From: Dang, Quynh H. (Fed)
To: internal-pqc; (b) (6)
Subject: Not asking for a level 5 option for NTRU Primes.
Date: Friday, June 12, 2020 6:33:02 AM

Hi Daniel,

I don't think we should say this " Finally, while NTRU Prime has considerable strength in its proposed level 1 parameters, NIST encourages the NTRU Prime team to provide a level 5 parameter set going into the 3rd round. ".

A possible reason you might have for the statement is that you want to have a better performance comparison with the other structured lattice KEMs which have level 5 options.

If that is the case, you should also ask Kyber and Saber's teams to include level 2 and level 4 options because NTRU Primes have these options.

If you say that levels 1 and 3 are more important, but levels 2 and 4 are not, then the question is why is that ? Why did we not say that in our call for proposals ?

If you say level 5 is more important than level 4, then the question is why is that ? Why did we not say that in our call for proposals ?

Quynh.