

**From:** [Moody, Dustin \(Fed\)](#)  
**To:** [Liu, Yi-Kai \(Fed\)](#)  
**Subject:** Re: PQC Round 2 report assignments  
**Date:** Wednesday, June 3, 2020 9:14:59 PM

---

No worries!

---

**From:** Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>  
**Sent:** Wednesday, June 3, 2020 4:47 PM  
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>  
**Subject:** Re: PQC Round 2 report assignments

Hi Dustin,

I'm sorry I've been slow in getting to this... there are too many other things happening at the same time. I'll work on it tonight...

--Yi-Kai

---

**From:** Moody, Dustin (Fed) <dustin.moody@nist.gov>  
**Sent:** Wednesday, June 3, 2020 11:34 AM  
**To:** Cooper, David A. (Fed)  
**Cc:** internal-pqc  
**Subject:** Re: PQC Round 2 report assignments

David,

We could put them wherever we think best. I agree with you that it seems to make more sense to move many of these details to 2.2.2. Section 2.2.3 is Algorithm and Implementation Characteristics, so it is appropriate to have some details there, but certainly 2.2.2. does seem like the more obvious place.

Please edit as you wish and make changes.

Dustin

---

**From:** David A. Cooper <david.cooper@nist.gov>  
**Sent:** Wednesday, June 3, 2020 11:23 AM  
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>  
**Cc:** internal-pqc <internal-pqc@nist.gov>  
**Subject:** Re: PQC Round 2 report assignments

I'm a bit confused about what material should be covered in what section. In particular, in Section 2.2.3 almost all of the text after the first paragraph is about cost/performance and security even though it would seem that such material belongs in the preceding two sections.

Section 2.2.3 mentions "performance in different use cases," "performance data in software and hardware," "costs of achieving constant-time implementations," and costs of countermeasures to side channel attacks. If these are all to be covered in Section 2.2.3, that doesn't leave much to say in Section 2.2.2.

On 6/2/20 3:08 PM, Moody, Dustin (Fed) wrote:

- \* Yi-Kai, Section 1 - Introduction
- \* Ray, Section 2.2.1 - Security
- \* David, Section 2.2.2 - Performance
- \* Quynh, Section 2.2.3 - Algorithm and implementation char.
- \* Daniel ST, Section 2.3 - selection of 3rd round candidates
- \* Angela, Section 4 - Conclusion. Maybe add in something about the on ramp idea (esp. for non-lattice general purpose signatures)