From: Dang, Thinh H. (Fed)
To: Thinh Dang
Subject: Fw: NTRU Prime write-up
Date: Tuesday, March 22, 2022 3:43:25 PM

From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Sent: Monday, March 21, 2022 1:31 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: NTRU Prime write-up

Hey,

I just realized that Ray's recollection of our position on NTRU Prime at the end of round 2 is in fact documented and public. It's briefly mentioned in our round 2 report, but it's much more explicit in the NTRU Prime Official Comments, in Dustin's email on page 6 here:

https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-3/official-comments/NTRU-Prime-round3-official-comment.pdf

So it's good that we're sticking to this message in our round 3 report. I'm inclined to cite Dustin's email in the round 3 report...

--Yi-Kai

_____
From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Sent: Thursday, March 17, 2022 10:00 AM
To: Chen, Lily (Fed); Perlner, Ray A. (Fed); internal-pqc
Subject: Re: NTRU Prime write-up

I updated that sentence in the Overleaf document.

--Yi-Kai

_____
From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Wednesday, March 16, 2022 4:47 PM
To: Perlner, Ray A. (Fed); Liu, Yi-Kai (Fed); internal-pqc
Subject: RE: NTRU Prime write-up

It sounds like when we made the 3rd round finalist/alternate decision, we thought 2) as a possibility. Now we do not see the "strong" reason. Then NTRU Prime will not move to 4th round.

In any case, when we designated NTRU Prime an alternate, we did not know whether NTRU Prime will be involved in the 4th round for sure, which is a possibility.

I think Yi-Kai's new text is clear to avoid a possible misunderstanding.

Lily

-----Original Message-----
From: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Sent: Wednesday, March 16, 2022 4:17 PM
To: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: NTRU Prime write-up

My general recollection is that our plan was as follows:

1) If the claimed attack avenue on cyclotomic Ring/Module LWE didn't pan out, we would standardize one of Kyber/Saber/NTRU at the end of the 3rd round
2) If the claimed attack avenue did pan out, we would look to see if there was a strong reason to believe that NTRUprime was immune as claimed, thinking we'd need at least until the end of the 4th round to be sure.

(Since it didn't look like we were going to standardize NTRUprime at the end of round 3, but might standardize it after round 4 if certain conditions were met, we designated it as an alternate.) I do recall this plan being explicitly discussed at the time, but maybe the whole team only agreed that NTRUprime should be an alternate, but didn't agree why. For reference, this is what we said in the second round report, about why NTRUprime was an alternate:

" NTRU Prime was advanced to the third round but not as a finalist. Additional motivation for NTRU Prime's unique choice of algebraic structure could be gained by new progress in algebraic cryptanalysis of cyclotomic structures during the third round, provided that it undermines NIST's confidence in cyclotomic structures but clearly does not extend to NTRUprime's choice of Z_q[x]/(x^p-x-1)."

-----Original Message-----
From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Sent: Wednesday, March 16, 2022 3:45 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: NTRU Prime write-up

Yeah, I am ambivalent about the sentence: "NTRU Prime was designated an alternate, with the expectation that the most likely path to standardization for NTRU Prime would involve a fourth round." I didn't write that. Ray might have a stronger opinion about it. How about: "NTRU Prime was designated an alternate, with the expectation that further study would be needed before possible standardization."

--Yi-Kai

-----Original Message-----
From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Wednesday, March 16, 2022 2:52 PM
To: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: NTRU Prime write-up

Thanks, Yi-Kai,

The new version has improved a lot. I think it is more readable and more objective (even though some statements in [15] is subjective.)

Here is the only place I like to check one more time. At the end of the first paragraph in Overall assessment, we have a sentence "NTRU Prime was designated an alternate, with the expectation that the most likely path to standardization for NTRU Prime would involve a fourth round."

Then at the end, we said that " For these reasons, NIST is not moving NTRU Prime to the fourth round of the evaluation process."

Actually, for 3rd round, the alternates are selected for further study in the 3rd round and may be in 4th round. We can say something like "For the 3rd round, NTRU Prime was designated an alternate for further study for the evidence to support the security advantages for the unusual design features."

I might have misunderstood the meaning of the first sentence. Please check.

Lily

-----Original Message-----
From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Sent: Wednesday, March 16, 2022 12:29 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: NTRU Prime write-up

Hi everyone,

I went through and revised the NTRU Prime section of our report. I took out the more opinionated bits, and moved some sentences around to make it flow better. What do you all think? Please feel free to comment or edit. In particular, Lily, does this seem better to you? I think you were right, in the old version, the discussion of DJB's "lattice risks" document was too opinionated, and it was not very helpful to an outside person who is reading about this for the first time. I think the new version is better.

Thanks,

--Yi-Kai