It seems weird to phrase it that way. I think the point of Andy's sentence there is that we may decide to standardize one of the alternates at the end of the third round, right? But I don't think that would change the fact that we had already named some things as finalists and others as alternates. I mean, if all the structured lattice KEMs get broken or dented and we decide to standardize Frodo at the end of the third round, it wouldn't mean that Kyber and Saber and NTRU got demoted to being alternates—it would mean that we just decided to standardize one of our alternates instead of one of our finalists.

That's a plausible outcome, as far as I can tell, for five or six alternates: SPHINCS+, GeMSS, HQC, SIKE, Frodo, and maybe BIKE. For example, imagine that over the next 18 months, we get a bunch of results that make us uneasy about the parameter selection for structured lattice schemes, and at the same time, there's a very clear upper bound on error rate for BIKE that lets them get CCA security. It seems very plausible to me that we standardize Frodo and BIKE as KEMs in that world. Then maybe we standardize a structured lattice KEM in another couple years when we feel like we know how the parameters should be selected.

But I don't think that would change the fact that Frodo and BIKE were both alternates instead of finalists. I can't imagine that we'd want to, say, announce that we'd demoted Saber to an alternate and Frodo to a finalist, six months from now.

--John

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, June 29, 2020 at 11:49
To: internal-pqc <internal-pqc@nist.gov>
Subject: PQC

Everyone,
    I don't have any plans for a meeting tomorrow. Let me know if you think we need one. The reviews for the report are still on going, and I'll make changes to suggestions we get back.
 Here's one Andy recommended we add in:

"It is possible that new analysis could result in an alternate candidate being elevated to being a finalist, in the case that NIST's confidence in the security of any of the finalists is greatly reduced."

Seems reasonable to me. It doesn't tie our hands and keeps our options open in case of an unexpected advance that breaks a finalist.

Dustin