

**From:** [Moody, Dustin \(Fed\)](#)  
**To:** [Kerman, Sara J. \(Fed\)](#)  
**Subject:** RE: another modification to the pqc page  
**Date:** Monday, December 19, 2016 2:22:00 PM

---

Thanks!!

---

**From:** Kerman, Sara J. (Fed)  
**Sent:** Monday, December 19, 2016 2:22 PM  
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>  
**Subject:** RE: another modification to the pqc page

This is done. Removing Q2 also removed the last two footnotes (which have been moved to the archived version).

Sara

---

**From:** Moody, Dustin (Fed)  
**Sent:** Monday, December 19, 2016 10:13 AM  
**To:** Kerman, Sara J. (Fed) <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)>  
**Subject:** another modification to the pqc page

Sara,

Ray would like FAQ #2 "[Why are hash functions assigned fewer bits of quantum security than classical security?](#)"

and it's answer put in the archive, instead of being one of our current FAQ. Would that be alright?

Thanks,  
Dustin