From:	Liu, Yi-Kai (Fed)
To:	(b) (6); Chen, Lily (Fed); Moody, Dustin (Fed)
Subject:	Re: Question
Date:	Wednesday, June 15, 2016 4:05:27 PM

Hi Daniel,

Another thing we can do is talk to program managers (at IARPA, for instance) who fund these projects, or attend some of the program review meetings. Those meetings can be informative, though they are quite technical. Most of that discussion is on a 5-year time scale, though, which may not be very helpful for planning the deployment of post-quantum crypto.

One issue is that as people start building larger quantum computers, more and more of that work is going to be engineering rather than science, and so it will be more likely to be proprietary, and less likely to be published. So we may need to talk directly with companies and funding agencies, to find out what they are working on.

Cheers,

--Yi-Kai

From: Daniel Smith (b) (6)
Sent: Wednesday, June 15, 2016 3:12:27 PM
To: Chen, Lily (Fed); Moody, Dustin (Fed); Liu, Yi-Kai (Fed)
Subject: Question

Hi,

I was wondering if we have any avenue for getting information directly from teams working on quantum engineering projects.

I was browsing a couple of nights ago through science news outlets and found an article saying that a team from NIST has been able to make a quantum simulator with as many as 219 entangled beryllium ions. The fact that I was finding out such interesting information from outside of NIST made me think about how communication with NIST groups (at least those who are directly working on quantum information technology) might grant us some different perspective, at least on the timing or perhaps the model of an eventual quantum computer. I'm not sure if such insight would significantly impact the pqc project, but any extra perspective should be useful in some way.

I think that Stephen and Yi-Kai have been our liaison officers in this respect. Do you think that there would be any benefit from communicating directly with these groups? Are there useful questions we might ask that might help us in planning (e.g. time-line, expectations of cost for certain algorithms)? Is there a benefit beyond getting periodic reports from Stephen and Yi-Kai?

I'm curious what you think.

Cheers,
Daniel