From:	David A. Cooper
To:	Alagic, Gorjan (Assoc)
Subject:	Re: PQC
Date:	Tuesday, June 30, 2020 8:50:05 AM

On 6/29/20 7:00 PM, Alagic, Gorjan (Assoc) wrote:

> David: I of course agree that our actions should not shock anyone. I meant that the scenario "Frodo > Saber/Kyber because structured lattices are broken" as being shocking, not that our reasonable reactions to such a scenario would be shocking. I really wish I hadn't used that word now though. ��

Hi Gorjan,

That's okay. I was really just responding to John's use of "shocking":

On 6/29/20 1:38 PM, Kelsey, John M. (Fed) wrote:

> That is, we could just decide, at the end of the third round, that we're standardizing, say, Saber, Classic McEliece, and Frodo + Falcon, Rainbow, and SPHINCS+, with Frodo and SPHINCS+ explicitly chosen as paranoid options for people who want postquantum security but also are concerned that these structured lattice algorithms aren't as well-understood as they should be. There would be nothing shocking about that, and it wouldn't require a shocking new sequence of cryptanalysis results.

John seemed to be suggesting that it would be okay to standardize SPHINCS+ at the end of the third round without any advance notice to the community and even if Falcon were also standardized. He seemed to say that this would be okay since it would not be "shocking." I was responding to that.

I would have no problem if we standardized Frodo at the end of the third round if Saber and Kyber are broken. If that were to happen, the community would know well before we started making our final decisions that there were security concerns with structured lattices, and I would hope that we would explicitly tell the community that as a result of these concerns we are now considering Frodo for standardization at the end of the third round.

Dave