

**From:** [Bassham, Lawrence E \(Fed\)](#)  
**To:** [Moody, Dustin \(Fed\)](#)  
**Subject:** Re: PQC API  
**Date:** Monday, November 14, 2016 12:28:08 PM

---

I changed the order of the parameters the way Dan suggested (output values listed fist), corrected the name problem (had omitted the "\_KAT") on the last two calls, and verified the use of pointers on certain values. I did not take the "randomness()" suggestion from Dan (for the KAT values) or the uint64 suggestion from someone else. I'll get you the file soon.

Larry

---

On: 14 November 2016 09:00, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:  
Larry,  
Any update on the PQC API? No rush yet, but wanted to see if you've had any issues come up. We need it by the end of this week for sure. Thanks,  
Dustin