can be solved using a meet-in-the-middle algorithm or by using quantum algorithms for claw-finding and collision-finding."
45) On Page 35, in the second sentence under *Performance*, a comma is needed following "However" (However, SIKE requires both parties…)."
46) On Page 35, in the third sentence under *Overall assessment*, it's not clear that the hyphen is needed ("better placed" rather than "better-placed."
47) On Page 37, in the first sentence under *Security*, the "a" in the sentence should probably be removed: "The NTRU KEMs have tight CCA-security proofs in the ROM and non-tight security proofs in the QROM."
48) On Page 38, in the third sentence of the fourth paragraph under Section 4.7, *Security*, the commas are not really needed: "The specification analyzes quantum versions of the above attacks as well but notes that all existing claims of a quantum speedup for lattice reduction algorithms rely on the Quantum-RAM model of computation which the submission describes as sufficiently unrealistic to be irrelevant to the security of NTRU in

practice.

49) On Page 38, in the first sentence of Section 4.8, the second comma is not needed:" NTRU Prime was first proposed in [220], as an exploration of the design space of "NTRU-like" cryptosystems, with the goal of improving on the original NTRU scheme in terms of security as well as performance."
50) On Page 38, in the second sentence of 4.8, the comma is not needed: "The original parameter sets for NTRU Prime had very good performance but relied on optimistic estimates of the concrete security strength of the cryptosystem."
51) On Page 39, Section 4.8, in the seventh sentence of the second paragraph under *Security*, the comma is not necessary: " Other risks are harder to manage or understand."
52) On Page 40, in the last sentence of the second paragraph of Section 4.8's *Performance*, the comma is not necessary: "Faster performance can be obtained by generating many keys simultaneously in batches and implementing the scheme in an FPGA [221, 222]."
53) On Page 41, in the second sentence of the second paragraph of Section 4.9, "precedent" is spelled incorrectly.
54) On Page 42, in the third sentence of Section 4.9's *Overall assessment*, the comma is not necessary: "Nonetheless, NIST determined that there was no compelling reason to standardize multiple different structured lattice KEMs and chose KYBER instead of Saber."
55) On Page 44, in the last sentence of Section 4.4.1's *Overall assessment*, the comma is not necessary: "It is an excellent choice for a broad range of cryptographic applications, and is the primary signature algorithm selected by NIST for standardization at this time."
56) On Page 45, in the last sentence of the first paragraph under Section 4.4.2's *Security*, the comma is not needed, and the sentence would read better as two sentences: "We remark that parameterizing FALCON for intermediate security levels is possible but may require a different choice of modulus and ring. This could further complicate implementation."
57) On Page 46, the third sentence of Section 4.4.3's second paragraph unde *Design* is hard to parse. It might read better as: "The designers of SPHINCS have considered a wide range of parameter set choices, and have proposed two sets for each security category. One set makes the signature faster at the cost of larger signatures, and the other set makes the signature smaller at the cost of slower signatures."
58) On Page 47, the fourth sentence of Section 4.5.1's *Performance* has an unnecessary comma: "The WhiteGeMSS, CyanGeMSS and MagentaGeMSS parameter sets were added in the third round and use fewer rounds in the Feistel-Patarin construction thanthe GeMSS, BlueGeMSS and RedGeMSS parameter sets."
59) The next to last sentence of the same paragraph is a bit long and hard to parse. The material might read better as: "GeMSS and WhiteGeMSS rely the least (although still significantly) on the vinegar and minus modifiers for their security. These parameter sets have the slowest signing algorithms as a result. RedGeMSS and MagentaGeMSS rely the most on the vinegar and minus modifiers and are the fastest."
60) On Page 49, there is an unnecessary comma in the fourth sentence under Section 4.5.3's *Design*: "Specifically, this map contains terms that are quadratic in the vinegar variables and terms that are bilinear in the oil and vinegar variables but contains no terms that are quadratic in exclusively the oil variables."
61) **On Page 49, should the second sentence under the second paragraph of *Design* say "map" rather than "maps"? (The entire maps is then composed with linear maps to hide**

the structure.)

62) On Page 50, the last sentence of Section 4.5.3's *Performance* has an unnecessary comma: "The key sizes of Rainbow parameters arequite large in comparison to other finalists, but are still significantly smaller than GeMSS."

63) On Page 50, the third sentence of *Significant events since Round 2* is confusing (possibly because I don't understand actually correct terminology. Did you really mean to say: "Together with the support minors method of solving MinRank instances, see [141], this new "rectangular MinRankattack" showed that all of the Rainbow parameters failed to meet their purported security levels in the gate metric."?

64) On Page 51, in the second sentence of the fourth paragraph of Section 5, a comma might follow "2022". [...must be submitted to NIST by July 1, 2022 and must…]

65) Is the next paragraph supposed to be indented?

66) On Page 51, in the sixth sentence of the third full paragraph on the page, the comma is not needed. [NIST will decide which (if any)of the submitted signature algorithms to accept and initiate a new process for evaluation]

67) In third sentence of the next paragraph, the comma is not needed. [NIST hopes for rapid adoption of these first standardized algorithms and will issue future guidance on the transition.

From: William Barker <william.barker@nist.gov>
Date: Wednesday, March 2, 2022 at 10:16 AM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Regenscheid, Andrew R. (Fed)" <andrew.regenscheid@nist.gov>
Cc: "Stine, Kevin M. (Fed)" <kevin.stine@nist.gov>
Subject: Re: ERB readers for PQC report

Sorry for the delay, Dustin. I'd be happy to be an ERB reviewer and will wait for the notice from ERB.

On: 02 March 2022 10:03, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:

> Andy and Curt,
>
> Curt - I haven't heard back from you, so I'm hoping you're okay with my request to be an ERB reviewer for our PQC report. Please do let me know.
>
> I'd like to start the review process for our PQC 3rd Round Report for the PQC, NISTIR 8413. This is a high profile project, and we are hoping to announce the outcomes by the end of this month (along with having the report published). I know it will take time to review, but I hope we can get it done.
>
> We have written it in Overleaf (an online latex editor), and you can see the always current file at the link:
> https://www.overleaf.com/read/hsyhgvzqjmdm
> (If you're not familiar with overleaf, when you first open the site it will take a

minute to compile the current version. You can then view the .pdf on the right hand side of the screen, or if desired, you can click the down arrow on the right menu bar to download the pdf for easier viewing elsewhere.)

I've also attached a .pdf and .docx version of the currrent version, since that might be easier for reviewing and commenting. The word document messed up the formatting for the Figures in a few places, but you can see the correct Figures in the .pdf version.

The report is finished, although in a few places we are still revising the wording to our team's satisfaction (no big changes).

To help speed up the review, I'm giving you the copies to review. I haven't yet entered the report into the system for official ERB review yet because Jim and Isabel have to provide me some comments first.

Please let me know any questions or concerns, or anything else I can do to speed up the process. Thanks,

Dustin