

From: [Alperin-Sheriff, Jacob \(Fed\)](#)
To: [Moody, Dustin \(Fed\)](#); [Perlner, Ray A. \(Fed\)](#)
Subject: Re: Another question
Date: Monday, October 31, 2016 12:40:32 PM

Okay, I guess Ray and I can figure it out

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, October 31, 2016 at 12:26 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: RE: Another question

I'll make sure you're signed up for the pqc-forum.

I'm going to have Ray respond to the questions on KEM. He's probably at lunch right now.

Dustin

From: Alperin-Sheriff, Jacob (Fed)
Sent: Monday, October 31, 2016 12:25 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Another question

Also, should I have done something to sign up for the PQC-forum emails? I thought I had but I don't seem to have gotten this forwarded to me ...

Also this whole KEM vs. key exchange thing is a major component of the summary, so if it has to be changed that's going to delay things some. I will focus on finishing up the security measures section ...

—Jacob Alperin-Sheriff