**From:** Moody, Dustin (Fed)
**To:** Regenscheid, Andrew R. (Fed)
**Subject:** Re: You were right
**Date:** Monday, June 29, 2020 2:44:46 PM

---

I'd say the reason was more like your first paragraph. We're confident in its security, but it is bad in performance. If we have Dilithium/Falcon then we don't need sphincs. If we decide we do need it, it can wait a little bit longer (4th round). We're just keeping it on ice.

I'm not sure what John thinks is more unclear about the new text. Is it because we say we'd only bump up an alternate to a finalist if there is a break, but he thinks there is a chance we might standardize an alternate at the end of the 3rd round for a different reason? I think once I understand his concern, we should be able to figure out a way to word things.

---

**From:** Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
**Sent:** Monday, June 29, 2020 2:34 PM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
**Subject:** Re: You were right

I'll rephrase.

If we're keeping SPHINCS+ around in case lattices and/or Rainbow fail, then it makes sense for SPHINCS+ to be an alternate. And if we start getting sufficiently worried about lattices or Rainbox, then we should come out and say SPHINCS+ is actively under consideration for standardization at the end of round 3.

If we're keeping SPHINCS+ around simply because we haven't decided if we should standardize on it, and the decision will be made somewhat independently of what happens with lattices/Rainbow, then it should have been a finalist. I don't think this was really the consensus of the group- at least, not for round 3.

-Andy

---

**From:** Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
**Sent:** Monday, June 29, 2020 2:27 PM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
**Subject:** Re: You were right

No! I was saying I didn't want to send that to the list for fear someone would interpret it that way.

---

**From:** Moody, Dustin (Fed) <dustin.moody@nist.gov>

**Sent:** Monday, June 29, 2020 2:03 PM
**To:** Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
**Subject:** Re: You were right

I'm not sure I understand what you are saying exactly, with your last message.

Are you wanting us to change some of the finalists and alternates?

---

**From:** Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
**Sent:** Monday, June 29, 2020 1:58 PM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
**Subject:** Re: You were right

I don't want to write this for fear it could blow up the delicate compromise that's been crafted here, but...

As John's last email said, there's a small number of alternates that are probably best described as backups. There's things we could standardize if we really wanted to, but something moderately drastic, or at least unexpected, would have to happen with the finalists.

If that's not the case for the things in John's list A, then they should probably be finalists, not alternates.

If that is the case, then I'm just saying we should say when that unexpected thing happens that causes us to strongly consider standardizing something from A.

---

**From:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
**Sent:** Monday, June 29, 2020 1:52 PM
**To:** Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
**Subject:** Re: You were right

You never know what some people will want to discuss. Some changes go without notice. But this one seemed likely to me.

Working on trying to tamp it down....

---

**From:** Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
**Sent:** Monday, June 29, 2020 1:51 PM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
**Subject:** You were right

I definitely underestimated the reaction that change would have.