From: Apon, Daniel C. (Fed)
To: Kelsey, John M. (Fed)
Subject: Re: Lattice based schemes
Date: Monday, August 26, 2019 2:53:17 PM

Sounds like you got the general message I had in my head..
Something like: There's an "ideal" lattice scheme out there (written in The Book, if you will) that is only attackable if things like complexity theory are attackable. And we have some decent candidate-approximations still alive in our process.

Hooray for cafeterias, this coast or that :-)

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Monday, August 26, 2019 2:48:25 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Re: Lattice based schemes

Sure!   Mainly, I just wanted to see if I understood what you were saying, and also to try to get my own thoughts w.r.t. how surprised I should be if something gets broken into coherent order.

I'll be in the office tomorrow, let's catch up. We can eat some ***different*** cafeteria food for lunch!

Thanks,

--John

From: "Apon, Daniel C. (Fed)" <daniel.apon@nist.gov>
Date: Monday, August 26, 2019 at 14:46
To: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>
Subject: Re: Lattice based schemes

Hey John!

This is probably too much case-analysis to labor into an email. Want to meet tomorrow to chat through it more?

--Daniel

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Monday, August 26, 2019 2:25:09 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Lattice based schemes

Daniel,

From our conversation last night, it seems like you have a lot of confidence in the underlying lattice problems (a much better solution to those implies all kinds of progress in other areas, and would likely be big news outside of crypto). And also I think I got that you think that there are several schemes where you don't think there's any other way to approach breaking the schemes but to attack the hard problem. Is that basically right? This left me with a couple questions:

a. Do you have a sense of what other possible losses of security you might get from those schemes, in terms of extra assumptions that are being made or something? Can we get that explicitly from the proofs? It seems like writing that down for each of the most solid schemes would be really helpful!

b. How big does an improvements in the best heuristic algorithms for solving the underlying problems have to be, before it calls the parameters of the current schemes into question? I'm imagining something equivalent to an improvement in the best factoring algorithms that don't make factoring trivial, but require us to move everyone to 4K RSA keys or something.

This is mainly so I understand things better, but probably a lot of other people are in the same boat w.r.t. not having a good sense of how likely it is that some scheme will get broken, either in the crushing "throw it away, it's dead" sense or in the "the scheme is fine but the level 5 parameters are now the new level 1 parameters" sense.

Thanks,

--John