From:	Moody, Dustin (Fed)
To:	Liu, Yi-Kai (Fed); Perlner, Ray A. (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Jordan, Stephen P (Fed)
Cc:	Chen, Lily (Fed); Peralta, Rene C. (Fed)
Subject:	RE: PQC talks
Date:	Thursday, May 5, 2016 1:36:32 PM

I'm not opposed to trying this out. It would be great to spread out the workload. However, I worry that not everyone will read the paper, and then the meeting won't be very effective. Perhaps we can discuss this on Tuesday, and set a schedule for which papers on which days.
Dustin

From: Liu, Yi-Kai (Fed)
Sent: Wednesday, May 04, 2016 11:32 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu) <daniel-c.smith@louisville.edu>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
Subject: Re: PQC talks
Hi everyone,
I was thinking about the way we've been running this reading group, and I wonder if anyone would be interested in trying out a different mode of operation?
Instead of having one person give a talk and everyone else listens, we could try to have more of a group discussion. For instance, we could go through the paper together and talk about any points that were interesting or confusing. To make this work, I think one person should (shall? must?) read the paper carefully and be responsible for leading the discussion (but no need to make slides). However, everyone else should also spend at least an hour skimming through the paper.
I like this idea because it spreads out the workload more evenly across people and across time, and because I think we will all learn more this way. What do you all think?
As for things to read, here are a few suggestions:
"Efficient Distributed Quantum Computing"
http://arxiv.org/pdf/1207.2307v2.pdf
(thanks, Ray!)
"Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?"
https://cr.yp.to/hash/collisioncost-20090517.pdf
(thanks, Ray!)
"Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3"
http://arxiv.org/abs/1603.09383
There's also a video: http://www.birs.ca/events/2016/5-day-workshops/16w5029/videos/watch/201604211609-Gheorghiu.html
(thanks to Julien Ross at QuICS for this suggestion)
Cheers,
--Yi-Kai

From: Moody, Dustin (Fed)
Sent: Monday, May 2, 2016 1:23 PM
To: Perlner, Ray (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu);

Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed)
Subject: PQC talks
Everyone,
We can probably start resuming our meetings with the NSA, where we have someone talk on a topic/paper. They are going to get several talks prepared, and we need to do the same here. Can all of us choose something that we can give a talk on sometime? Thanks.
Dustin

- I will do Microsoft's recent paper on **Efficient algorithms for supersingular isogeny Diffie-Hellman**