From: Perlner, Ray (Fed)
To: Moody, Dustin (dustin.moody@nist.gov)
Subject: Draft response to HQC
Date: Friday, April 5, 2019 1:24:00 PM

Dear HQC team,

It appears there are a few omissions in the specification document. In particular

1. It does not appear the use of the seed expander is fully specified. A full specification should include the value used for seed, diversifier, and maxlength, and the lengths of any outputs used in the various algorithms.
2. The generator matrix for BCH1 and BCH2 do not appear to be unambiguously specified except by reference to a coding theory text book. The specification should be self-contained, and it should be possible to reconstruct the generator matrix for each code without having to find external references or examine the reference implementation source code.

If you could correct these omissions by Monday, that would be appreciated
Thanks,